

# Security Designs for the Cloud, IoT, and Social Networking

Edited by:

**Adele Kuzmiakova**





# **Security Designs for the Cloud, IoT, and Social Networking**



# **Security Designs for the Cloud, Iot, and Social Networking**

*Edited by:*

**Adele Kuzmiakova**



[www.arclerpress.com](http://www.arclerpress.com)

# **Security Designs for the Cloud, IoT, and Social Networking**

*Adele Kuzmiakova*

## **Arcler Press**

224 Shoreacres Road

Burlington, ON L7L 2H2

Canada

[www.arclerpress.com](http://www.arclerpress.com)

Email: [orders@arclereducation.com](mailto:orders@arclereducation.com)

## **e-book Edition 2022**

ISBN: 978-1-77469-286-8 (e-book)

This book contains information obtained from highly regarded resources. Reprinted material sources are indicated and copyright remains with the original owners. Copyright for images and other graphics remains with the original owners as indicated. A Wide variety of references are listed. Reasonable efforts have been made to publish reliable data. Authors or Editors or Publishers are not responsible for the accuracy of the information in the published chapters or consequences of their use. The publisher assumes no responsibility for any damage or grievance to the persons or property arising out of the use of any materials, instructions, methods or thoughts in the book. The authors or editors and the publisher have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission has not been obtained. If any copyright holder has not been acknowledged, please write to us so we may rectify.

**Notice:** Registered trademark of products or corporate names are used only for explanation and identification without intent of infringement.

## **© 2022 Arcler Press**

ISBN: 978-1-77469-105-2 (Hardcover)

Arcler Press publishes wide variety of books and eBooks. For more information about Arcler Press and its products, visit our website at [www.arclerpress.com](http://www.arclerpress.com)

## ABOUT THE EDITOR



**Adele Kuzmiakova** is a computational engineer focusing on solving problems in machine learning, deep learning, and computer vision. Adele attended Cornell University in New York, United States for her undergraduate studies. She studied engineering with a focus on applied math. While at Cornell, she developed close relationships with professors, which enabled her to get involved in academic research to get hands-on experience with solving computational problems. She was also selected to be Accel Roundtable on Entrepreneurship Education (REE) Fellow at Stanford University and spent 3 months working on entrepreneurship projects to get a taste of entrepreneurship and high-growth ventures in engineering and life sciences. The program culminated in giving a presentation on the startup technology and was judged by Stanford faculty and entrepreneurship experts in Silicon Valley. After graduating from Cornell, Adele worked as a data scientist at Swiss Federal Institute of Technology in Lausanne, Switzerland where she focused on developing algorithms and graphical models to analyze chemical pathways in the atmosphere. Adele also pursued graduate studies at Stanford University in the United States where she entered as a recipient of American Association of University Women International Fellowship. The Fellowship enabled her to focus on tackling important research problems in machine learning and computer vision. Some research problems she worked on at Stanford include detecting air pollution from outdoor public webcam images. Specifically, she modified and set up a variety of pre-trained architectures, such as DehazeNet, VGG, and ResNet, on public webcam images to evaluate their ability to predict air quality based on the degree of haze on pictures. Other deep learning problems Adele worked on

include investigating the promise of second-order optimizers in deep learning and using neural networks to predict sequences of data in energy consumption. Adele also places an emphasis on continual education and served as a Student Leader in PyTorch scholarship challenge organized by Udacity. Her roles as the Student Leader were helping students debug their code to train neural networks with PyTorch and providing mentorship on technical and career aspects. Her hobbies include skiing, playing tennis, cooking, and meeting new people.



# TABLE OF CONTENTS

---

<i>List of Figures</i> .....	<i>xi</i>
<i>List of Tables</i> .....	<i>xiii</i>
<i>List of Abbreviations</i> .....	<i>xv</i>
<i>Preface</i> .....	<i>xix</i>
<b>Chapter 1 Cloud Computing Overview</b> .....	<b>1</b>
1.1. Introduction.....	2
1.2. Cloud Computing Layers.....	3
1.3. Deployment Models for Cloud.....	4
1.4. Computing Architectures .....	5
1.5. Expected Benefits.....	7
1.6. Reduced Costs .....	8
1.7. Architectural Considerations .....	10
1.8. Information Classification .....	13
1.9. Security Fundamentals of Cloud Computing Software.....	15
1.10. Symmetric Encryption Algorithms .....	20
1.11. Advanced Encryption Standard (AES) .....	20
1.12. Asymmetric Encryption Algorithms .....	23
1.13. Confidentiality, Integrity, and Availability (CIA) .....	24
1.14. Cloud Security Services .....	26
1.15. Conclusion .....	27
References.....	29
<b>Chapter 2 Risks Issues and Security Challenges in Cloud Computing</b> .....	<b>31</b>
2.1. Introduction.....	32
2.2. What Is Cloud Computing? .....	33
2.3. Cloud Computing Risks and Challenges in Businesses .....	35
2.4. Standardization Activities in Cloud Computing.....	42

2.5. Vulnerabilities and Threats .....	46
2.6. Strategies to Mitigate Cloud Risk.....	54
2.7. Conclusion .....	58
References .....	59
<b>Chapter 3    Application Safety and Service Vulnerability in Cloud Network .....</b>	<b>63</b>
3.1. Introduction.....	64
3.2. Cloud Application Security in Different Cloud Services.....	65
3.3. Top Cloud Application Security Threats .....	71
3.4. What Cloud Application Security Options Are Available?.....	76
3.5. Who Is In Charge of Cloud Application Security?.....	77
3.6. Essential Characteristics of Cloud Network .....	79
3.7. Cloud-Specific Vulnerabilities .....	80
3.8. The Best Defense in Cloud Network Safety .....	92
3.9. Privacy-Preservation for Sensitive Data in Cloud Computing.....	94
3.10. Conclusion .....	97
References .....	99
<b>Chapter 4    Introduction to Internet of Things (IoT) Security and                   Its Open Challenges .....</b>	<b>101</b>
4.1. Introduction.....	102
4.2. What is IoT ?.....	103
4.3. Security Role in the IoT Development.....	105
4.4. IoT Architecture.....	107
4.5. The Importance of IoT Security .....	108
4.6. Essential Focus Areas for IoT Security.....	109
4.7. How to Ensure Your IoT System is Secure? .....	112
4.8. Trust, Data Confidentiality, and Privacy In IoT .....	113
4.9. Biggest Security Challenges for IoT .....	118
4.10. Future of IoT .....	123
4.11. Conclusion .....	126
References .....	127
<b>Chapter 5    IoT Architecture Security .....</b>	<b>131</b>
5.1. Introduction.....	132
5.2. IoT Architecture.....	134

5.3. IoT Security Threats, Impacts, and Challenges.....	138
5.4. IoT Ecosystems Are Difficult to Monitor and Manage.....	144
5.5. IoT Ecosystems Can Be Inherently Insecure.....	144
5.6. IoT Standards and Regulations are Obscure .....	145
5.7. Security in IOT.....	146
5.8. Security Features At Various Layer of IoT .....	147
5.9. Software Defined Networks (SDN) .....	148
5.10. SDN Based Architecture for IOT .....	152
5.11. Security Architecture Issues in the IOT .....	154
5.12. Insecure Access Control .....	155
5.13. Conclusion .....	157
References .....	158
<b>Chapter 6 Security in Enabling Technologies .....</b>	<b>159</b>
6.1. Introduction.....	160
6.2. Application of Tracking Technology.....	160
6.3. High-Reliability System Configuration .....	163
6.4. Privacy Concerns for 6LoWPAN .....	165
6.5. Security Concerns For 6LoWPAN.....	165
6.6. Challenges in Fog Computing .....	167
6.7. Temporary Stateless Addresses Auto-Configuration.....	169
6.8. Discussion of Security Framework for SDN.....	172
6.9. Conclusion .....	173
References .....	174
<b>Chapter 7 Introduction to Social Network and Its Security Issues .....</b>	<b>175</b>
7.1. Introduction.....	176
7.2. Social Networking .....	177
7.3. Historical Development of Social Networking Sites .....	179
7.4. Types of Social Networks .....	181
7.5. Popular Social Websites.....	183
7.6. Applications .....	185
7.7. Impact of Social Networks on Society .....	188
7.8. Some Security Issues In Social Network .....	190
7.9. National Security Issues .....	195
7.10. Recommendations and Countermeasures .....	197

7.11. Conclusion .....	202
References .....	203
<b>Chapter 8 Cyberspace Security in Digital Age .....</b>	<b>205</b>
8.1. The Start of Cybersecurity .....	206
8.2. Importance of Cyber Security in the Digital World? .....	208
8.3. Why Cyber Security is Critical for Companies? .....	208
8.4. The Importance of Cybersecurity In Digital Transformation .....	209
8.5. Why is Cybersecurity Lagging In Digital Transformation? .....	211
8.6. How Can Cybersecurity Ensure Successful Digital Transformation?.....	214
8.7. Overcoming Paralysis by Analysis When it Comes to Cyber Risk and Cyber Security .....	216
8.8. Embedding Cybersecurity Into Digital Transformation .....	217
8.9. Security in the Digital Age .....	218
8.10. Cybersecurity Best Practices .....	220
8.11. Cybersecurity's Dual Mission During the Coronavirus Crisis .....	222
8.12. Vulnerability Discovery Models (VDMS) .....	229
8.13. Conclusion .....	233
References .....	235
<b>Index .....</b>	<b>237</b>

# LIST OF FIGURES

---

- Figure 1.1.** Cloud computing environment.
- Figure 1.2.** Cloud deployment models.
- Figure 1.3.** Cloud security issues classification.
- Figure 1.4.** Example of an AES algorithm.
- Figure 1.5.** Authentication process.
- Figure 2.1.** Functioning of cloud computing.
- Figure 2.2.** Cloud computing security issues.
- Figure 2.3.** Maintaining cloud standard.
- Figure 2.4.** Threats in cloud computing.
- Figure 2.5.** Insider threat in cloud computing.
- Figure 2.6.** Strategies to mitigate cloud risk.
- Figure 2.7.** Data protection.
- Figure 2.8.** Using cloud cables to reduce risks.
- Figure 3.1.** Cloud application security.
- Figure 3.2.** Cloud security threats.
- Figure 3.3.** Cloud migration.
- Figure 3.4.** Cloud specific vulnerabilities.
- Figure 3.5.** Core-technology vulnerabilities.
- Figure 3.6.** Cloud web application.
- Figure 3.7.** Analytics in cloud network.
- Figure 3.8.** Cloud computing privacy challenge.
- Figure 4.1.** Connected devices in IoT.
- Figure 4.2.** Importance of IoT.
- Figure 4.3.** IoT in smart home.
- Figure 4.4.** IoT security and privacy.
- Figure 4.5.** Future of IoT things.
- Figure 5.1.** Layers of the IoT architecture.

**Figure 5.2.** IoT threats with level of impact.

**Figure 5.3.** DDoS attack.

**Figure 5.4.** IoT device vulnerabilities.

**Figure 5.5.** SDN components.

**Figure 6.1.** RFID technology can be used to track and manage inventory, assets, or people.

**Figure 6.2.** Automated vehicle system technology hierarchy.

**Figure 6.3.** 6LoWPAN routing.

**Figure 7.1.** Social network.

**Figure 7.2.** Popular social websites.

**Figure 7.3.** Effect of social network on society.

**Figure 7.4.** National security issues.

**Figure 8.1.** Cybersecurity alert.

**Figure 8.2.** Ransomware attack.

**Figure 8.3.** Encryption process.

**Figure 8.4.** IP spoofing.

**Figure 8.5.** ARP cache poisoning.

# LIST OF TABLES

---

**Table 7.1.** Timeline of social network sites.





# LIST OF ABBREVIATIONS

---

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
Amazon EC2	Amazon Elastic Compute Cloud
API	Application Programming Interfaces
ARP	Address Resolution Protocol
ASE	Asymmetric Searchable Encryption
AWS	Amazon Web Services
BC	Business-Continuity
BI	Business Intelligence
CADF	Cloud Audit Data Federation
CAGR	Compound Annual Growth Rate
CASB	Cloud Access Security Broker
CASP	Cloud Application Security Platforms
CDMI	Cloud Data Management Interface
CERT	Computer Emergency Response Team
CGA	Cryptographically Generated Address
CIA	Confidentiality, Integrity, and Availability
CMWG	Cloud Management Working Group
COTS	Commercial Off the Shelf
DDoS	Distributed DoS
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster-Recovery
DTLS	Data Transport Layer Security
ECC	Elliptic Curve Cryptography
EDoS	Economic Denial of Sustainability
ETC	Electronic Toll Collection

FCA	Financial Conduct Authority
GCP (CE)	Google Cloud Platform Cloud Extension
HDD	Hard Disc Drive
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IAAA	Identity Management, Authorization, Authentication, and Auditing
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ID	Identification
IDS	Intrusion-Detection Systems
IID	Interface Identifier
IoT	Internet of Things
IP	Intellectual Property
IPS	Intrusion-Prevention Systems
IR	Incident-Response
ISACA	Information Systems Audit and Control Association
ISSS	Information Security Society Switzerland
ITU	International Telecommunication Union
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
LAN	Local Area Networks
M2M	Machine to Machine
MDR	Managed Detection and Response
MFA	Multifactor Authentication
MFLOPS	Million Floating-Point Operations Per Second
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NoT	Network of Things
OCC	Open Cloud Consortium
OPSE	Order Preserving Symmetric Encryption
OSA	Open Security Alliance
OVF	Open Virtualization Format
PaaS	Platform as a Service

PCI DSS	Payment Card Industry Data Security Standard
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Risk Analysis
RFID	Radio Frequency Identification
SaaS	Software as a Service
SANs	Storage Area Networks
SCPM	Standard Cloud Performance Measurement
SDLC	System Development Life Cycle
SDN	Software Defined Networks
SDOs	Standard Development Organizations
SIEM	Security-Information-and-Event-Management
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SNIA	Storage Networking Industry Association
SNSs	Social Networking Sites
SOA	Service-Oriented Architecture
SOC	Security Operations Center
SOX	Sarbanes-Oxley
SQL	Structured Query Language
SSE	Symmetric Searchable Encryption
TM	Tele Management
TPMs	Trusted Platform Modules
URL	Uniform Resource Locator
VDMs	Vulnerability Discovery Models
VM	Virtual Machines
VMEs	Virtual Machine Environments
WSAN	Wireless Sensor and Actuator Networks



# PREFACE

---

Currently, the world is facing rapid technological advancement in every field. Unarguably, the most affected area is digital technology. The use of digital devices has increased to a much greater extent in the last decade. In this book three major aspects of digital technology data, social media, cloud computing, and internet of things (IoT) are discussed.

This book thoroughly examines the issues and vulnerabilities of IoT services. Due to the low cost of cloud services, almost every organization is storing their data in the cloud. This causes a big chunk of users' personal data to be saved in the cloud, which can be a target for hackers who are always trying to get access to cloud storage.

Apart from that, IoT security and its open challenges have been thoroughly discussed in this book. We assume the readers have little previous knowledge of IoT and cloud computing. The first three chapters focus on the cloud and its security aspects. The encryption standards, such as AES and RSA algorithms, are considered in Chapter 1 to understand the working of encryption algorithms for securing data over the cloud. In Chapter 2 the basic definition of cloud computing is discussed along with risk issues and security challenges in cloud computing.

The vulnerabilities and threats associated with cloud computing are also discussed. Chapter 3 discusses the roles and responsibilities of the cloud service providers in terms of the security of the user's data. The major focus has been placed on the analytics and its importance for cloud security.

In Chapter 4 the IoT and its concepts are discussed along with the discussion of the threats and vulnerabilities of IoT. Specifically, cyber attacks taking place on IoT devices are becoming more prevalent and are increasing by up to 50% every year.

In Chapter 5 the IoT aspects of security, such as network access control and software verification, have been evaluated. In Chapter 6 embedded systems have been discussed along their security aspects.

Chapter 7 explores different types of social networks. Finally, in Chapter 8 various cybersecurity aspects are examined.

I hope that this book has the potential to be referred by the scholar for their work. It provides them with the up-to-date knowledge on security designs for cloud, IoT, and social networking.

## CHAPTER 1

# Cloud Computing Overview

## CONTENTS

1.1. Introduction.....	2
1.2. Cloud Computing Layers.....	3
1.3. Deployment Models for Cloud.....	4
1.4. Computing Architectures .....	5
1.5. Expected Benefits.....	7
1.6. Reduced Costs .....	8
1.7. Architectural Considerations .....	10
1.8. Information Classification .....	13
1.9. Security Fundamentals of Cloud Computing Software.....	15
1.10. Symmetric Encryption Algorithms .....	20
1.11. Advanced Encryption Standard (Aes).....	20
1.12. Asymmetric Encryption Algorithms .....	23
1.13. Confidentiality, Integrity, and Availability (Cia).....	24
1.14. Cloud Security Services .....	26
1.15. Conclusion .....	27
References.....	29

In this chapter the general concept of cloud computing will be discussed together with their security concerns. Different services provided by cloud computing and their benefits will also be discussed. Features of cloud computing discussed in the chapter include cloud computing adoption due to its speed, lower cost, productivity, global scale, performance, and security. Cloud computing reduces or eliminates the capital expense in terms of buying important software and hardware. Cloud services can be set up within a few minutes; and most of them are offered on demand. The encryption algorithms and its benefits are discussed in the middle of this chapter.

## 1.1. INTRODUCTION

Cloud computing can be defined as the delivery of computing services that consist of servers, databases, storage, software, and networking over the internet in order to provide resource flexibility as well as decreasing the operating cost for its users.

In addition, cloud computing is location independent because everything is easily accessible online. Optimized performance is achieved because the data centers contain efficient computing hardware. Below given are subsections that describe key features of cloud computing, different kinds of layers, and available deployment models.

### 1.1.1. Characteristics of Cloud Computing

Below are outlined five key characteristics of cloud computing:

- **On-Demand Self-Service:** An end-user can acquire the needed services automatically, without any need for human interaction with each service provider.
- **Broad Network Access:** Services are available all over the network and can be accessed through standard mechanisms that utilize thin and thick client platforms.
- **Resource Pooling:** Computing resources are selected across the variety of consumers using a multi-tenant model. Physical and virtual resources are dynamically assigned and reassigned based on the consumer demand. The consumer has very little knowledge regarding the location of resources. Some examples of resource information that may be available include storage, processing, memory, and network bandwidth.



- **Elasticity:** Depending on the user need or demand, resource allocation can be increased or decreased.
- **Measured Service:** Cloud systems control and optimize resource use automatically by leveraging a metering capability at certain level of abstraction suitable for the kind of service (for example, storage, processing, bandwidth, and active user accounts). Usage of resources is strictly monitored, controlled, and then reported in order to provide complete transparency to the consumer as well as provider.

## 1.2. CLOUD COMPUTING LAYERS

- **Infrastructure as a Service (IaaS):** IaaS is considered as an option that provides base infrastructure only. The end-user requires to configure and manage the platform and the environment, and eventually build all the needed applications on top of it. Examples include AWS (EC2), GCP (CE), and Microsoft Azure (VM).
- **Platform as a Service (PaaS):** PaaS is a model of cloud computing where software and hardware tools are usually delivered by a third-party provider. The user can build as well as manage different applications without suffering the hazards of building and maintaining the infrastructure. Examples of PaaS include Google App Engine, Cloud Foundry, Heroku, and AWS (Beanstalk), etc.

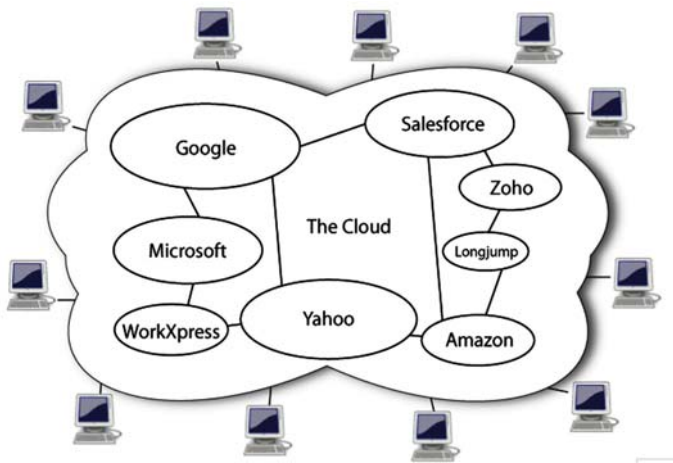
Simplicity and convenience for the users are the key benefits of PaaS. The reason behind this is that they can easily access the infrastructure from any location just through a web browser. Consequently, capital expenditure is reduced or removed to a high level, that is, usually needed in the business (Kruse, 2002).

Although, customers can face certain challenges or difficulties if the providers experience any kind of service outage or disruption of infrastructure.

- **Software as a Service (SaaS):** SaaS model traditionally allows providing software applications as a kind of service to the users. In general, it refers to the notion of “software availability based on demand.” Usually, users access it via a thin client through a web browser.

Some of the key features of SaaS comprise availability of software over the net, maintenance of the software by the vendors, subscription-based software licensing, centralized feature updating that mandates the user to download patches and upgrades (Halder, 2011).

Most of the services such as applications, middleware, data, servers, networking, and storage in this model are maintained as well as managed by the vendors; and only users can use it. The common example of this model is Gmail (Figure 1.1).



**Figure 1.1.** *Cloud computing environment.*

Source: Image by Wikimedia Commons.

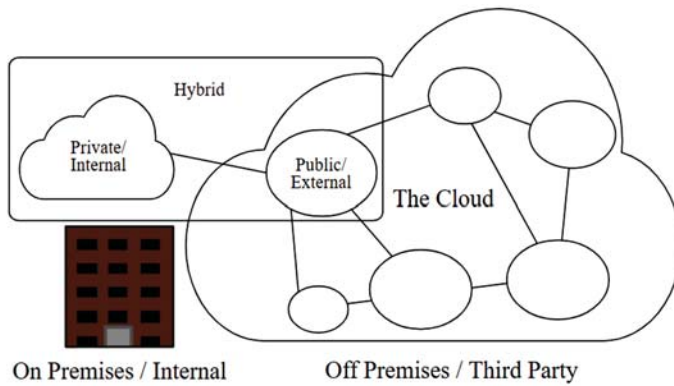
### 1.3. DEPLOYMENT MODELS FOR CLOUD

There are three deployment models that are generally used all around the world. The appropriate model must be selected depending on the need of an organization:

- **Private Cloud:** A private cloud includes resources that are wholly available to a particular organization. The data center can be situated onsite or can be managed by a third party service provider. As a result, all services as well as infrastructure are maintained in a private network.
- **Public Cloud:** A public cloud is traditionally owned and maintained by the cloud service providers of third party, where

all of the resources are available to multiple stakeholders or organizations. The service providers provide important access to the services depending upon the account created by the users. The users then pay the cost depending on the services they use.

- **Hybrid Cloud:** Hybrid cloud merges other two types-public and private-by using the technique that allow data as well as applications to be shared between them. The business gets greater flexibility, more deployment options, enhancement in existing infrastructure, compliance, and security by permitting the movement of data as well as applications between public and private clouds (Figure 1.2).



**Figure 1.2.** *Cloud deployment models.*

Source: Image by Wikimedia Commons.

## 1.4. COMPUTING ARCHITECTURES

Based on the work of Hower and Uradnik (2011), cloud computing adoption was affected by architectural developments, such as advances in high-performance computing and parallelism advances. Certain principal architectural developments that provide support to cloud computing are further summarized below.

### 1.4.1. High-Performance Computing

Due to the availability of high-performance computers, cloud computing is always evolving. The evolution characterizes certain kinds of cloud

computing applications that are practical to run due to the availability of high-performance computers (Matusitz, 2005). Computers play a major role in cloud computing and some of the key milestones in their developments are discussed in further sections.

In 1960s, the computers known as supercomputers were developed. In 1961 IBM developed the IBM 7030 “Stretch”, which was the first transistor-based supercomputer.

It was developed for Los Alamos National Laboratory and was able to perform at 1.2 MFLOPS (million floating-point operations per second). Here, it is also worth mentioning Seymour Cray, who is credited with developing the first “real” supercomputers.

According to Gupta and Adat (2017), the developments in supercomputing technology increased during the next three decades with a range of products. An exciting milestone along with the path of supercomputer development was the concept or idea of connecting low cost, commercially available personal computers in a network cluster to form a high-performance computing system.

This idea was formulated in 1993 as the Beowulf computing cluster concept. This was developed by Thomas Sterling and Donald Becker of NASA. Beowulf uses open-source operating systems, such as Solaris or Linux.

One of the key characteristics of Beowulf is that all the connected machines seem as a powerful, single resource to the user. The first prototype in the Beowulf project used 16 Intel DX4 processors connected by 10 Mbit/second Ethernet.

The DX4 processor is an Intel chip with triple clocking. As the DX4 processor speed was great for a single Ethernet bus, a “channel-bonded” Ethernet was developed by distributing the communications across two or more Ethernet buses.

This approach is no longer important with the beginning of Gigabit Ethernet. The primary cluster demonstrated the ability of COTS (commercial off the shelf) products to execute high-performance computing systems.

### **1.4.2. Autonomic Computing**

The cumulative complexity and connectivity of the computing resources are highly needed to execute a cloud call for an innovative mechanism to operate, manage, and maintain the infrastructure of the cloud. Autonomic

computing is one of the ways that holds a good promise in aiding to meet the major expectations of cloud computing (Jouini and Rabai, 2016).

IBM developed the notion of autonomic computing. On their website of autonomic computing, they describe it as “an approach to self-managed computing systems with a minimum of human interference. As per Yaqoob et al. (2019), the term derives from the body’s autonomic nervous system, which controls key functions without conscious awareness or involvement.” The major aim of autonomic computing is to provide complex, heterogeneous systems with self-diagnosis, self-healing, and self-optimizing capabilities Dorsemayne et al. (2015).

## 1.5. EXPECTED BENEFITS

Cloud computing has numerous benefits, but some accompanying caveats also. Similar to the case of any physical system, cloud computation should work or operate within the parameters of that physical boundary. The cloud provides the ability to provision a huge amount of computing power as well as storage, but such qualities are finite (Nayyar, 2019).

As a result, the cloud users might have to adjust their applications into one set of the resources usage categories that are defined by the cloud provider. The cloud computational resources can be further scaled up and scaled down on demand and can be paid for on the basis of meter usage (Moustafa et al., 2015).

This specific ability eventually offers significant benefits for end clients because they don’t have to maintain their internal computing systems. In addition, the cloud paradigm supports the innovation in that a large variety of new and advanced applications can be utilized in an affordable way while decreasing the total cost of ownership (Nasrin and Radcliffe, 2014).

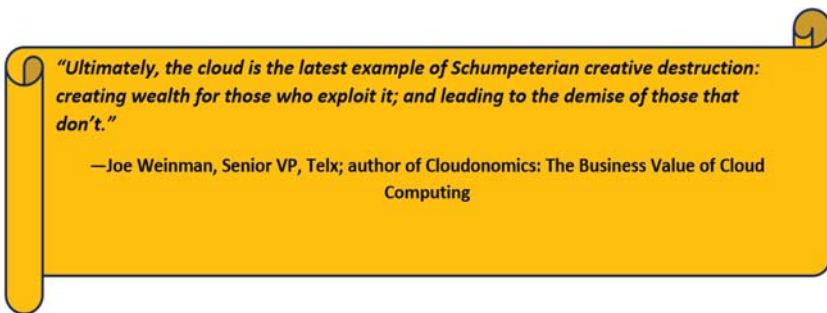
Silva (2014) argues that some of the applications are of quite long duration and have constant computational requirements might be served better by in-house or leased computers and storage than by paying the cloud fees over a long period of time. Such options have to be assessed on a case-by-case basis.

Key benefits of cloud computing include:

- Being able to move to an operational expenditure environment;
- Being able to organize innovative business and research applications rapidly and cost efficiently;

- Being able to use virtualization to detach business services from the underlying execution infrastructure;
- Being able to utilize disaster recovery and business continuity capabilities that are intrinsic in the cloud paradigm;
- Being able to apply security safeguards centrally, effectively, and efficiently;
- Being able to select cloud suppliers that offer reliable scalable services, metered billing, and advanced development resources;
- of cloud suppliers to build scalable infrastructure that can provide and re-allocate significant resources on an as-needed basis.

The key benefits of the cloud paradigm can further be distilled based on its intrinsic resiliency, flexibility, and availability of large amount of centralized data storage (Dunlap, 2002).



## 1.6. REDUCED COSTS

In general, the cloud paradigm offers significant cost savings because cloud resources can be paid for without any large investments in the computing infrastructure. As a result, capital costs are reduced and replaced by scalable, manageable operating expenses. On the other hand, there might be some conditions, where cloud computation might not have the advantage of cost overusing internal resources or directly leasing equipment (Jaeger, 2008). For instance, if the total volume of data storage and computational resources needed are basically constant and there is no actual need for rapid provisioning and flexibility, then the local computational capabilities of an organization might be more cost-effective as compared to using a cloud (Lamb, 2009).

There is another factor to consider while choosing the cloud. The factor is that the client organizational support as well as maintenance costs are

reduced dramatically as such expenses are transferred to the cloud provider, comprising 24/7 support. Also, the need for highly trained and expensive IT personnel is reduced (Payne, 2008).

In cloud computing, the resources are used in a more efficient manner. This eventually results in significant support and energy cost savings. As per IDC Worldwide and Regional Server 2009–2013 Forecast, expenses of server administration are now the largest data center costs and have approximately increased by 400% in the past 15 years.

Another consideration is energy costs in moving to the cloud. 1E, a London-based consulting organization that aids clients in reducing the IT operational costs, published a survey that found approximately 4.7 million servers all around the world are idle most of the time and are wasting \$25 billion per year in energy costs (Perry, 2008).

In addition, they also found that, usually organizations spend twice as much on the server energy costs as on the hardware. Cloud computing provides an alternative to such expenses. Generally, cloud computing provides a reduction in energy costs, system administration, provisioning expenses, hardware costs, software licensing fees, and hardware costs (Schwartz and Ephraim, 2008).

With all the benefits of the cloud paradigm as well as its potential for reducing the costs and decreasing the time needed to initiate new initiatives, cloud security will always be a key concern. Geographically dispersed servers, virtualized resources, and co-location of storage and processing impose opportunities and challenges for the users and cloud providers both (Theilmann and Baresi, 2009). The security posture of a cloud system is completely based on its security architecture.

As there is no standard definition for security architecture, according to the open security alliance (OSA), security architecture is “the design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes, among them confidentiality, integrity, availability, accountability, and assurance.”

Another definition given by the Information Security Society Switzerland (ISSS) describes a security architecture as “a cohesive security design, which addresses the requirements (e.g., authentication, authorization, etc.), and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process should be reproducible.”

In further sections, the general issues of security architecture involved in cloud computing, the architectural components of trusted cloud computing, core security architectural functions, and the potential of autonomic systems to execute secure architectures will be discussed.

## **1.7. ARCHITECTURAL CONSIDERATIONS**

A large number of factors affect the performance and execution of the cloud security architecture. There are general issues or problems such as regulatory requirements, security management, adherence to standards, information classification, and security awareness.

In addition, there are more specific architecturally linked areas, consisting of trusted software and hardware, providing for a safe and secure implementation environment, executing secure communications and hardware augmentation via microarchitectures.

### **1.7.1. General Issues**

Numerous aspects, such as security management, compliance, controls, administrative issues, and security awareness, impact the architecture of cloud security. Compliance with legal regulations must be supported by the cloud security architecture.

Consequently, the cloud security policy must address the classification of information, what kind of entities can actually access the information, under what kind of conditions the access needs to be provided, the geographical jurisdiction of the data stores, and whether or not the access is apt.

Proper controls should be verified and determined by using assurance methods, and effective personnel awareness education must be put in place. Compliance in a public cloud environment, the provider does not usually inform the clients of the storage location of their data.

Actually, the distribution of processing as well as data storage is one of the basic features of cloud. Although, the cloud provider should cooperate to consider the data location requirements of the client.

Also, the cloud vendor should provide clear transparency to the client by giving accurate information about storage used, processing features along with other relevant account information. Another major compliance issue is the accessibility of the data of the client by the system of provider.



This factor is an important part of providing as well as maintaining cloud services, however the act of getting sensitive information must always be monitored, controlled, and then protected by the safeguards, for example, the separation of duties.

In such situations where information is stored in a foreign jurisdiction, the capability of local law enforcement agencies to easily access a client's sensitive data is a major concern. For instance, such a scenario might happen when a government entity performs a computer forensics investigation of a cloud provider under the suspicion of some kind of illegal activity.

The claim of cloud provider for data protection and compliance should be backed up by relevant logging, certifications, and auditing. Particularly, at a minimum, a cloud provider should undergo a Statement on Auditing Standard # 70 (SAS 70) "Service Organizations" Type II Audit.

Such audits assess the internal controls of a service organization to determine whether accepted best practices are being applied for protecting the client information. Cloud vendors are needed to undergo subsequent audits to retain their SAS 70 Type II Audit certification.

A related issue is the management policy linked with the data stored in the cloud. When the engagement of the client with the cloud provider is terminated, a compliance and privacy requirements have to be considered.

In certain cases, information has to be preserved as per the regulatory requirements, and in some situations, the provider must not hold a client's data in primary or backup storage if the client feels that it has been destroyed.

If stored in a foreign jurisdiction, the data might be subject to the privacy laws of the country and not the laws applicable in the geographic location of the client.

The application and evolution of appropriate cloud standards focused on the legal requirements will serve to meet the compliance requirements of the client and provide the effective protection. A great number of standards organizations have joined the forces under the title "Cloud Standards Coordination Working Group" so as to develop a cloud computing standardization approach.

The working group comprises the object management group, the distributed management task force, the tele management (TM) Forum, the Organization for the Advancement of Structured Information Standards, the Open Grid Forum, the Cloud Security Alliance, the open cloud Consortium

(OCC), the Storage and Network Industry Association, and the Cloud Computing Interoperability Forum.

### 1.7.2. Security Management

Security architecture involves operative security management to realize the advantages of cloud computation. Proper cloud security management as well as administration should recognize management issues in some of the critical areas like vulnerability analysis, access control, change control, fault tolerance, change control, continuity planning and disaster recovery. These areas are further enhanced and supported by the application and verification of cloud security controls.

### 1.7.3. Controls

The key aim of cloud security controls is to decrease the vulnerabilities to such a level that they can be tolerated and reduce the effects of any attack. To attain this, an organization determines what impact an attack might have, and the probability of loss.

Certain examples of losses are the compromise of sensitive information, loss of reputation, financial embezzlement, and also, the physical destruction of resources. The process of assessing different threat scenarios and producing a representative value for the approximated potential loss is basically known as risk analysis (RA).

In terms of vulnerabilities, there exist four major types of controls:

- **Deterrent Controls:** These reduce the chances of a deliberate attack.
- **Preventative Controls:** These protect the vulnerabilities and make an attack ineffective or reduce its impact. Preventative controls constrain attempts to violate the security policy.
- **Corrective Controls:** These reduce the effect of an attack.
- **Detective Controls:** These discover attacks and activate preventative or corrective controls. Detective controls warn of violations or endeavored violations of security policy and comprise controls such as intrusion detection systems, video cameras, organizational policies, and motion detectors.

Cloud security management fosters enhanced abilities to perform forensic analysis on cloud-based information by using a network forensic model. This model provides more rapid acquisition as well as verification of

the evidence like taking good advantage of automatic hashing. In general, automatic hashtag is applied when storing data on a cloud.

Cloud security management can be improved by the selective application of automation and also by the use of emerging cloud management standards to certain areas such as interoperable security mechanisms, accounting, quality of service, provisioning, and API specifications.

APIs provide for control of the cloud resources by program interfaces, and remote APIs need to be managed in order to assure that they are consistent and documented. Cloud security management addresses specific applications with the aim of enterprise cost containment by scalability, pay as you go models, on-demand implementation and provisioning, and re-allocation of information management operational activities to the cloud.

## **1.8. INFORMATION CLASSIFICATION**

Another key area that links to the compliance and can impact the cloud security architecture is considered as information classification. The process of information classification supports the disaster recovery planning as well as business continuity planning.

### **1.8.1. Objectives of Information Classification**

There are various reasons to classify information. Not all of data has the same value to an organization. For instance, some data is much more valuable to the upper management, as it helps in making strategic short-range or long-range business direction decisions.

Certain data such as trade secrets, formulas, and new product information, is so valued that its loss could create a major problem for the enterprise in the marketplace, either by developing public embarrassment or by causing a credibility of lack.

As a result, it is clear that the classification of information has a higher benefit at the enterprise level. Information stored in a cloud environment has a major impact on the entire business. The main goal should be to improve confidentiality, availability, and integrity. Additionally, by directing the protection mechanisms and controls on the areas of information areas that most need it, you attain a more effective cost-to-benefit ratio.

In the governmental sector, information classification is incredibly important for establishing trusted systems. Information classification is used mainly to prevent the unauthorized disclosure of information and subsequent

failure of confidentiality. The information classification supports privacy requirements and regulatory compliance.

In the private sector, a business might want to utilize information classification to sustain a competitive edge. In addition to that, there might be comprehensive legal reasons for an organization to engage in the information classification on the cloud, such as decreasing the liability or securing valuable business information.

### 1.8.2. Benefits of Information Classification

Employing information classification offers a multitude of benefits for an organization which is involved in cloud computing:

- Information classification demonstrates the commitment of an organization to security protections.
- Information classification helps in identifying which information is the most vital or sensitive to an organization.
- Information classification supports the tenets of integrity, confidentiality, and availability as it pertains to data.
- Information classification helps in identifying which security measures apply to which information.
- Information classification might be required for regulatory, compliance, or legal reasons.

### 1.8.3. Concepts of Information Classification

Generally, information is classified based on the sensitivity of an organization to information loss or disclosure. The owner of the information system is responsible for defining the level of sensitivity of the data. Classification enables the security controls to be implemented in an accurate way. Below are some of the classification terms that are generally used in the private sector:

- **Public Data:** The information similar to the unclassified information. Each piece of information that does not fit into any of the other categories are considered to be public. Although its unauthorized disclosure may be against policy, it is not expected to seriously impact the organization, its employees, or its customers.
- **Sensitive Data:** This information that needs special precautions in order to ensure its integrity by safeguarding it from unauthorized

deletion or moderation. In general, it is information that requires higher-than-normal assurance of accuracy and completeness.

- **Private Data:** This information is intended for use within a specific organization. The unauthorized disclosure could adversely or severely impact the organization as well as its employees. For an instance, salary information or health care information is considered to be private.
- **Confidential Data:** This is the most sensitive business information which is strictly intended to use within the organization. Its unauthorized disclosure could adversely and seriously impact the organization, its business partners, its stockholders, or its customers. This information is relieved from the disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. For instance, information regarding new product development, trade secrets, and merger negotiations is considered confidential.

## 1.9. SECURITY FUNDAMENTALS OF CLOUD COMPUTING SOFTWARE

Since most of the organizations are now migrating to cloud platforms to store their data, they have to be extremely cautious about their security concerns. Most of the data that is stored on remote cloud storage systems is personal user data. Losing user's personal data reduces the market value of the organization and, as a result, security needs to be a high priority for every cloud service provider. Additionally, data stored on remote cloud storage systems is likely not stored in a single data center or a single geographical region.

During the software development life cycle, certain design aspects need to be considered in order to reduce the risk of data breach or cloud attack. These aspects include:

- **Information Life Cycle Management:** Here, we need to understand cloud provider policies as they pertain to data retention and whether these policies are in line with the internal organizational policy. It is important that the organization performs regular backups and tests the logical segregation so that the effectiveness of these controls can be assured.

- **Application Security:** Here, different cloud services of cloud, such as IaaS, PaaS, and SaaS, play important roles since their trust boundaries are different during each software development life stage, such as development, production, and testing of the application.
- **Cloud Storage Security:** Security in terms of storage for cloud applications is very important. In case of any accidental data stealing or deletion, the cloud provider should store a backup copy of the same data records on other servers.

It is also important that cloud providers establish similar security procedures at every data center in which they store the data from the same organizations.

Since a cloud computing provider is essentially an SaaS platform, they face a critical issue in terms of software security. They need to ensure that all of their software is up-to-date regarding latest bug patches, encryption protection measures, and security features. As a result, a cloud customer using SaaS services does not need to worry about cloud security because it is the responsibility of the cloud provider.

Designing security measures for cloud services is a critical task and involves various processes such as designing, testing the system, deploying the system securely, patch management, and disposal. All these processes need to be implemented by the software developer who is responsible for developing the cloud platform.

All the security requirements need to be fulfilled so that the cloud system is secure. Being an integral part of the cloud environment, the software security is considered a core feature in the software development process.

### 1.9.1. Cloud Information Security Objectives

Secure software development is dependent on applying software design principles that are secure and work on the basis of software assurance. Software assurance is defined in the context of the software development. Hence it is very important to understand the basic concept of the cloud platform.

The common definition for software square security assurance is that the software will continuously, at least with the properties that have been provided the software will continuously activate the properties that have

been provided for the software developer to the software developer and it will work and operate without encountering any intentional faults.

That means in the event of any attack the software must have the capability to register from most of the attacks, if it is not capable of resisting the attack then it must tolerate as many attacks as possible and recover to a normal level of operation quickly in the event when the attacks are a registrable or intolerable by the security system of the software.

In other terms software assurance is the confidence level in software functionalities that they will perform as intended and will be free from vulnerabilities that have been inserted intentionally or intentionally at the software development level.

In order for the software to be considered secure these three properties are must for them to exhibit such as:

- **Dependability:** It is defined as for a software that has the capability to be able to operate correctly in various conditions, including when the system is under attack or it is controlled by a malicious host.
- **Trustworthiness:** This property is executed by the software air that is found to have lesser vulnerabilities or it is not incorporated with any weakness at all that affects the dependability of the software.
- **Survivability (Resilience):** Software must have the capability to resist if not tolerate as many attacks as possible and should have the capability to recover from these attacks as well without causing much harm to the system.

### 1.9.2. Data Security in Cloud Storage

Cloud storage is one of the more convenient Technologies that have been developed over time and allows the users to access their data irrespective of their geographical position or time. One of the major benefits of cloud storage is that the business organization now does not have to worry about their organizational data since the IT overhead has been decreased for the organization with the help of cloud storage.

Apart from scalability and accessibility, this benefit of reduced IT overhead has been the major cause of technology adoption by the business organization at a rapid rate. So, this leads to a major focus over these technologies in terms of the data stored over cloud storage being safe.

Several enterprises have shifted to cloud storage for their data storage functions since it has reduced their cost for implementing local hardware and also reduced the cost of area required for that hardware. But as there are two sides of a coin so the other side of this coin is that the data stored over cloud storage is at risk of being stolen or getting damaged at all times. While choosing the cloud provider, it is very important for the enterprises to look at their security procedures and their previous clients. If the organization thinks the data needs to be secured at all entry levels so, but it is not necessary, they implement security protocols at their levels as well in addition to the security protocols followed by the cloud service provider.

The primary Protection Scheme includes basic encryption techniques being implemented, access control author authentication.

### **1.9.3. Security Issues in Cloud**

In the case of cloud infrastructure, data security becomes a prominent challenge which is a common concern in any other technology. This is because the cloud is supposed to store user's personal data, and hence additional data security protocols are required by the cloud system to be implemented in order to secure the data stored in the cloud.

Security concerns for the cloud are related to risk areas such as lack of control, external data storage, integration with internal security, multi-tenancy, and the dependency on the public internet. The sensitive data stored on cloud storage systems are secure due to various encryption algorithms. Since encryption techniques are not easily compromised, the sender and receiver are the only parties responsible for the encryption or decryption of the data (Theilmann et al., 2008).

All this process of encrypted data transfer and the data being deported again works when both the parties have the key to decrypt the data. Thus, anyone with the key can get access to the data transferred. This however is merely an assumption that the encryption techniques or Encryption Algorithm implemented are strong and has the capability to secure the data saved over cloud storage.

All over the world there are a few common security issues that most of the organization face while working in the cloud environment and these issues can be overcome with the help of appropriate security algorithms deployment.

In most of the organizations around the world, the resources are shared within the organizations and in some cases with other companies as well. This

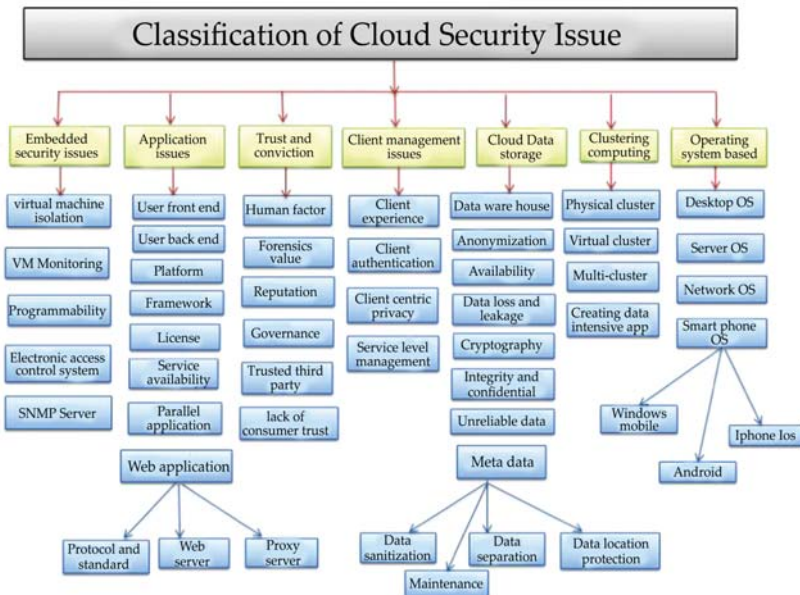


causes loss in physical security while working in the cloud environment this is because when the resources are running, then there is no control over who can access what data when the resources are shared among the organizations (Al Ameen et al., 2012).

Functions such as data storage, data transfer, and data retrieval are performed on the data present in the cloud at all times, and hence it becomes a major issue in terms of data integrity. Now, these transactions are often performed with proper security measures, and only authorized people can make these transactions; however if in a case of unauthorized transaction, it can be a major threat to the organization's data.

That is why applying appropriate security algorithms are a way to ensure that the data transmission performing within the organization or among the organization are secured.

It is also a major threat that the cloud service provider can share the sensitive data of users or organizations with an intended receiver without the knowledge of the owner of the data. Also, security issues can arise if the keys for encryption or description of data are not managed properly (Figure 1.3).



**Figure 1.3.** Cloud security issues classification.

Source: Image by Wikimedia Commons.

## 1.10. SYMMETRIC ENCRYPTION ALGORITHMS

The major purpose of symmetric encryption algorithms is that these are used primarily for bulk data encryption. This data encryption technique is considered to be fast and has various possible keys. The secrecy provided by these algorithms is top-notch.

The disadvantage or the drawback associated with this technique is that it consumes more time while decrypting the data, so the same key is required for the decryption of data which was used for data encryption. These algorithm techniques are classified into two categories that are stream and block.

As the name suggests block algorithm encrypts the data block-wise while the stream algorithm encrypts the data byte by byte. The strength of these encryption techniques is dependent on the area over which the encryption techniques are used; that means they have expertise in specific areas, and hence both these techniques are of utmost importance.

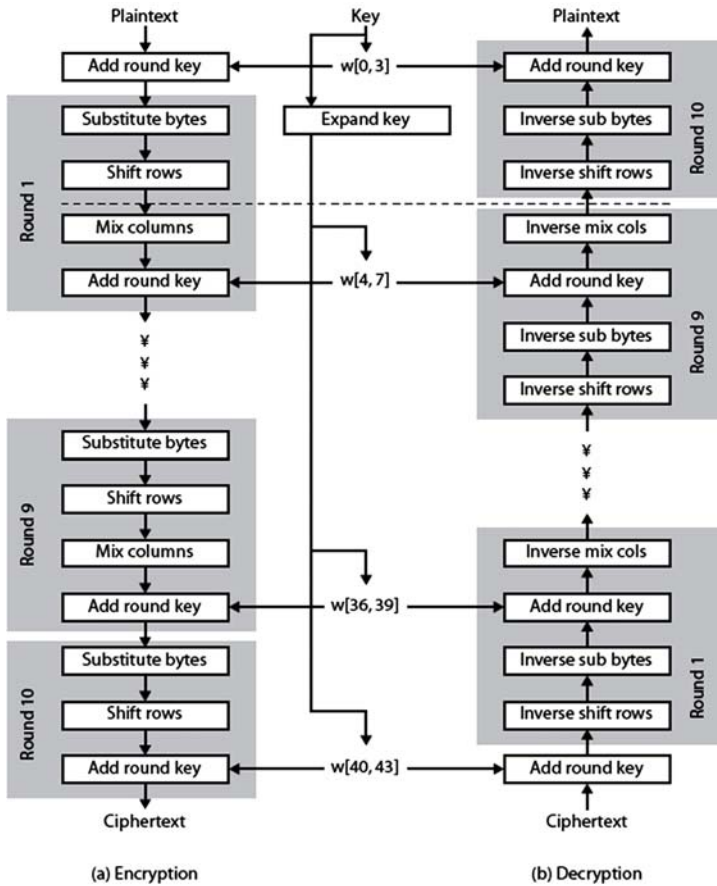
This can be further understood from the fact that some of these encryption techniques are not efficient enough in protecting the data since they allow the decryption process without considering the requisite key and some of these encryption techniques are very much competent in order to resist the obvious attacks.

## 1.11. ADVANCED ENCRYPTION STANDARD (AES)

In order to protect user's data from external attacks, cryptography is considered to be the most desired and notable technique that uses two different processes. These processes involved in cryptography technique are encryption and decryption. Encryption is the process in which the data is converted into some sort of code so that the attackers cannot read what the original data is conveying (Dohr et al., 2010).

This process involves converting plain text into a format that is unreadable or not make sense, this converted format is called ciphertext. This allows the sender of the data or message to send it to the desired receiver more securely. Since the attacker cannot understand what the data means.

The next process of cryptography that is decryption is performed at the receiver's end, where with the help of related keys, the encrypted text is converted to original data. For the future IT applications, the cloud computing is considered to be an emerging technology and has a promising future (Figure 1.4).



**Figure 1.4.** Example of AES algorithm.

Source: Image by Wikimedia Commons.

However, data security and privacy issues are considered to be major hurdles that prevent cloud computing from being adopted more rapidly. Using processes, such as encryption and decryption, can be a way to secure the data against external attacks over cloud storage.

Here, the advanced encryption standard (AES) encryption technique are discussed. The AES algorithm is easy to implement, provides flexibility, and requires less memory space than the blowfish algorithm. There are various attacks, such as differential attack, key recovery attack, key attack, and square attack (Lim et al., 2010), which the AES encryption technique protects against.

There is one more reason as to why the AES encryption technique is considered to be highly secure. It has the ability to provide protection against future attacks, such as smash attacks. The reason is that this AES encryption technique requires minimum space of storage and its implementation is very smooth with no limitations.

### **1.11.1. Existing System**

There are various security issues that have been identified for data storage in the cloud. There are various security issues related to cloud computing, such as identity management, leakage, internal threats, multi-tenancy, information loss and cloud accessibility, etc.

Since the cloud has various users and implementing security measures to such a large number of users is not an easy process. This is due to the fact that uses of cloud services have different security concerns as per their use of cloud services. But still, there are some general security measures that the cloud service providers implement in terms of ensuring the security of the users' data.

They make sure that in the event of any cyber-attack, their system is capable of resisting such attacks, and if for some environmental reasons the data is damaged, then it is the duty of the cloud service provider to store duplicate data at some other location with similar security implementations.

In the last few years there has been an extreme surge in the number of cloud users and the main reason for that is that it reduces the cost for organizations to store their data locally as they can pay a fee to store their data at some cloud service providers such as Amazon web services (AWS).

However, there are various security concerns related to storing and trusting any Cloud Service Provider over an organization's user's personal data, so there are some mandatory regulations that have been implemented over the cloud service providers that makes them responsible for any type of security concerns causing loss to the business organization.

### **1.11.2. Architecture**

AES performance is dependent on the hardware and software needs of the platform where these techniques are used in different spectrum of environments. Two different platforms that are used are 8 bit and 64 bits.

The software performance has improved efficiency due to the in there and parallelism in the use of processor resources. This algorithm is very

much suitable for environments with restricted space, and it has advantages in terms of memory allocation for the implementation purpose.

It is identified in the AES technique are not weak, that means even when an attacker gets access to the cryptographic keys still, they won't be able to gather the original data. The block sizes and key sizes over 128 bits are supported by this algorithm.

Even when huge test cases are used till the statistical analysis is not possible for the ciphertext. Thus, any linear or differential cryptanalysis attack has not been proved on the AES technique.

## **1.12. ASYMMETRIC ENCRYPTION ALGORITHMS**

Cloud Computing services are on demand services as these services can be used by paying a fee. In the cloud computing paradigm, various users share resources in terms of storage and service for their data, and hence they pay for the services such as storage and resources used.

On the basis of user requirements, there are three categories of cloud services such as SaaS, PaaS, and IaaS. SaaS or Software as a service provides an environment of cloud services that can be accessed via the Internet. But in order to use this service, the user gets a proper license from their Cloud Service Provider (Medaglia and Serbanati, 2010).

PaaS or platform as a service in which the user gets access to the platform in order to develop their application and IaaS or infrastructure as a service in which the user gets access to resources like operating systems, storage devices, and servers. The major aim of the IaaS is not more than the physical maintenance.

Although Cloud Computing provides various such services that have varied and vast users that get Cloud Computing services for their own purposes such as some may use it for just storing their data or for some users may get Cloud Computing services for the development of some applications.

Thus, providing various services to a large number of users need proper maintenance of the system and its resources as it is shared among so many people. Now, in this case, when a resource is shared among various users, there are some security issues that are bound to occur, which may be intentional or unintentional.

Since the cloud holds the most sensitive information so it is the duty of the cloud provider that they offer high profiled security. In order to enhance the security of data over cloud mechanisms such as authentication processes have been deployed so that the system can become more secured.

One such form of authentication mechanism is cryptography that allows users to send or receive their personal data in the form of ciphertext that cannot be deciphered without proper keys. The cryptography technique protects sensitive user data by delivering robust access controls and without any delay in the information exchange.

In cryptography, surety of data security is done with the help of Encryption Algorithm categories that are public-key cryptography and secret-key cryptography. In symmetric encryption, only a single key is used for encryption as well as decryption processes. When two different keys are used for encryption and another key for decryption in the public key Cryptography than this encryption method is called a symmetric encryption.

### 1.13. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)

The CIA triad of information system security is known as confidentiality, integrity, and availability, and these are considered to be important pillars of cloud software.

#### 1.13.1. Confidentiality

In the confidentiality aspect of cloud computing the prevention is ensured over unauthorized disclosure of information, whether intentional or unintentional. The aspects related to confidentiality in cloud systems are in the areas of:

- **Intellectual Property (IP) Rights:** IP means literary works, musical, and artistic works, designs, and inventions. The IP rights are taken care of by the copyright laws that ensure that no copyright infringement takes place in terms of patents for new inventions.
- **Covert Channels:** This is a communication path that is unintended and authorized at the same time and has the ability to enable information exchange. In order to accomplish covert channels, message timings are used, and use of inappropriate storage mechanisms takes place.

- **Traffic Analysis:** It is a type of confidentiality breach in which destination of message traffic, source, rate, and volume of the message traffic is analyzed even when the message is in encrypted form. This traffic analysis indicates the occurrence of some major event when a burst of traffic is found and the message activity increases.
- **Encryption:** It makes sure that even if the message is intercepted, it is unreadable by the attacker for any unauthorized entity. In order to decrease the message sent via encryption technique depends on encryption key strength and the quality and robustness of the algorithm used (Tsiftes and Dunkels, 2011).
- **Inference:** It is associated with database security. In this, an entity gathers the ability to correlate information that is secured at it only one level so that on a higher security level, the information can be uncovered.

### 1.13.2. Integrity

The three major principles that require for the concept of cloud information integrity:

- The data cannot be modified by any unauthorized entity or via any unauthorized process.
- The information stored over the cloud is not altered without the knowledge of the user and without their approval.
- The data needs to be consistent externally and internally that means the internal information needs to be consistent among sub-entities and with the external situation of the real world as well.

### 1.13.3. Availability

The availability aspect provides certainty that the appropriate personnel can access the cloud data over Cloud Computing resources with timely and reliable process. This aspect and shows that the proper functioning of the systems is taking place when their requirement arises.

In addition to that, the concept of availability provides a guarantee to the fact that cloud systems are working properly. A denial-of-service attack is a perfect example for the threat against the availability aspect of cloud computing.

## 1.14. CLOUD SECURITY SERVICES

There are few other essential factors related to cloud security that affect the assurance provided by cloud software. These factors mainly include accountability, auditing, authorization, and authentication and are summarized:

### 1.14.1. Authentication

Authentication is a process that allows the identification of authorized user to access the cloud services. This is done with the help of user ID and password provided to the user which they use while accessing the cloud platform and the cloud system matches the credentials and ensures whether the user is really the one who they are claiming to be. The users are given access to the system once the user ID and password matches with the information in the system and if the credentials do not match then the access is denied (Figure 1.5).



**Figure 1.5.** *Authentication process.*

Source: Image by OneSpan.

Using user ID and password are the basic form of authentication in the cloud system however there are much more secured authentication techniques have been developed such as two-factor authentication (2FA). For instance, the user ID and password can be hacked, but the 2FA provided an additional layer of security that is not easy to hack.

### 1.14.2. Authorization

Authorization in simple terms means the number of resources a user can get access to. Once they are authenticated to use the cloud services after that the



authorization factor determines the system rights extent that a user holds.

### **1.14.3. Auditing**

Monitoring and system audits are two basic methods by organizations to make sure that the operational assurance is maintained. The employment of these methods is dependent on the deployments and assets architecture and on the basis of that it is decided whether cloud service provided or the cloud customer can employ these methods or both can:

- System audit is performed to take care of the system security and it is performed either once or periodically.
- Monitoring, on the other hand, is a continuous process in which the system or the user is examined in order to identify or find any vulnerability in the system one such example of monitoring is intrusion detection.

Cloud services auditors or the IT auditors in general are of two types, one who are employed by the organization to perform audits of their systems are called internal auditors, and the other one is called external auditors who are not employed by any organization but provide their services by charging fee for that.

Internal auditors are employed by big IT organizations whose major job is to identify any threat within the system while the system audit is a periodic process, monitoring is done on a regular basis to ensure the security of the system.

### **1.14.4. Accountability**

Since various users are using shared cloud resources so all of these users are bound to follow the data obligation, thus, in order to identify any user responsible for any misconduct in the cloud system by determining their behavior and actions while accessing the cloud services.

## **1.15. CONCLUSION**

For the future IT applications cloud computing is an emerging technology and it will play a major role in most of the businesses. In this chapter, various security concerns related to Cloud Computing have been discussed along with their solutions.

The existing system for cloud computing security has been evaluated in order to find out how capable it is to secure users and organizations data and what future innovations are required in this field. Techniques such as cryptography have been discussed in which encryption and decryption processes are present that allows secure transmission of data over the cloud.

The chapter also elaborate various benefits of cloud computing for users and organizations since it allows unambiguous data access to the user and reduces cost for the organization in terms of physical data storage system.

The conclusion can be made from this chapter is that cloud computing is emerging technology for future IT applications and hence it is very important that all the security concerns related to cloud need to be tackled so that it can be used effectively without much worries. Further, in terms of future development, encryption techniques and security standards can be improved.

## REFERENCES

1. Agrawal, D., Gupta, B., & Wang, H. (2018). *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives* (1<sup>st</sup> edn.). CRC Press.
2. Delfin, S., Sai, R., Meghana, V., Lakshmi, K., & Sharma, S., (2018). *Cloud Data Security Using AES Algorithm*. Retrieved from: <https://www.irjet.net/archives/V5/i10/IRJET-V5I10224.pdf> (accessed on 1 April 2021).
3. Dey, N., Babo, R., Ashour, A., Bhatnagar, V., & Bouhlef, M., (2018). *Social Networks Science* (1<sup>st</sup> edn.). Springer.
4. Krutz, R., & Vines, R., (2011). *Cloud Security* (pp. 1–277). Indianapolis, IN: Wiley & Sons.
5. Le, D. N., Bhatt, C. M., & Madhukar, M., (2019). *Security Designs for the Cloud, IoT, and Social Networking*. John Wiley & Sons, Incorporated.
6. Li, S., Xu, L., & Romdhani, I., (2017). *Securing the Internet of Things* (pp. 1–137). Cambridge, MA: Syngress.
7. *Payment Card Industry, (PCI) Data Security Standard Requirements and Security Assessment Procedures*. (2008). Version 1.2.1



## CHAPTER 2

# Risks Issues and Security Challenges in Cloud Computing

## CONTENTS

2.1. Introduction.....	32
2.2. What Is Cloud Computing? .....	33
2.3. Cloud Computing Risks and Challenges in Businesses .....	35
2.4. Standardization Activities in Cloud Computing.....	42
2.5. Vulnerabilities and Threats .....	46
2.6. Strategies to Mitigate Cloud Risk.....	54
2.7. Conclusion .....	58
References .....	59

While cloud computing can be considered as big step going forward for many business, it also poses numerous security challenges and risks. This chapter examines risks and security challenges in cloud computing that businesses are facing these days. Additionally, the chapter also outlined several important standardization activities, the vulnerabilities, and threats associated with cloud computing. These include data breaches, hijacking account, strategies to mitigate cloud risk, insider threat, and limited cloud usage visibility. Finally, important strategies that can play a crucial role in mitigating cloud risks are also explored.

## 2.1. INTRODUCTION

Usage of cloud computing has increased dramatically and Microsoft, Google, and Amazon played a critical role in adoption of cloud computing amongst big and small enterprises.

The term “cloud” simply represents a remote data center and has two main roles. Firstly, the data center provides an access to data resources and information using a web browser. Secondly, the data center provides payment functionality based on the cloud storage size and frequency of usage of cloud resources. Cloud computing has been defined by The National Institute of Standards and Technology (NIST) as “a model for enabling universal, apt, on-demand network access to allocate pool of configurable resources of computing (e.g., networks, servers, applications, services, and storage) that can be released quickly and provisioned with insignificant management effort or service provider interaction.”

In addition, Gartner defines cloud computing as a category of computing style tremendously scalable IT that assists the deliverable and capable IT as services to external customers with the help of internet technologies.

Kepes describes cloud computing in a naive term as “the infrastructural paradigm shift that empowers the ascension of SaaS. Basically, it is a broad array of web-based on services which is concerned with permitting users to attain a variety of functional capabilities on a pay-as-you-go basis that formerly necessitated magnificent software/hardware investments and professional skills to acquire.”

In addition, Kumar et al. outline cloud computing as a storage system that enable admittance to the files anywhere using any technology via the internet by amassing the info on cloud server instead of a traditional computer. Cloud computing generally make use of virtualization methods as well as automation decision-making for server virtualization as well as for hardware virtualization.

Cloud computing generally empower their clients with a virtual infrastructure with the help of which they can simply store any information on the internet and run software and disseminate the server resources for frequent applications using virtualization techniques rather than running one application in the server with the traditional servers. It is probable to run many applications in one server by making use of hypervisor to apply virtualization.

Facebook, Outlook, G-mail, YouTube, and Google docs are few examples of cloud services. Services delivered via the internet can be usually referred to as cloud computing. Cloud computing basically has five key characteristics: broad network access on-demand self-service, measured service, resource pooling, and rapid elasticity.

Taking into consideration the minimal cost, it is particularly concerned with enhancing the performance and efficiency of computing systems. According to a report, it was found that 91% of the enterprises and organizations in the US and Europe that decide to shift to cloud environment was because of its minimal cost of execution as well as running costs.

## **2.2. WHAT IS CLOUD COMPUTING?**

Cloud computing can be defined as the delivery of various software and hardware services via the internet, through a network of remote servers. These remote servers are basically concerned with storing, processing, and managing data that empower users to upgrade or expand their present infrastructure (Figure 2.1).



**Figure 2.1.** *Functioning of cloud computing.*

Source: Image by BuffaloTech.

The breadth and capabilities of the cloud are enormous. The IT industry categorized it into these parts in a way to help better define use cases:

- **Software as a Service (SaaS):** This software is owned, carried, and organized remotely by one or more providers. Rather than installing software on the existing servers owned by the organizations, SaaS companies allow their users to rent software that is hosted on remote cloud storage. Typically it works on a basis of a monthly or yearly subscription fee. Marketing, CRM, finance-related tools use SaaS business intelligence (BI) and technology. Specifically, Adobe's Creative Suite has also made use of this model.
- **Infrastructure as a Service (IaaS):** Compute resources, complemented by networking capabilities and storage are hosted and owned by providers and available to their clients with respect to on-demand service.
- **Platform as a Service (PaaS):** The broad collection of application infrastructure (middleware) services. These services include integration, application platform, database services, and business process management.


All of this is an aberration from traditional on-premise computing that is executed via a local server or with the help of a personal computer. These traditional methods are increasingly being left behind. In fact, the IDG's



recently published Enterprise Cloud Computing Survey (2018) found that 73% of organizations have at least one application, or a portion of their computing infrastructure so far in the cloud-17% plan to do so within the next 12 months.

It is well known that cloud computing is consistently increasing. As we are living in a digital age, where big data and data discovery simply exceed the convention storage and hand-operated implementation and manipulation of business information, companies are looking for the best adequate solution for managing their data and information.

Traditional spreadsheets are now not feasible to accomplish their objective; there is just too much data to manage, store, and analyze. Whether it is in the form of online BI tools or an online data visualization system, there is a need on the part of companies to organize their data with respect to the location of data. Even the most traditional sectors have to adjust:



*"In an effort to do everything from offer better in-store customer service to fully leverage advances in manufacturing, companies from even most traditional and change-resistant sectors are seeing the writing on the wall: Cloud technology strategies cut cost and risk."*

—Lalit Bhatt, Project Leader at Maruti Techlabs.

Though the opportunities are great, this explosion hasn't come without issues in cloud computing. We discussed already some of these cloud computing challenges when comparing cloud vs on-premise BI strategies. Now let's go over more of those challenges that organizations are facing and how they are being addressed.

## **2.3. CLOUD COMPUTING RISKS AND CHALLENGES IN BUSINESSES**

### **2.3.1. Security Issues**

It is important to note that security risks related to cloud computing have become the key concern in 2018, as 77% of respondents stated in the referred survey. For the vast period of time, the lack of expertise/resources was the

serious cloud challenge. Although, in 2018 security inched ahead (Figure 2.2).



**Figure 2.2.** *Cloud computing security issues.*

Source: Image by CloudCodes.

Security will always be a major area of concern and in fact has been a concern from the start of cloud computing technology: one is not able to view the precise location where the data is being or processed. This resulted in enhancing the risks related to cloud computing that can arise during the management or implementation of the cloud.

Headlines highlighting compromised credentials, breach of data, and hacked interfaces, broken authentication, and APIs, account hijacking didn't help lessening concerns. Such incidents conducive to making the trust sensitive and proprietary data to a third party hard to stomach for some and, to be sure, worsening the challenges of cloud computing.

Luckily as cloud providers and users, security related to cloud computing are consistently increasing. In order to make sure that the privacy and security related to organization remain intact, verify the SaaS provider has strong user identity management, access control mechanisms and authentication in place.

In addition to the security and privacy issues, another major concern is compliance. It is important for the organizations to be able to comply with standards and regulations, no matter where the data is being stored. Speaking of storage, it is also important to have strict data recovery policies in place.

Security risks of cloud computing have now become a reality for each and every company, whether it's a small or large organization. That's why it is imperative to implement a secure BI tool that can leverage proper security measures.

### **2.3.2. Cost Management and Containment**

Another major risk associated with cloud computing costs. In the majority of cases, cloud computing can help in saving enormous costs of businesses. In the cloud, an organization can straightforwardly amplify its processing potential without putting huge investments in new hardware and software.


Instead, businesses can access extra processing via pay-as-you-go models from public cloud providers. Although, the on-demand and scalable nature of cloud computing services sometimes make it challenging to predict and regulations costs and quantities.

Thankfully, there are a number of ways one can keep in check about the costs related to the cloud, for instance, optimizing costs by engaging in improved financial analysis and reporting, automating policies for governance, or ensuring the management reporting practice on course, so that these issues related to cloud computing can be addressed.

### **2.3.3. Lack of Resources**

One of the common challenges facing by the companies using cloud are lack of expertise and/or resources. Organizations are comparatively placing more workloads in the cloud while technologies related to cloud are continuously expanding.

Because of all these factors, companies are facing serious challenges in keeping up with the tools. Also, the need for expertise has been increasing and will continue to increase in future. These challenges can be reduced with the help of additional training of IT and development staff. A strong CIO championing cloud adoption also helps.



*"The success of cloud adoption and migrations comes down to your people—and the investments you make in a talent transformation program. Until you focus on the #1 bottleneck to the flow of cloud adoption, improvements made anywhere else are an illusion."* —Drew Firment, Cloud Engineer

It is often seen that companies that are relatively small scale (especially the companies of small and medium scale) often witness that recruiting cloud specialists to their IT teams significantly increase their operations costs.

However, some of these tasks can be performed mechanically, but not all of them, therefore recruitment of specialist is unavoidable. In order to make the process automated, some companies are using tools such as DevOps like Chef and Puppet, in a way to carry tasks like monitoring usage patterns of resources and automatically backups at a particular period of time. These tools also help optimize the cloud for governance, cost, and security.

#### **2.3.4. Governance**

There are several challenges related to cloud computing and governance/control is also a key challenge. There is a need for IT governance in order to make sure that the IT assets are being implemented and used in accordance with the agreed-upon policies and procedures; make sure that these assets are thoroughly maintained and controlled, and certify that such assets are supporting strategies and objective of organization.

In the present cloud-based world, IT usually have no entire control over the provisioning, de-provisioning, and functioning of infrastructure. This resulted in enhancing the challenges for IT to deliver the compliance, governance, risks, and data quality management needed.

In order to lessen several uncertainties and risks in transitioning to the cloud, there is a need for IT to adapt its traditional IT governance and control processes to include the cloud. To this effect, the basic functioning of central IT teams in the cloud has been unfolding over the past several years.

Along with business units, central IT is continuously playing an enormous role in brokering, selecting, and governing cloud services. In

addition to this, third-party cloud management and computing providers are actively delivering governance support and best practices.

### **2.3.5. Compliance**

One of the potential risks of cloud computing that are in existence today is compliance. It is a major prevalent issue for those using backup services or cloud storage. Each time a company conveys data from the internal storage to a cloud, it needs to follow the procedure of being compliant with industry regulations and laws.

For instance, if healthcare organizations in the USA need to store any data on cloud, it would need to comply with HIPAA (Health Insurance Portability and Accountability Act of 1996), PCI DSS (Payment Card Industry Data Security Standard), and SOX (Sarbanes-Oxley Act of 2002).

Depending on the requirements and various industry standards, there is a need on the part of every organization to ensure that such standards are respected and carried out responsibly and ethically.

This is just one of the several challenges facing cloud computing, and although the procedure can consume a significant amount of time, the data should be stored well.

Cloud customers are required to have a look for vendors that can deliver compliance and keep an eye on whether these are regulated by the standards they need. Some vendors offer certified compliance, but in few scenarios, additional input is required on both sides to ensure proper compliance regulations.

### **2.3.6. Managing Multiple Clouds**

Challenges that are faced in cloud computing haven't just been concentrated in one, single cloud. The state of multi-cloud has been significantly grown in the past few years. Companies are shifting or combining private and public clouds and, as discussed earlier, tech giants such as Amazon and Alibaba are dominating the race.

In a recent survey, 81% of enterprises have a multi-cloud strategy. Enterprises with a hybrid strategy (merging private and public clouds) fell from 58% in 2017 to 51% in 2018, while companies having strategy of multiple private clouds and numerous public clouds rise gradually.

While organizations leverage an average of about five clouds, it is apparent that the use of the cloud will steadily grow in the future. That's

why it is utmost imperative to answer the critical questions organizations are facing today: what are the challenges for cloud computing, and how one can address these?

### **2.3.7. Performance**

When an organization starts hosting its data and resources on the cloud, it becomes fully reliant on the cloud service providers.

Nonetheless, this collaboration often provides businesses with innovative technologies they wouldn't otherwise be able to access.

While on the other side, the performance of the companies' BI and other cloud-based systems is also collaborated with the potential of the cloud provider when it vacillates. So, when there is a malfunction in the provider server, then it means the vendor's business is also down.

This isn't unusual, over the past several years, all the big cloud players have witnessed outages. Thus, it is important to make sure that the provider of a business has the adequate processes in place and that they will be sent notification of alert on time if any issue or problem is on cards.

For the data-driven decision-making process, organizations using real-time data is very crucial. Having the facility of accessing the data on a real-time basis that is stored on the cloud is one of the noteworthy decisions that an organization should take into consideration while choosing for the right partner.

With an inherent lack of control that is prevalent in the case of cloud computing, companies may face the real-time monitoring issues. Therefore, it is utmost important to make sure that the organizations' SaaS provider has real-time monitoring policies in place which will help in lessening such issues.

### **2.3.8. Building a Private Cloud**

Although it is often seen that having a private cloud is not the prerequisite for the majority of the organization, for those that are looking into such a solution, it is a major roadblock for them-private solutions should be carefully addressed.

Looking for private or internal cloud will result in providing greater benefit: having all the data in-house. But IT departments and managers will need to face building and gluing it all together independently, which can

cause one of the challenges of shifting to cloud computing tremendously demanding.

Therefore, it is utmost important to have a look on some of the steps that are essential in ensuring smooth operations of the cloud:

- Looking for shifting as many manual tasks as possible into mechanically (which would require an inventory management system);
- Orchestration of tasks in order to check that each one is executed in the right manner.

### **2.3.9. Segmented Usage and Adoption**

It is usually seen that the majority of the organizations did not have a robust cloud adoption strategy in place when they started shifting their operations onto the cloud. Rather, ad-hoc strategies sprouted, triggered by several components.

Among them, one is the speed of cloud adoption. Another one was the staggered expiration of data center equipment/contracts, leading to irregular cloud migration. Finally, there were also individual development teams making use of public cloud services for specific projects or applications. These bootstrap environments have fostered full maturation and integration issues including:

- Isolated cloud projects devoid of shared standards;
- Ad hoc security configurations;
- Lack of cross-team shared resources and learnings.

In fact, according to a recent survey by IDC of 6,159 executives, it was observed that just 3% of respondents outline their cloud strategies as “optimized.” Fortunately, centralized IT, control policies, and strong governance, in addition to some heavy lifting can get adoption, usage, and cloud computing strategies inline.

Almost 50% of the decision-makers have an opinion that their IT workforce is not completely ready to tackle the cloud computing industry challenges and controlling their cloud resources over the next 5 years. Since businesses are making use of the cloud strategy more often than ever, it is worth noticing that the workforce should keep an eye on and cautiously address the potential issues.

### **2.3.10. Migration**

One of the biggest cloud computing industry challenges in recent years is migration. It refers to the process of shifting an application on a cloud. Although shifting a brand new application is comparatively a straightforward process, shifting an existing application may bring significant challenges.

According to a recent survey by Velostrata, over 95% of companies are currently migrating their applications to the cloud and over 50% of them find the process very tedious.

What challenges and difficulties arise when we migrate applications to cloud? Most common challenges include:

- Security challenges;
- Extensive troubleshooting;
- Slow data migrations;
- Cutover complexity;
- Migration agents;
- Application downtime.

## **2.4. STANDARDIZATION ACTIVITIES IN CLOUD COMPUTING**

The major area of focus of this section is to discuss various initiatives and actions taken by several different standard development organizations (SDOs) across the world in the field of cloud application and service deployments, especially with respect to privacy and security issues. For each and every SDO, there is a need to have a center of attention on cloud computing-related works, especially with respect to privacy and security issues.

### **2.4.1. NIST Cloud Standards**

NIST is basically a reputable organization in outlaying several standards for cloud computing. In context to privacy and security aspects of cloud computing, NIST has produced and published standard guidelines for public clouds (Figure 2.3) (Badger et al., 2011).





**Figure 2.3.** *Maintaining cloud standard.*

Source: Image by Vecteezy.

The major area of the report published by NIST is to provide a brief summary about public cloud computing and the privacy and security considerations involved. It is basically concerned with discussing the potential threats, and safeguards surrounding public cloud environments, technology risks, and their suitable defense mechanisms.

The report observes that “since the cloud computing has grown out of an amalgamation of technologies, including service-oriented architecture (SOA), virtualization, Web2.0, and utility computing, many of the security and privacy issues involved in cloud computing can be viewed as known problems cast in a new setting” (Badger et al., 2011).

Although, public cloud computing portrays itself as a thought-provoking paradigm shift from traditional computing to an open organizational infrastructure-at the greater extent, relocating applications from the infrastructure of one organization to the infrastructure of another one, where the applications of possible adversaries may also operate. Some of the privacy and security issues that are recognized by NIST which can play a critical role in cloud computing are discussed as follows:

- Compliance;
- Governance;
- Trust;

- Identity and access management (IAM);
- Hardware and software architecture;
- Data protection;
- Software isolation;
- Incident response; and
- Availability.

### 2.4.2. Distributed Management Task Force

DMTF is responsible for developing standards for interoperable IT management solutions. DMTF is actively engaging with several topics, such as:

- **Open Virtualization Format (OVF):** That is concerned with the configuration of distributing and packaging software to run over virtual machines (VM).
- **Open Cloud Standards Incubator:** Which is responsible for engagement between cloud environments by producing cloud resource management protocols. The activity was shifted to cloud management working group (CMWG).
- **Cloud Audit Data Federation (CADF):** Working group which is responsible for the development of solutions that helps in sharing of audit logs or information.

As there are security issues associated with cloud computing, DMTF has entered into collaboration with CSA in a way to promote standards for cloud security as part of DMTF Open Cloud Standard Incubator.

It is worth noticing that the Open Cloud Standard Incubator group is held accountable for first developing of a series of management protocols, security tools, and packaging formats to initiate interoperability between cloud, accompanied by a description that will further help in cross-cloud management persistency and cloud service portability.

### 2.4.3. Storage Networking Industry Association (SNIA)

It was found that the SNIA has created the Cloud Storage Technical Work Group with the objective to develop SNIA architecture with reference to system implementations of cloud storage technology.

It is actively promoting cloud storage as a potential delivery model which will play an important role in providing elastic, on-demand storage billed for the space being used for this purpose. This type of feature called by the name cloud data management interface (CDMI), provide the access to customers to tag his/her data with special metadata (data system metadata) that the cloud service provider what data services to provide that data (archive, backup, encryption, etc.).

These data services will help in providing value to the data which is stored by customers onto their system by the implementation of the standard interface of CDMI. This will further enable customers to shift their data from one client to another client without witnessing the challenges of recoding to diverse interfaces. It is also important to note that SNIA is actively involved in storage network security-related activities.

Although storage network security is a completely new subject, it has rapidly capturing the market whether it be users or product developers. This high acceptance of network security with both hands by all the people across the world is only because of its increasing importance and value of the information held in online systems and of the separation of storage and processing functions triggered by the execution of storage area networks (SANs).

The overall objective of SINA's is "to ensure that storage networks become complete, efficient, and trusted solutions across the IT community." However, in order to attain this goal, SNIA will need to produce new technologies and standards in storage network security.

#### **2.4.4. Open Cloud Consortium (OCC)**

OCC is a member-driven organization, which had several roles, such as (a) being responsible for development of standards; (b) helping with setting benchmarks; (c) supporting reference executions of cloud computing; and (d) being engaged in sponsoring events and organizing workshops or awareness programs related to cloud computing.

It is worth noticing that the OCC has four working groups:

- Large working groups for data clouds;
- Open cloud test-bed working group;
- Standard cloud performance measurement (SCPM) working group; and

- Information security and sharing working group.

The major area of function for the SCPM working group is responsible for establishing benchmarks appropriate for four use cases:

- Moving an application between two clouds;
- Obtaining burst instances from multiple cloud service providers for a private/public hybrid application;
- Moving a large data cloud application to another large data cloud storage service; and
- Moving a large data cloud application to another large data cloud computing service.

## 2.5. VULNERABILITIES AND THREATS

As a modern technology, cloud computing offers several benefits. To reap all the advantages, one has to rigorously scrutinize as many cloud securities processes as possible. These threats vary from susceptibility to hijacked accounts malicious to code penetration to entire data breaches (Figure 2.4).



**Figure 2.4.** *Threats in cloud computing.*

Source: Image by Veritis.

Major cloud threats and vulnerabilities include:

### **2.5.1. Data Breaches**

Cloud computing services are comparatively new and permit accessing remote data via the internet. However, the internet can be the most ill-protected source for exploitation or misconfiguration.

Data losses breaches can be any form of cybersecurity attack in which sensitive or confidential information is stolen, viewed, or used by an un-allowed or unwanted person, or it may be conducive to accidental deletion by a natural catastrophe such as earthquake or fire outbreak, or by service provider.

It may result in causing loss of intellectual property (IP) to rivals, affecting the competitive strength, monetary impact out of regulatory implications, affecting goodwill and brand value of organization and thus gross market value may be at the verge as it fosters mistrust from business partners and customers.

Although, by the use of Encryption techniques, one can make the data more secure, but at the cost of system performance. Thus, robust and well-tested Data breach avoidance, strategies related to prevention of data loss, data backup, and data recovery and management procedure should be embraced before thinking about being migrated to the cloud.

### **2.5.2. Denial of Service (DoS) Attacks**

The preliminary functioning of cloud that delivers speed and scalability also becomes supporting ground for conveying super scalable malware. It is important to note that cloud applications are themselves potential weapon for disseminating the malicious attacks on a large scale, resulting in significant harm such as breaching data and hijacking accounts.

Malware injections generally refer to as code scripts that are integrated into the basic cloud service modules, thus functions as legitimate instance getting ingress to all the sensitive information and thus trespasser can eavesdrop, impacting the overall integrity of critical resources such as information.

Denial of service (DoS) attack makes key services unavailable to the legitimate user, thus affecting the overall security and performance. DoS may

work as a catalyst and used as a smokescreen in order to prevent malicious activities bypassing the firewall of the cloud and, thus can disseminate effortlessly to cause greater impact rather than infecting a single device.

### **2.5.3. Hijacking Account**

With the increase in the adaption and growth of cloud services in the past few years, there has been a surge in the hijacking case reported by the companies. It was found that imposter can now effortlessly exploit the potential to obtain access to login credentials, resulting in sensitive data such as business logic, data, functions, and applications stored on the remote cloud.

Account hijacking methods, which includes guessing reused passwords, using scripting bugs, and cross-site scripting enables the intruder to manipulate and forge information. Key-logging, man-in-cloud attack, buffer overflow, and phishing, are similar threats which can lead to a theft of user token and hijack a user account.

The impacts from a hijacked user account can be severe and cause disruption of business operations by means of whole eliminations of capabilities and assets. Thus, there is a need to take the issue of account hijacking seriously as intangible and tangible impact out of leakage of personal and sensitive data may damage the brand value as well as reputation.

### **2.5.4. Inadequate Change Control and Misconfiguration**

Scope and volume of the various resources used in cloud environment augmented with dynamism and complexity of resources poses serious threats in configuring effectively for adequate usage. Inappropriately configure precious computing resources, resulting in making such resources easy target for vulnerable evil unwanted activities and thus whole cloud repositories may revealed to trespasser. The overall impact on the organization relies on the nature of the misconfiguration, and how rapidly it has been resolved and detected.

Immoderate unwanted permission, unrestricted access to services and ports, unchanged configuration settings and default credentials, unsecured data storage, disabling standard security controls, monitoring, and logging are some particular issues associated with misconfiguration that should be dealt with utmost care by consistently scanning for misconfigured resources in real-time as traditional configuration management and change control technique becomes worthless in cloud environment.

### **2.5.5. Insecure Interfaces and Poor APIs Implementation**

Application programming interfaces (APIs) refer to an interface between the system and outside un-trusted entities most exposed parts of a system approachable through the Internet, allows their clients to customize their cloud experience and also indirectly provide the entry points or safe conduit for strangers.

It is often seen that a novice designed weak set of interfaces exposes a company's critical information to various security issues related to integrity, confidentiality, accountability, and availability. Apart from facilitating the programmers with the tools needed to build and integrate their applications with other job-critical software, API also perform the job of authentication, effect encryption and provide access.

There may be compromise of cloud assets if the susceptibility of an API that in the communication which occurs in-between applications is exploited. Thus, open and standard API frameworks should be referred while designing the interfaces that would accommodate in protecting against both malicious and accidental attempts to circumvent security.

### **2.5.6. Insider Threats**

The intervention of people in data security has many faces and can be done in a variety of ways. The insider human element can be from any hierarchy; both client organizations as well as service providers can abuse their authorized access to the cloud provider's or organization's systems, networks, and data as they are safely centered to pose threat without even shattering the firewalls and other security guarding mechanism (Figure 2.5).





**Figure 2.5.** *Insider threat in cloud computing.*

Source: Image by IntechOpen.

Data security has many aspects which can be misused by bad actors who may indulge in nefarious activities or misuse information through accidents, malicious intent, malware, or carelessness.

Several precautionary measures that organizations can take to prevent these accidents include day-to-day audits of on-offsite servers, password changes at regular intervals, restricted access to central servers and security systems.

Prevention is better than cure, and therefore it is important to proactively deal with any threats. Otherwise, threats will become more complex



and expensive and would require forensic investigation, containment, surveillance, escalation, and monitoring.

### **2.5.7. Insufficient Credentials and Identity**

Inadequate credentials, identity or key management would result in providing unauthorized access to information and data. As a result, a malicious encroacher camouflaged as an organizational user can access and manipulate the critical information.

If an impostor manages to attain authority to cloud user's credentials, it can target the complete information of the cloud along with the clients' companies' assets and even have an impact on the organization's administrative user as well. In addition to this, other users of the same cloud are also vulnerable to security breaches and incidences.

An automated regular rotation of cryptographic passwords and keys, removal of unutilized credentials, application of actual scalable central programmatic credential management system, and use of strong and secure authentication process are some of the measures that should be employed by the cloud provider to circumvent the potential hazard of data breaches.

Furthermore, due diligence must be taken into consideration that third parties to whom cloud provider may have maintenance work or outsources operations fulfill the conditions of security as contracted by cloud service provider as it incidentally levitates the threats, compromising with the entire security system.

Strictest credential access, segregated, and segmented accounts, and multifactor authentication (MFA) are some of the improved measures to reduce the risk of the identity theft.

### **2.5.8. Insufficient Due Diligence**

Non-standard APIs, non-standard data formats, and greater dependency on cloud provider's proprietary tools make it challenging and expensive affairs to migrate from one vendor to another. This may result in either cloud provider will start exploiting or in case if for some reason cloud provider halt its functioning and goes out of business, shifting database to another at adequate time becomes hectic, eventually leading to loss of data too.

Thus, in order to levitates circumvent such a grim situation of Vendor lock-in, due diligence and appropriate control plan should be in existence before taking decision related to migration to other cloud.

Any quick decision about predicting the nature and quality of services from cloud provider may lead to potential security risk, especially when the required services are control and bound under statutory and legal services or obligations hired for handling highly sensitive or financial or personal data.

Cloud service should involve in the activity of due diligence and also make sure that the proposed cloud service provider possesses a satisfactorily strong control plane in place; absence of this would result in loss of data, either by corruption or theft.

Apart from the technical issues discussed above, we also need to consider the human factor. If a person responsible for this function is unable to exercise full control over data security, verification, and infrastructure, then security, stability, and integrity of data may be at stake.

### **2.5.9. Shared Vulnerabilities**

It is generally seen that the multi-tenancy feature of cloud makes the services of cloud more economical for individual organization, but incidentally it results in yet another security issue. Exploitation of software and system vulnerabilities within cloud infrastructure, services result in screw-up to maintain logical and physical separation among distinct tenants in multi-tenant environment.

This foundering to keep separation can further be misused by intruders to get unauthorized access from one client's resource to others. Such attacks can be attained by misusing the vulnerabilities of either cloud provider or any of the tenants whose security can be compromised easily.

This may result in enhancing the attack surface, resulting in a higher probability of data leakage. In addition, by default the cloud security is a shared responsibility of both client organization as well as cloud service provider, thus it is important to have proper understanding in a way to implement security effectively and efficiently. Lack of success in achieving this seamless integration for security implementation may result in compromise of data and resources.

### **2.5.10. Nefarious Use or Abuse of Cloud Services**

Intruders by misusing the vulnerabilities of cloud computing resources may target the data of cloud provider's clients to host malware activities. Some of the ways adopted by the intruder to engage in such unfair means is either by launching DoS attacks, thus making the services unavailable to legitimate

users or such critical information can be made into some illegitimate use for illicit purpose like mining crypto-currency, automated click trailing, brute-force attacks for security breach by intruders and while the customer foots the bill.

The bill could be significantly giant as activities such as mining needed greater resources. Attackers make use of high cloud storage capacity in a way to propagate and store illicit and malware activities such as sharing of books, pirated software, music or videos, and invites legal consequences in intellectual copyright settlements and fines that could be even more cost exorbitant.

In addition, such complex structure of cloud service implementation assists intruders to hide and remain undercover for lengthy durations of time and such unnoticed risks, threats, and discrepancies poses more challenges for legitimate client and service provider.

To prevent the unethical usage and abuse of cloud services and lessen the risks caused by cloud service usage, there is need to procure security technology for actively scrutiny of cloud infrastructure usage and implementation of proper guidelines related to security that outlays what are the appropriate and legitimate behavior and what leads to exploitation and ways of identifying these behaviors.

### **2.5.11. Lack of Cloud Security Strategy and Regulatory Violations**

It is utmost important to develop a robust cloud security strategy; risk management and regulations policy should be devising before taking the decision related to shifting the base to cloud provider for various services instead of simply shift and lift without any due diligence.

Mostly, several companies are bound by and force to follow certain rules and restrictions, laws, and regulations of land of origin, and these compliances should be the epicenter for overall security policy. Sensitive data related to healthcare services, personal financial data, private student information, proprietary research data, IP data, and confidential business-related information logics constitutes different category of data.

These data and information are generally shifted to cloud for several services, and mostly security of these data and information are cover under particular apex commission or authorities and infringement of any type will result in formidable penalties and fines.

Security framework and architectures should be incorporated with the underlying business objectives and goals. Cloud provider being third party, after coming into contract for delivering the services, also become liable for ensuring the proper security measures as weak security would result in huge financial loss, legal repercussions, reputational damage, and fines.

### **2.5.12. Limited Cloud Usage Visibility**

The time when the company prepared to shift its assets and operation to the cloud, it starts losing the overall command and transparency over those assets. The ability to visualize, decide, and analyze whether the services rendered by clouds are malicious or safe, decides the extent of transparency of cloud usage. Even though organizations are taking the services of cloud provider, still it is their job to engage in analysis and interpretation and run time monitoring.

To enhance the transparency in the cloud and to lessen the risk, it is essential to produce a comprehensive solution that brings people, technology, and process together at one common platform and outlays accepted cloud usage policies to each and every member.

Otherwise, lack of cognizance about companies' governance policies and controls may results in compromising with the sensitive data by placing it into the hands of the public and compromising the cloud containers by inadequate setup of cloud services.

Thus, lack of governance, lack of awareness and lack of security would result in catastrophic risk. Installation of firewall, implementation of organization-wide zero-trust model, real-time interpretation of outbound activities, and keeping an eye on anomalies are some of the measures that may be helpful in controlling the skeptical behavior and lessening the overall risk.

## **2.6. STRATEGIES TO MITIGATE CLOUD RISK**

While the list of implied security and compliance considerations for cloud migration is large, the potential advantage of using the cloud computing is significantly higher than its risks if they are managed in a proper and better way. Utilize these methods to mitigate cloud migration risk (Figure 2.6).



**Figure 2.6.** *Strategies to mitigate cloud risk.*

Source: Image by BusinessTechWeekly.

### 2.6.1. Utilizing Data Encryption at Rest

Encryption at rest is concerned with protecting the data which is not in use or in transit. As data at rest is generally protected by monitoring and firewalls, it can be enticing to consider that is secure without encryption. However, in case a user password is compromised for some reason, the privacy of this data would no longer be secure (Figure 2.7).



**Figure 2.7.** *Data protection.*

Source: Image by Medium.

When sensitive data is shifted to a third-party cloud provider, the risk of unauthorized access significantly enhances. Data encryption at rest lessens this insecurity by ensuring data security even in case there would be unauthorized access arise via stolen credentials.

In addition, data encryption at rest is imperative to fulfill industry mandates such as PCI DSS, HIPAA, and SOX and preserve compliance with the government. In order to lessen the risk and support compliance mandates, both two-factor authentication (2FA) and data encryption at rest are baked into Expedient's newest multi-cloud solution, expedient enterprise cloud.

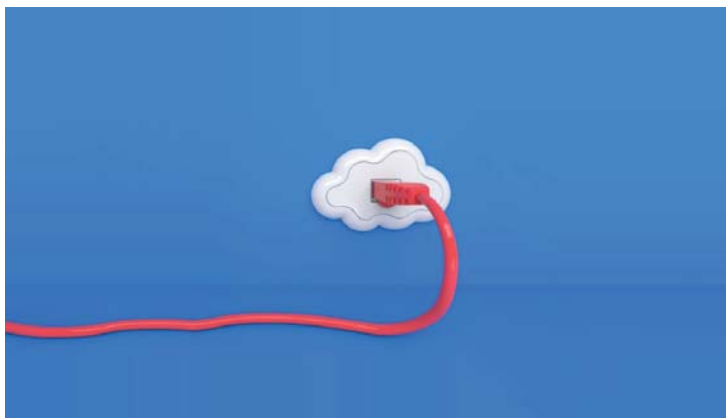
### 2.6.2. Utilizing Two-Factor Authentication (2FA)

By adding another security shield of 2FA, which means sending a one-time password generated by a personal PIN, every time when a person wants to use a system along with the general password, IT executives can add an extra layer of security to their cloud-hosted environments.

Not only is 2FA much more secure than just dependent on username and password combinations, it is also easy to use from the perspective of the end-user. Just as data encryption at rest, 2FA also greatly follows the government and industry compliance mandates.

### 2.6.3. Eliminating Shared Accounts

Sharing cloud platform credentials is a common practice among co-workers.



**Figure 2.8.** *Using cloud cables to reduce risks.*

Source: Image by Eleks.

Even though sharing cloud accounts may be more cost-effective than setting up a unique account for each user, sharing the cloud account poses a risk (Figure 2.8). In order to preserve data integrity and auditability, cloud accounts should not be shared amongst users for any reason.

#### **2.6.4. Insisting on a Well-Defined Shared Responsibility Model**

Whether a company uses infrastructure as a service (IaaS), software as a service (SaaS), or platform as a service (PaaS) model, a well-defined and reciprocal shared responsibility agreement with each cloud service provider is essential to reduce the risks associated with cloud-hosted services.

In addition, ensuring that each employee of the organization (whether they are consultants or full-time employees) has proper amount of knowledge about the various shared responsibility models in use by your various cloud providers.

As the complexity of enterprise cloud environments will consistently to increase in the near future, implementing the methods outlined above will likely to elevate in significance to lessen the inherent risk allied with the cloud.

#### **2.6.5. Using Standardized Cloud Assessment Questions**

Having a set of up-to-date cloud provider assessment questions that are descriptive of companies' cybersecurity and compliance objective is an imperative. With cloud services are now serving in all sizes and shapes, asking a standardized set of questions to each potential vendor will accommodate companies in setting a comparison baseline to evaluate which cloud service provider will be at best for fulfilling the needs of the business. Some of the questions that would be useful in assessing the services of a prospective cloud provider are discussed as follows:

- Do you have owned your data center facility or you are using the services of any other third party?
- Do you provide any leverage to third parties for your services? If so, do any one of them have access to the organization's systems and customer data?
- Comprehensive background checks for staff?
- What is the various solution of data encryption? How do you cope with the encryption keys?

- How are backups retained and protected? Is there is any facility of Disaster Recovery?
- Does the storage solution fulfill the necessity of data retention requirements (think SOX, PCI, HIPAA, etc.)?
- How one can get notification of alerts and potential issues with its services?
- How one can have a control over their data and crucial information?
- How the service provider isolate organizations' data from other clients?
- What types of attestations do service provider deliver in order to support the company's compliance efforts (i.e., SOX, PCI, HIPAA, HITRUST, etc.)?
- Can company get an access of provider's your attestation reports before signing a service agreement?
- Can organization have independent auditors visiting service provider data center?

## 2.7. CONCLUSION

Within the past few years, the trend of cloud has been increasing at a rapid rate, even in the context of the fast-moving IT sector and have been in high demand across the world. As it evolves, lack of faith in the security features imparted by the cloud is considered as the major roadblock and concerns that doubt users about storing their confidential data and information into this faceless intangible and nebulous entity known as the cloud.

Data protection and Information security are the two key concerns that interlope in the way of a wider acceptance and deployment of cloud. Over a period of time, most of the highly secure and powerful security standards are become emerging and steadily evolving with the aim to address several of such challenges. Undoubtedly, there are both opportunities and challenges associated with the cloud and because of the economics of scale, Cloud service provider are looking for a dedicated team of security specialists and cloud data storage hubs have physical protection at right place with military installations, thus ensuring highly secure and better security procedures, physical protection than any medium or small-scale enterprise.

Overall, as each technology is emerging at its own rate, cloud will also take its own time to fully develop and gain the trust of the people at large.



## REFERENCES

1. Calyptix Security, (2016). *Top 5 Cloud Computing Risks Cloud Computing Risks*. [Online] Available at: <https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/> (accessed on 1 April 2021).
2. Casey, S., (2021). *What are the Key Risks of Cloud Computing?* [Online] Nccgroup.com. Available at: <https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2019/october/what-are-the-key-risks-of-cloud-computing/> (accessed on 1 April 2021).
3. CDNetworks, (2021). *Five Key Cloud Computing Security Challenges-CDNetworks*. [Online] Available at: <https://www.cdnetworks.com/cloud-security-blog/5-key-cloud-security-challenges/> (accessed on 1 April 2021).
4. Cypressdatadefense.com. (2020). *Six Cloud Security Challenges and How to Address Them*. [Online] Available at: <https://www.cypressdatadefense.com/blog/cloud-security-challenges/> (accessed on 1 April 2021).
5. Dadhich, P., (2020). *Data Security Challenges in Cloud Computing-ZNetLive Blog: A Guide to Domains, Web Hosting and Cloud Computing*. [Online] ZNetLive Blog: A guide to domains, web hosting and cloud computing. Available at: <https://www.znetlive.com/blog/data-security-challenges-in-cloud-computing/> (accessed on 1 April 2021).
6. Deshmukh, S., (2018). *Cloud Computing Security Challenges and Considerations-DZone Cloud*. [Online] dzone.com. Available at: <https://dzone.com/articles/cloud-computing-security-challenges-and-considerat> (accessed on 1 April 2021).
7. Dosal, E., (2019). *Seven Cloud Security Challenges and Risks to be Aware of*. [Online] Compuquip.com. Available at: <https://www.compuquip.com/blog/cloud-security-challenges-and-risks> (accessed on 1 April 2021).
8. Durcevic, S., (2019). *What is Data Discovery?: A Professional Guide to Modern Tools*. [Online] BI Blog | Data visualization and analytics blog | Datapine. Available at: <https://www.datapine.com/blog/what-are-data-discovery-tools/> (accessed on 1 April 2021).
9. Durcevic, S., (2021). *Cloud Computing Risks, Challenges and Problems Businesses are Facing*. [Online] BI Blog | Data visualization

- and analytics blog | Datapine. Available at: <https://www.datapine.com/blog/cloud-computing-risks-and-challenges/> (accessed on 1 April 2021).
10. Harkut, D. G., (2020). *Introductory Chapter: Cloud Computing Security Challenges*. [Online] Available at: <https://www.intechopen.com/books/cloud-computing-security-concepts-and-practice/introductory-chapter-cloud-computing-security-challenges> (accessed on 1 April 2021).
  11. Innovativearchitects.com. (2017). *Eight Common Risks of Cloud Computing*. [Online] Available at: <https://www.innovativearchitects.com/KnowledgeCenter/cloud-computing/cloud-computing-risks.aspx> (accessed on 1 April 2021).
  12. Morrow, T., (2018). *Twelve Risks, Threats, and Vulnerabilities in Moving to the Cloud*. [Online] Insights.sei.cmu.edu. Available at: [https://insights.sei.cmu.edu/sei\\_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html](https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html) (accessed on 1 April 2021).
  13. Rosenson, J., (2021). *Five Strategies to Mitigate Cloud Risk-Expedient*. [Online] Expedient. Available at: <https://expedient.com/knowledgebase/blog/2018-10-01-five-strategies-to-mitigate-cloud-risk/> (accessed on 1 April 2021).
  14. Sen, J., (2021). *Security and Security and Privacy Issues in Cloud Computing*. [Online] Arxiv.org. Available at: <https://arxiv.org/pdf/1303.4814.pdf> (accessed on 1 April 2021).
  15. Shirky, C., (2021). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. [Online] O'Reilly online learning. Available at: <https://www.oreilly.com/library/view/cloud-security-a/9780470589878/ch04.html> (accessed on 1 April 2021).
  16. Soni, V., (2021). *Six Biggest Cloud Security Challenges and Risks in 2020 and Their Solutions*. [Online] Web hosting | Cloud computing | Datacenter | Domain news. Available at: <https://www.dailyhostnews.com/biggest-cloud-security-challenges-risks> (accessed on 1 April 2021).

17. Subramanian, N., & Jeyaraj, A., (2021). *Recent Security Challenges in Cloud Computing*. [Online] [www.sciencedirect.com](http://www.sciencedirect.com). Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0045790617320724> (accessed on 1 April 2021).
18. W3schools.in. (n.d.). *Cloud Security Challenges*. [Online] Available at: <https://www.w3schools.in/cloud-security-challenges/> (accessed on 1 April 2021).



## CHAPTER 3

# Application Safety and Service Vulnerability in Cloud Network

## CONTENTS

3.1. Introduction.....	64
3.2. Cloud Application Security in Different Cloud Services.....	65
3.3. Top Cloud Application Security Threats.....	71
3.4. What Cloud Application Security Options Are Available?.....	76
3.5. Who Is In Charge of Cloud Application Security?.....	77
3.6. Essential Characteristics of Cloud Network .....	79
3.7. Cloud-Specific Vulnerabilities .....	80
3.8. The Best Defense in Cloud Network Safety .....	92
3.9. Privacy-Preservation for Sensitive Data in Cloud Computing.....	94
3.10. Conclusion .....	97
References .....	99

With the advancement in technology and increased attacks, application safety of the cloud network become the chief target of the service provider. In the chapter application safety and service vulnerability in cloud network, the basic definition of cloud application security is discussed? It also highlighted some of the key cloud application security threats.

Some cloud application security options are also explored in this chapter. This chapter also try to give the answer that is play a much-needed role in cloud security. Similarly, it also tries to explain who's in charge of cloud application security. In addition, it also highlighted some of the essential characteristics of cloud network. It also shed some light on the vulnerabilities of cloud network. In the end, it demonstrated that the best defense in cloud network safety is analytics.

### 3.1. INTRODUCTION

Nowadays the term “the cloud” is becoming more and more popular. “The cloud” refers to the physical servers that can be accessed over the internet. The term also encompasses the software, applications, and databases that run on these servers. These servers provide better data storage facility, more enhanced data security, high flexibility, enhanced collaboration among employees, and changes the workflow of large enterprises as well as small businesses in order to empower them with better decision making with minimal costs.

In order to make virtual machines (VM), equipment, system, and computing assets are productively used by clients, and an on-request access to varied framework level administration which is in-manufactured stage is provided by cloud computing for this purpose.

A large number of crosswise utilizations over varying areas can thus be executed remotely by clients, for instance, activities like: utility administration, human services, e-administration, and many others. Due to its adaptability and cost-effectiveness amongst all the other available innovation zones, cloud computing totally stands out.

It is well known that the trend of utilizing the cloud is on a fast pace and is continue to increase in the future. It has been already predicted in business intelligence (BI) trends, the significance and execution of the cloud in companies such as Amazon, Alibaba, Microsoft, Google.

Utilizing the web, various facilities are delivered through cloud computing. Applications and instruments like databases, programming,

storage, systems management and servers are integrated through these assets. It becomes possible to store documents in remote databases through cloud-based empowerment, unlike the system of keeping these documents in equipment that has restrictive storage or is of a local storage kind.

The imperativeness of the cloud is highly exponentially. According to Gartner, it was forecasted that the cloud services market will rise at the rate of 17.3% in 2019 (\$206.2 billion) and by the year 2022, 90% of companies will be using the services of cloud computing.

### 3.2. CLOUD APPLICATION SECURITY IN DIFFERENT CLOUD SERVICES

Cloud application security can be defined as a series of defined processes, policies, controls, and technology which is responsible for governing or managing all information exchanges that occur in collaborative cloud environments such as Google G Suite, Microsoft Office 365, Slack, and Box (to name a few) (Figure 3.1).



**Figure 3.1.** *Cloud application security.*

Source: Image by datapine.com.

Hence, if an employee regularly shares or stores data in cloud applications such as the ones listed above (or the total available tens of thousands available), it is extremely essential to add a cloud application “safety net” to zero trust security infrastructure.

Moreover, in the cloud set-up, a different kind of security prerequisite is put into place by these models. Both SaaS and PaaS are based on the IaaS which is essentially the establishment of all the administrations of cloud. The dangers and security issues also multiply as more and more capacity is acquired.

Each one of these models has its own benefits when it comes to coordinated highlights, unpredictability vis-à-vis security and extensibility. Confidentiality and security issues are being looked into by associations that are using cloud computing for their administration framework.

The security of corporate information is definitely feasible in the “cloud” even though it is difficult as various administrations distinctive to it like SaaS, IaaS, and PaaS are provided by this. All the same different security issues are relevant to each administration.

### **3.2.1. Security Issues in SaaS**

Owing to the trust factor, namely data security, many organizations are still not comfortable in adopting SaaS even though a large number of vendors are adopting SaaS technology due to the varied benefits it provides, including a tremendous reduction in cost.

In order to attract users, the trust factor needs to be work upon and enhanced. An organization’s performance with respect to IT can be expanded fruitfully by the utilization of SaaS. However, many companies still turn shy of using the same due to the absence of trust factor.

There is inflexibility in SaaS where the companies want to modify the software as per their requirements or if they wish to keep data at their site as they have critical data and want to support their architecture by themselves.

Another issue that can be threatening is where the service provider removes the data from its end. According to Hayes in cloud computing, it is not possible to know as to whether the data removed by the client has been deleted by the service provider or if for reasons not known, the same has been saved at their end.



A series of security challenges arise from this very aspect. It is essential, especially where there are multiple users that the provider ensures the non-availability of one users' data to another user in a SaaS environment.

The user needs to be assured about the availability of the application whenever it is required and at the same time that all the requisite security measures are in due order. The data center of the SaaS provider stores the data of the all the users in the SaaS model.

For instance, SaaS applications that are not related to an enterprise may be stored with it where public cloud computing service is being dealt with by the provider. At the same time, to ensure high availability, the data may be replicated in a number of places/locations over a wide span of countries by the cloud provider. Little awareness and control over the security and storage of the user's data has given rise to a lot of anxiety with respect to the SaaS model.

In the process of deployment and development of the SaaS application certain key security concerns need to be considered carefully namely: network security, web application security, backup, virtualization, availability, identity management, authentication, and authorization, data integrity, data access, data confidentiality, data breaches, data security, data locality and data segregation.

### **3.2.1.1. Existing Security Solutions**

In this model of delivery, many researchers have been contributing towards finding a resolution to various kinds of security threats like network security, authentication, availability, data security, backup, and recovery, etc., the accessibility by users who are not known can be reduced as well as the patches can be kept updated by shutting down the services that are unused.

SLAs (service level agreement), which have been enhanced in isolation, can be used for the deployment of VMs by isolating the resource so as to ensure that during processing, data is secured. In approaches that are three-dimensional, a new way to authenticate them is through this technique.

Many problems that currently exist like data leakage and denial of service (DoS), among the others, are overcome through this catering for the availability of data. However, any unauthorized user can easily retrieve the data on the loss of login information as the data is not stored in encrypted form in this model.

A purely cryptographic storage service-based technique was proposed in a model by Lauter and Kamara. In this model, first, the message gets encrypted through the generation of a master key whenever data needs to be sent by a user to other users.

The receiver system has a secret decryption key stored in it which helps to decrypt the message once it is received. For the encrypted data, the method for searching is quite inefficient. Asymmetric searchable encryption (ASE), symmetric searchable encryption (SSE) and encrypted data searching techniques were discussed by them even though the overall complexity increases through these techniques.

After discussing the shortcomings of SSE and asymmetrical searchable encryption (ASE), they suggested that overcloud the usefulness of these techniques was negligible. Utilizing the order-preserving symmetric encryption (OPSE), a new model was introduced; however, no information with respect to confidentiality, security attacks and integrity was provided in this model. For the purpose of enhanced security over the cloud, a secure storage system is Presents Cloud Proof.

Users shall be able to not only detect but also prove cloud misbehavior through the scalable and efficient system obtained through various cryptographic tools used in this proposed model. Integrity and confidentiality-related violations shall be detected by the users with the help of this model.

Data security is ensured through each of the layers in the proposed structure, which is a three-layer system. Authentication is the responsibility of the first layer, data encryption of the second layer and data recovery of the third layer.

Various problems with regard to cloud computing like files system, backups, and security of data has been discussed and the digital signature concept with RSA algorithm has been proposed for the encryption of data whilst network is used to transfer it.

The problems of security and authentication have been solved through this technique. Implement software to cloud provider. Eight modern encryption algorithms have been compared, and two-factor authentications are used for the implementation of this software.

Based on the infrastructure of the cloud, the software that is proposed gets the highest and faster security algorithm which is compatible with the

cloud architecture that is in existence.

The main inhibitor for cloud computing has been deduced as data security and an analysis has been provided across data life cycle's all stages with regard to data security whilst proposing a system that helps to protect data by utilizing various schemes, such as Airavat.

Privacy leakage can be prevented in this system with no authorizations in the process for map-reduce computing. The main drawback of this work is that it mainly theoretical, and for its implementation it depends on others' schemes.

A development framework which has a security structure that is tough seems to be the best security solution for applications that are web-based. The four-tier framework that has been proposed for development that is web-based only deals with the security aspect of the entire process if though it seems quite interesting.

### **3.2.2. Security Issues in PaaS**

Without having to buy and maintain the requisite software layers and hardware, cloud-based applications can be deployed through PaaS. PaaS, just like SaaS and IaaS relies on a web browser that is secure and a network that is both reliable and secure.

Two software layers are involved in the PaaS application security, namely: Security of PaaS platform deployed customer applications and PaaS platform's own security (i.e., runtime engine).

Securing of the platform software stack is the responsibility of the PaaS providers whereby the runtime engine which runs the applications of the customers is included. Certain challenges like data security issues as are faced in SaaS also crop up in PaaS. Some of these are mentioned below.

#### ***3.2.2.1. Third-Party Relationships***

PaaS provides third-party web services components like mashups in addition to the programming languages that are traditional. More than one source element is combined into a single unit that is integrated in mashups.

As a result of this security issues like network and data security that are a part and parcel of mashups become a feature of PaaS models as well. At the same time, both the third-party services as well as web-hosted development tools' related security is depended upon by PaaS users.

### ***3.2.2.2. Development Life Cycle***

A number of applications are hosted on the cloud, and from the developer's side, there is an increased complexity for ensuring that secure applications when they go about the various stages of application development. Security and system development life cycle (SDLC) are affected by the speed with which applications in the cloud change.

Developers should make sure that they set up flexible application development processes because PaaS applications need to be frequently upgraded. These frequent updates may, however, pose security issues.

To avoid storage of data in locations that are inappropriate, the legal issues involved with respect to data should be clearly understood by developers in addition to having development techniques that are secure. Security and privacy can be severely compromised as a result of the storage of data at different places that have varying legal aspects applicable there.

### ***3.2.2.3. Underlying Infrastructure Security***

The underlying layers are usually not accessible to the developers in PaaS as a result of which the responsibility of securing the application services and underlying infrastructure lies with the providers.

There is no assurance available to the developers that the PaaS provider provides them with the environmental tools that are totally secure even though the developers may have full control over their application related security.

By and large, PaaS related security issues do not have much of available literature. The software that is to be delivered over the web is provided by SaaS, whereas the creation of SaaS applications is done through the tools provided through PaaS.

An architecture that is essentially multi-tenant is used by both of them so that the same software is used concurrently by a number of users. As discussed previously, the storage of users' data and PaaS applications in cloud servers could be a major concern as far as security is concerned.

Applications that are running on the cloud have data that is used by both PaaS and SaaS. The provider is the solely responsible for the security when the storage, transfer, and processing of this data takes place.

### 3.2.3. Security Issues in IaaS

Internet is used to access various resources that are provided by IaaS like storage, servers, networks, and other resources for computing which are in the form of virtualized systems. As far as the resources are concerned for all the ones allocated to the users, they have a free hand as far their management and full control is concerned in order to run any software.

In comparison to the other models, better control is available to the cloud users with IaaS as long as the virtual machine monitor has no security hole. The responsibility for correctly configuring security policies lies with the users and they have control over the software that operates or runs in their VM. All the same the cloud providers control the storage infrastructure, network, and the underlying compute. The communication, mobility, creation, modification, and monitoring pose certain threats to the overall security of the systems, and sufficient efforts must be taken by the IaaS providers to minimize these threats. IaaS related certain security issues have been discussed below.

## 3.3. TOP CLOUD APPLICATION SECURITY THREATS

In the current times, a majority of the organizations are using cloud computing. Work form becomes conservative, effective, and versatile due to it. Effectively it is quite open, has an engineering that is adaptable and is net-driven (Figure 3.2).



**Figure 3.2.** *Cloud security threats.*

*Source: Image by Compuquip.*

All the same organizations can still be rendered vulnerable by cloud. In the survey majority of the people projected that the adoption of cloud is inhibited mainly due to the concerns over security.

Without the resources of the corporate being affected as far as security is concerned, the organizations need to have policies and strategies in place so that their workers can exploit the cloud effectively. Find appropriate corrective measures after recognizing the main security-related issues is extremely essential.

It is well known by everyone that security poses a major threat in the cloud computing and IT teams of large companies are well aware of it. According to the cybersecurity Insider Report published in the year 2018, four widely known and prevalent cloud application security threats that IT teams face in their day-to-day life are discussed as follows:

### 3.3.1. Data Breaches

When the system proprietor is not aware that company information is stolen, a data breach incident occurs. Data breach may occur equally in small and large companies.

Exclusive, sensitive, or private information, such as user data, security details, or credit card details, is an example of information that can be stolen by hackers or bad actors. Data breach may cause betrayal of trust, which can hamper organization's reputation immediately and negatively affect company's users.

Some of the factors causing data breach include:

- **Obsolete software:** An intruder can easily take information by injecting malware into a PC that contains an obsolete software.
- **Easy-to-guess Passwords:** Simple and easy-to-guess passwords used by clients are always an easy target for attackers, especially if the password contains words or parts of the word. Simple or short passwords should never be used because they can be easily guessed by sophisticated or brute force attacks.
- **Drive-by Downloads:** When an individual browses a website that is compromised, they inadvertently download a malware or threat. A working framework, application, or program that has security issues or is outdated is often exploited by a drive-by download.

- **Intended Malware Attack:** Phishing emails and spam are used by scammers where they guide clients to sites that have been compromised or by downloading files that are infected, thus attempting to obtain client credentials.

### 3.3.2. Insider Threat

Any industry can be significantly threatened by insiders. Being able to access the framework from within the company, the insiders can easily bypass a series of security measures incorporated in the organization.

Insider threats should be promptly recognized and stopped, especially if they are causing damage inadvertently or purposefully damaging the resources through the techniques identified by the experts in the computer emergency response team (CERT). Regardless of the computer environment, insider threats play a destructive role. For instance, there is a perpetual threat of information being unfiltered or revealed to outsiders, which can cause a major damage to the company. The arbitrariness of the insider threat is a major cause for concern and may lead to the victim being affected in multiple ways, such as guilt, shame, or substance abuse. Insider attacks are often referred to as rational bombs, which result in loss of information.

A well-known case in this context is of a document server being planted with a logic bomb at one of the assembling offices of Omega Engineering. The software running the manufacturing process of the organization was decimated effectively by this logic bomb.

Another noteworthy case took place in San Francisco, where for 12 days, the employees were unable to access the system as an administrator changed the credentials. This matter was also reported in various news items. The infamous NSA leaks and the Department of Defense's secret internet protocol router network (SIPRNet) are other newsworthy cases where employees were involved to launch insider's threats.

### 3.3.3. Insecure APIs

Software developers and cloud vendors are able to help clients extricate data, oversee, and communicate over the cloud platform owing to the application programming interfaces (APIs). Various things can be done through APIs like furnishing a combination of storage segments and databases, assembling logs from an application or even controlling explicit cloud data.

An application that is versatile can backend benefits or associates with a site and at the same time provide capacity for client validation and query data with the help of APIs. To ensure that there is no revelation of data, it is essential that the development of APIs takes place bearing the security concerns and a sufficient amount of access control and confirmation techniques are in place.

A greeting card merchant that is web-based called Moonpig faced a data breach due to an uncertain API. Attackers consecutively attempted all client IDs and accumulated client data due to the static validation being used by a versatile application. APIs are like the front door to the application which is open thus the challenge posed by them in the cloud is quite serious. These need to be remotely available if this challenge is to be met.

Organizations that deal with APIs following a configuration method for security shall be able to understand the prerequisites for security and shall be able to ensure that a way is available that can guarantee sufficient approval, validation, and encryption in the same manner as making it certain that no vulnerabilities that are conspicuous are contained in the code.

Unfortunately, coding strategies that are secure have still not been within the reach of a majority of companies, thus releasing a not so solid production code.

### 3.3.4. Denial of Service (DoS) Attacks

A malicious attacker attempts to disable the intended users of a computer or such another similar device by attacking it through a denial-of-service (DoS) whereby the normal functioning of the device is interrupted. Normal traffic is not able to proceed in a DoS attack whereby the targeted machine is flooded or overwhelmed with requests so that the additional users are denied service. A single computer is used as a launchpad in DoS attack.

DoS attacks typically fall in two categories:

- **Buffer Overflow Attacks:** An attack in which all the hard disk space that is available, CPU time or memory is consumed by the machine is called a memory buffer overflow. Denial-of-service results from the exploitation of this kind that leads to crashing of the system, sluggish behavior or other deleterious behavior by the server.
- **Flood Attacks:** The server capacity can be over saturated by the malicious actor whereby a series large number of packets are used, thus again leading to a denial-of-service. The bandwidth



available with the malicious actor should be more than that of the target for the success of these DoS flood attacks.

### ***3.3.4.1. Rapid Elasticity and Measured Service Leading to a New Breed of Distributed Denial of Service (DDoS) Attacks***

Pay-per-use model is used for charging the adopters of the cloud service based on how often they use network resources and cloud servers. The economic resources of the cloud adopter, such as economic denial of sustainability (EDoS), can be targeted with this model. Here a new breed of attack is used to target in the cloud environment which is far different from the conventional DDoS attacks on the network and server resources.

Denial of the victim's economic viability in the long-term is the main aim of an EDoS attack. For instance, the cloud customer who owns the website gets billed for hosting the ostensible legal cloud service clients that continuously requests it to host the same in cloud servers so that bandwidth can be consumed.

The distinction of a legitimate traffic from the EDoS attack is quite tedious, and the webserver feels that the level of service denial has not been reached by the traffic.

It is important to note that the misconfiguration of application setup is one of the largest threats to cloud security because the incident of data breaches usually arises when services are inadvertently exposed to the public internet.

Unauthorized/unwanted access to a server, website, service, or other system is also one of the major areas for concern because once they're in, they can do the loss to the extent that we all are aware about.

Insecure interfaces and APIs offer eye-catching opportunities for attackers to breach systems because they are the only external assets which is not in the control of the organizational boundary as it is on the public IP address.

Account hijacking is feared by almost everyone because highly sensitive information and data stored and accessed on devices is shared and disseminated across several distinctive users—and because keeping tabs on rogue employees is problematic.

### 3.4. WHAT CLOUD APPLICATION SECURITY OPTIONS ARE AVAILABLE?

One of the common misconceptions in the present marketplace is that there is a need of a browser extension, proxy, or some other agent in a way to secure cloud applications. Although, there are availability of several cloud security solutions that use a cloud application's native APIs to control, monitor, regulate, and secure activities and functionality within them.

The two keys as well as basic options on the market are between proxy CASB vs an API. API-based cloud application security platforms (CASP) are rapidly becoming the most preferable security model for admins. The key reasons for this are discussed as follows:

First, a CASP doesn't required to route access through a proxy or broker, so it does not have any impact on the experiences of end-users in reference to the speed of network or access performance. Second, in contrast to the proxy-based solution, CASP is basically concerned with providing an additive layer of security to the architecture of a company.

They are known for working well with prevailing network security appliances, such as an individuals or company's firewall, by offering an additional level of control and security over information stored in cloud applications, that a gateway or firewall can't provide alone.

A proxy-based cloud access security broker (CASB) solely replicas the functioning of a firewall and puts it between the applications and the users and automatically occurs in a new application when a user opens it. It results in compromising with the user's experience as it further degraded (hitting significantly two different firewalls) with negligible to no extra security benefits.

Finally, most popular cloud applications advise against using a proxy-based CASB. Particularly, Microsoft and Google have both issued suggestions against their use. The key reason for this is because of CASB's incapability to stay updated as they make modernizations to their application infrastructures; application developers make changes to authentication methods, protocols, and more fairly regularly.

Because of the type of the CASB architecture, these variations can effortlessly break the relation in any number of ways. Application developers (particularly the eminent ones Microsoft and Google) do not commit to

threatening CASB developers when a variance could impact their product. Nor will they impact the creation of their own products for the sake of CASB vendors.

So, when this modification arises, the CASB developers would not be aware of it, and they won't comprehend the degree of the impact and gaps it creates in your security infrastructure until those gaps are mended by the CASB developers.

It is important to take into notice that some cloud security providers use Chrome browser extensions, instead of any broker and agent, to secure cloud access. They termed it as "agentless" cloud security, but an extension is merely a distinctive type of proxy.

Traffic is still directed through it, and they suffer from the same pitfalls as other CASBs. In addition, Google is considering a major revamp of Chrome extension support that could toss the entire technology through a loop.

While on the other hand, CASP, work as a closely intuitive feature within each cloud application. They develop deep one-to-one incorporations using the cloud applications APIs (usually in close association with the application service provider). Only alterations in API protocols can impact the efficiency of a CASP, and those alterations are constantly updated and documented for developers.

According to a 2018 cybersecurity insider report, it was found that almost one third of the IT security professionals do not even think they do not have the potential to keep with the pace at which SaaS application changes.

The good news is that CTsO, CTOs, and CISOs can integrate API-based CASP to roll with the punches without skipping a beat. These complex platforms can also effortlessly spot prevailing and/or potential risks in cloud applications on the basis of variance in OAuth permissions settings, security reports, customer complaints, and so much more.

### **3.5. WHO IS IN CHARGE OF CLOUD APPLICATION SECURITY?**

One of the best possible answer for this is the SaaS vendor and the customer themselves. But opposing to prevalent belief, the cloud application service provider does not take the accountability for the security of its client's data through its services.

It is often seen that the SaaS vendor is liable for safeguarding the application's infrastructure, along with its APIs. It means that they are accountable for the security of the servers, code, and networks that makes the application a product for customers.

It is the duty of the customers or respective clients to set up everything in a proper way, making sure everything is configured appropriately. They are in charge of founding and upholding a zero-trust security program. It is also the job of application users to monitor access to a cloud environment and control it with phishing, data loss prevention policies, and malware protection, and so on.

For instance, if a hacker by any means takes an entry into the system of a person and starts copying sensitive or critical information, send phishing emails, it is the entire duty of the users to remediate and detect that activity. It is important to note that the SaaS provider is not accountable or responsible for the data that is uncovered or any of the reparations a breach event may cause.

Cloud security is the topmost threat factor that IT managers view as a major roadblock to cloud transformation. But, for the majority of the industries and organizations, the advantage of this is far higher than the risks.

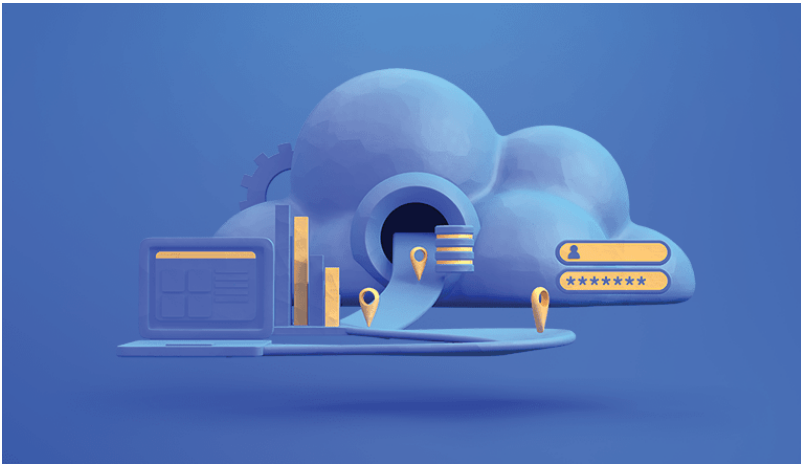
There are several sides to constructing an effective cloud computing security infrastructure, and safeguarding the data generated, accessed, and stored in company cloud applications is a big part of that. What often ends up being lost in the cloud computing story is just how safe cloud computing really is in comparison to on-premise.

When an organization transformed its operations onto the cloud, it is outsourcing some of the more problematic infrastructure and server security processes to another vendor (often, to a vendor having significantly larger and superior funded security team just like in the case of Microsoft and Google).

It is well known that cloud computing is still comparatively new, and the security risks are chiefly misinterpreted. If a company is using cloud applications, or they are preparing for a changeover to the cloud, they need to comprehend what is essential to properly safeguard it. There is also a need to access the control and visibility, over access and use, that they had with on-premise software.

### 3.6. ESSENTIAL CHARACTERISTICS OF CLOUD NETWORK

In its explanation of essential cloud characteristics, the US National Institute of Standards and Technology (NIST) seizes well what it means to provide IT services from the conveyor belt using economies of scale (Figure 3.3).



**Figure 3.3.** *Cloud migration.*

Source Image by objectivity.

#### 3.6.1. On-Demand Self-Service

Users can manage and order services without any interaction or communication with the service provider, using, for instance, management interface and a web portal. Provisioning and de-provisioning of services and allied reserves arise instinctively at the provider.

#### 3.6.2. Ubiquitous Network Access

It is important to note that the cloud services can be accessed via the network (typically the Internet), using protocols and standard mechanisms.

#### 3.6.3. Resource Pooling

Computing resources that are set up using a consistent infrastructure shared amongst all service users.

### 3.6.4. Rapid Elasticity

Resources can be scaled up and down elastically and rapidly.

### 3.6.5. Measured Service

Resource or service usage is persistently metered, supporting fuller utilization of resource usage, pay-as-you-go business models and usage reportage to the customer.

## 3.7. CLOUD-SPECIFIC VULNERABILITIES

A vulnerability is cloud-specific if it:

- is inherent to or ubiquitous in a core cloud computing technology;
- has its basis foundation in one of NIST's essential cloud characteristics;
- is instigated when cloud inventions make tried-and-tested security controls impossible or difficult to execute; or
- is prevalent in established state-of-the-art cloud offerings (Figure 3.4).



**Figure 3.4.** *Cloud-specific vulnerabilities.*

Source: Image by Hacker Noon.

### 3.7.1. Core-Technology Vulnerabilities

Cloud computing's core technologies-Web applications and services, cryptography, and virtualization have susceptibilities that are either

congenital to the technology or widespread in the implementations of technology. Three examples of such vulnerabilities are session hijacking and riding, virtual machine escape, and obsolete or insecure cryptography (Figure 3.5).



**Figure 3.5.** *Core-technology vulnerabilities.*

Source: Image by Lucid Chart.

First, the likelihood that an invader might effectively escape from a virtualized environment dependent on the very nature of the virtualization. Consequently, there a need to consider this vulnerability as inherent to virtualization and extremely pertinent to cloud computing.

Secondly, Web application technologies need to address the problem that, by purpose, the HTTP protocol is a stateless protocol, while Web applications needed some idea of session state. Several types of techniques



execute session handling, and as any security expert experience in Web application security will attest-many session handling executions are susceptible to session hijacking and session riding.

Whether session hijacking/riding susceptibilities are inherent to Web application technologies or are “only” predominant in numerous present-day implementations is debatable; in any case, such susceptibilities are definitely pertinent for cloud computing.

Finally, cryptanalysis advances can result in any algorithm insecure or cryptographic mechanism as novel methods of contravening them are exposed. It is now even more easy to find critical flaws in cryptographic algorithm executions, which can change strong encryption into weak encryption (or occasionally no encryption at all).

Because the overall applicability of cloud computing is unimaginable without the use of cryptography to guard data privacy and maintain integrity in the cloud, obsolete or insecure cryptography susceptibilities are extremely pertinent for cloud computing.

### **3.7.2. Essential Cloud Characteristic Vulnerabilities**

As it is discussed, NIST labels five critical cloud characteristics: ubiquitous network access, on-demand self-service, rapid elasticity, resource pooling, and measured service. Following are instances of susceptibilities with root causes in one or more of these characteristics:

### **3.7.3. Unauthorized Access to Management Interface**

The cloud characteristic on-demand self-service demands a management interface which is available to cloud service users. Unofficial access to the management interface is therefore a particularly germane susceptibility for cloud systems: the likelihood of happening of unapproved access is significantly greater than for traditional systems where the functioning of management is only limited or accessible to a few administrators.

### **3.7.4. Internet Protocol Vulnerabilities**

The cloud characteristic ubiquitous network access means that services of cloud can be accessed via network by using standard protocols. In majority of the instances, this network is the Internet that are mostly believed to be untrusted. Internet protocol susceptibilities-such as exposures that permit man-in-the-middle attacks-are thus important for cloud computing.



Data recovery vulnerability. The cloud characteristics of elasticity and pooling necessitate that resources assigned to one user will be transferred to a distinct user at a later period of time. For storage or memory resources, it might therefore be conceivable to recuperate data penned by a former user.

### **3.7.5. Metering and Billing Evasion**

The cloud characteristic of measured service means that any services of a cloud service have the potential of metering at an abstraction level adequate to the type of service (such as processing, storage, and active user accounts).

Metering data is basically taken into use to enhance service delivery as well as the process of billing. Appropriate susceptibilities include billing and metering data manipulation, and billing evasion.

### **3.7.6. Defects in Known Security Controls**

Susceptibilities in standard security controls should be deliberated cloud specific if cloud innovations unswervingly cause the complications in executing the controls. Such susceptibilities are also known by the name control challenges.

Three instances of such control challenges are discussed here. First, virtualized networks offer inadequate network-based controls.

Given the basis or foundation of cloud services, the managerial access to IaaS network infrastructure and the potential to customize network infrastructure are normally restricted; hence, standard controls such as IP-based network zoning would not be applicable here.

Also, standard techniques such as network-based susceptibility scanning is generally prohibited by IaaS providers because, for instance, friendly scans cannot be distinguished from the activities of the attacker.

Lastly, technologies such as virtualization mean that network traffic arises on both virtual and metering networks, such as when two virtual machine environments (VMEs) introduced on the same server communicate. Such concerns organize a control challenge because tested and tried network-level security controls might not be able to perform in a certain cloud environment.

The second challenge is because of the poor key management procedures. As found in an existing European Network and Information Security Agency study, structures in cloud computing needed storage and controlling of several distinct kinds of keys.

Because VM do not facilitate with a fixed hardware infrastructure and content of cloud is distributed on the basis of geographic locations, it is highly problematic to apply standard controls-such as hardware security module (HSM) storage-to keys on cloud infrastructures.

Finally, it is important to note that security metrics aren't adapted to cloud infrastructures. Currently, there are no standardized cloud-specific security metrics that can be used by cloud clients in a way to monitor the security status of their cloud resources.

Until such standard security metrics are implemented and developed, controls for security audit, interpretation, and accountability are much more challenging and exorbitant, and might even be unreasonable to employ.

### **3.7.7. Prevalent Vulnerabilities in State-of-the-Art Cloud Offerings**

Although cloud computing is a comparatively young and rapidly evolving discipline, there is already a large number of cloud providers on the market. Hence, we can complement the three cloud-specific susceptibility pointers formerly with another empirical pointer:

If a susceptibility is widespread in state-of-the-art cloud offerings, it should be taken into consideration as cloud-specific. Instances of such susceptibilities include weak authentication schemes and injection susceptibilities.

Injection susceptibilities are manipulated by exploiting application or service inputs to execute and interpret parts of them against the intentions of the programmer. Instances of injection vulnerabilities include:

- SQL (structured query language) injection, the input of which is SQL code that is mistakenly implemented in the database back end;
- Command injection, the input of which comprises instructions that are inaccurately executed via the OS;
- Cross-site scripting, the input of which comprises JavaScript code that is executed by a victim's browser;
- Furthermore, several extensively used authentication mechanisms aren't strong. For instance, authentication's usernames and passwords are majority of the time weak due to:
- Uncertain behavior of user (using same passwords again, choosing weak combination of passwords, and so on), and

- Inherent limitations of one-factor authentication mechanisms.

Also, the execution of authentication mechanisms might have shortcomings and let, for example, credential interception and replay. A large number of Web applications in present state-of-the-art cloud services employ passwords and usernames as authentication mechanism.

### 3.7.8. Cloud Software Infrastructure and Environment

The *cloud software infrastructure* layer stipulates a concept level for fundamental IT resources that are presented as services to higher layers: computational resources (usually VMEs), (network) communication, and storage.

These services can be used independently, as is archetypally the situation with storage services, but these are generally equipped such that servers are distributed with certain network connectivity, along with storage access. This package, without or with storage, is typically indicated to as IaaS.

It is important to note that the *cloud software environment* layer delivers services at the application platform level:

- A progress and runtime phase for applications and services inscribed in one or more supported languages;
- Storage services (a database interface instead of file share); and
- Communication infrastructure, such as Microsoft's Azure service bus.

Susceptibilities in both the environment and infrastructure layers are typically precise to one of the three resource types offered by these two layers. Although, cross-tenant access susceptibilities are pertinent for all these three types of resources. The vulnerability escape by virtual machine is one of the perfect examples that was discussed earlier.

It is generally used to validate a susceptibility that is inherent to the core virtualization technology, but it can also be view as having its root cause in the critical feature of resource pooling: whenever reserves are amalgamated, unapproved access across reserves becomes a prevailing problem.

Henceforth, for PaaS, where the technology to distinct distinctive tenants (and tenant services) is not essentially dependent on virtualization (though that will be progressively true), cross-tenant access susceptibilities play a very critical role as well.

In a similar way, cloud storage is vulnerable to cloud communication and cross-tenant storage access-in the shape of virtual networking is vulnerable to cross-tenant network access.

### 3.7.9. Computational Resources

A significantly important set of computational resource susceptibilities distresses how virtual machine images are managed or handled: the only best possible way of providing nearly similar server images-thus delivering on-demand service for virtual servers is by duplicating template images.

It is generally seen that virtual machine template images that are prone to misuse cause application or OS susceptibilities to spread over many systems. An attacker might be able to scrutinize configuration, code or patch level in detail with the help of organizational rights by letting a virtual server as a service customer and resulting in acquiring information imperative in attacking other images of customers.

A similar challenge is that an image can be attained from an unreliable source, a new phenomenon brought on particularly by the developing marketplace of virtual images for IaaS services. In such a scenario, an image could, for instance, have been prejudiced in order to enable back-door access for the attackers.

It is often seen that leakage of data by virtual machine duplication is a susceptibility that's also entrenched in the use of cloning for stipulating on-demand service. Cloning resulted in causing problems related to leakage of data with respect to machine secrets: certain elements of an OS-such as cryptographic salt values and host keys-are meant to be private to a single host.

Cloning can disrupt this privacy assumption. Again, the developing marketplace for virtual machine images, just like in Amazon EC2, conducive to an associated problem: users could disseminate template images for other users by transitioning a running image into a template. Contingent on how the image can be used before generating a template from it, it might comprise of information that the user does not want to reveal on a public platform.

In addition to this, it also entails control challenges, including those associated with cryptography use. Cryptographic susceptibilities because of weak random number generation may be prevalent if the generalization layer between the OS kernel and hardware initiated by virtualization is challenging for creating random numbers within a VME.

Such origination necessitates an entropy source on the hardware level. It might be possible that virtualization have faulty mechanisms for tapping that entropy source, or having several VMEs on the same host might drain the presented entropy, resulting in weak random number creation.

As it is demonstrated earlier, this abstraction layer also obscures the applicability of advanced security controls, for example, HSMs, probably resulting in insignificant key management procedures.

### **3.7.10. Storage**

Apart from the data recovery susceptibility because of elasticity and resource pooling, there is a linked control confront in media sanitization that is in majority of the cases impossible or hard to execute in a cloud setting. For instance, policies in context to data destruction pertinent at the end of a life cycle that needed physical disk annihilation can't be conveyed out if another tenant is still using a disk.

Because cryptography is often used in order to address storage-related susceptibilities, this vulnerability of core technology-obsolete or insecure cryptography as well as poor key management-play a very eminent role in cloud storage.

### **3.7.11. Communication**

One of the important examples of a cloud communications service is the networking provided for VMEs in an IaaS environment. Because of pooling of resources, numerous clients are more likely to distribute definite network infrastructure constituents: susceptibilities of components of shared network infrastructure, such as Dynamic Host Configuration Protocol, susceptibilities in a DNS server, and IP protocol susceptibilities, might trigger attacks of network-based cross-tenant in an IaaS infrastructure.

It is generally seen that virtualized networking also offers a control challenge: again, in cloud services, the managerial access to IaaS network infrastructure and the probability for modifying network infrastructure are usually restricted.

Also, making use of technologies such as virtualization resulted in enabling a situation where network traffic arises not only on "real" networks but also within virtualized networks (for instance, for interaction between two VMEs that are functioning on the same server); most executions of

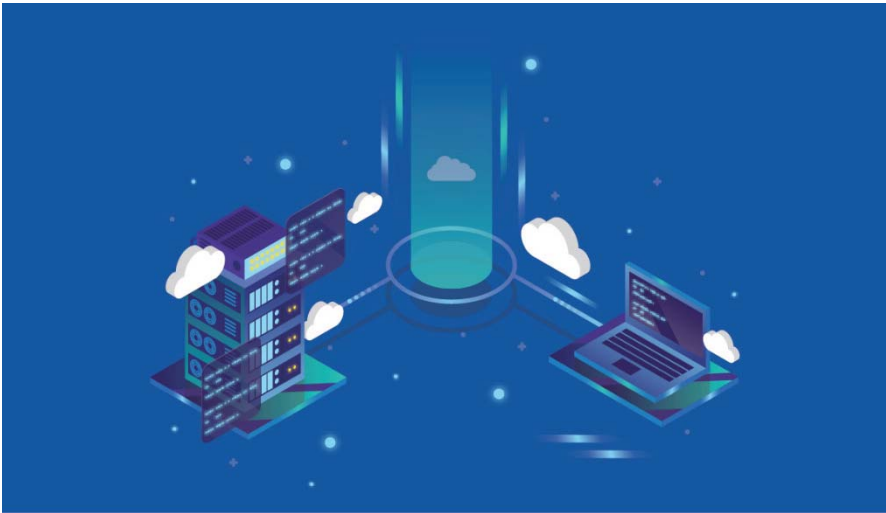
virtual networking propose restricted prospects for incorporating network-based security.

In sum, this represents a control challenge of inadequate network-based controls as tested and tried network-level security controls might not be able to perform in a given cloud environment.

### 3.7.12. Cloud Web Applications

It is important to note that cloud-based web applications generally make use of browser technology as the front end for user interaction. With the augmented uptake of browser-based computing technologies such as Java, JavaScript, Silverlight, and Flash, a Web cloud application can be categorized into two parts:

- An application component operated anywhere in the cloud; and
- A browser component functioning within the browser of a user (Figure 3.6).



**Figure 3.6.** *Cloud web application.*

Source: Image by rapid value solutions.

It is expected that in the near future, developers will more likely to enhance the use of technologies such as Google Gears in order to permit offline usage of a browser component of Web application for use cases that do not need steady access to remote data. The two typical susceptibilities

for Web application technologies have already been described: session injection vulnerabilities and hijacking and riding vulnerabilities.

Other Web-application-specific susceptibilities distress the front-end component of a browser. Among them are client-side data handling susceptibilities, in which attackers manipulate Web applications by sending data from their application constituent to the server's application component.

In other words, the input which is acknowledged by the server component is not the "predictable" input propelled by the client-side component, but transformed or entirely user-generated input.

Also, Web applications also dependent on browser mechanisms for segregating content inserted in the application by third-party (such as mashup components, advertisements, and so on). Browser isolation susceptibilities might thus allow third-party content to bias the Web application.

### **3.7.13. Services and APIs**

It is well known that all layers of the cloud infrastructure offer services, but for interpreting cloud infrastructure security, it is imperative to clearly think about all of the services of infrastructure and APIs.

The majority of the services are just like Web services that share several susceptibilities with Web applications. Certainly, the Web application layer might be comprehended entirely by one or more Web services such that the application URL (uniform resource locator) would only give the user a browser component. Thus, the API functions and supporting services share numerous susceptibilities with the Web applications layer.

### **3.7.14. Management Access**

NIST's description of cloud computing defines that one of cloud services' vital characteristics is that they can be quickly provisioned and freed with insignificant management effort or interaction by service providers.

Subsequently, a usual element of every cloud service is a management interface that directly contributes to the susceptibility regarding unauthorized access to the management interface. In addition, because management access is often recognized using a Web service or application, it regularly shares the susceptibilities of the API component/services, and Web application layer.

### 3.7.15. Identity, Authentication, Authorization, and Auditing Mechanisms

All cloud services (and every management interface of cloud services) needed mechanisms for identity management, authorization, authentication, and auditing (IAAA). To some degree, segments of these mechanisms might be point out as a stand-alone IAAA service to be used by other services.

Two IAAA elements that must be part of each service execution are implementation of satisfactory authorization checks (which, of course, use authorization and/or authentication information or data received from cloud infrastructure auditing or an IAA service).

Most susceptibilities allied with the IAAA component must be considered as cloud-specific as they are widespread in state-of-the-art cloud assistances. Formerly, the example related to weak user authentication mechanisms were discussed; other examples include:

- **Denial of Service (DoS) by Account Lockout:** One of the most widely used security control-particularly for verification using username and password-is to lock out accounts that have received numerous failed validations tries in rapid succession. Attackers can indulge in such effort to launch DoS attacks against a user.
- **Weak Credential-Reset Mechanisms:** It is generally seen that when cloud computing service providers manage their user's credentials themselves instead of using federated authentication, they must provide a method for resetting credentials in the case of lost or forgotten credentials. Earlier, password-recovery means have upheld chiefly weak.
- **Faulty or Insufficient Authorization Checks:** State-of-the-art Web application and service cloud offerings are usually susceptible to faulty or inadequate authorization checks that can make actions or unauthorized information presented to users. Missing authorization checks, for instance, are the major reason for the attacks related to URL-guessing attacks. In such attacks, users modify URLs to exhibit information or data of other user accounts.
- **Coarse Authorization Control:** It is generally seen that interfaces of Cloud services management are chiefly vulnerable to proposing authorization control models that are too coarse. Thus, standard security measures, such as duty separation, cannot



be applicable in this case as it is almost challenging to offer users with only those rights, they severely necessitate to carry out their work.

- **Insufficient Logging and Monitoring Possibilities:** Currently, there are no mechanisms or standards exist to give cloud customers monitoring and logging facilities within cloud resources. It gives boost to a severe problem: log files record all tenant events and cannot be simply shortened for a single tenant.

Also, security monitoring by service providers is usually hindered by inadequate monitoring capabilities. Until we create and execute usable monitoring and logging standards and capacities, it's tough-if not impossible to execute security controls that necessitate monitoring and logging.

Of all these IAAA susceptibilities, in the knowledge of cloud service providers, presently, authentication matters are the chief susceptibility that puts the data of clients in cloud services at jeopardy.

### 3.7.16. Provider

Susceptibilities that are pertinent for all cloud computing components normally worry the provider- or instead users' incapability to govern cloud infrastructure like the one they do to their own infrastructure.

Among the control confronts are inadequate security audit potentials, and the fact that security metrics and certification schemes are not embraced to cloud computing. In addition, standard security controls with respect to certification, audit, and constant security supervising can't be effectively executed.

It is important to note that cloud computing is in persistent development; as the arena mellows, additional cloud-specific susceptibilities will certainly arise over time, while others will become less of an issue.

Control challenges normally emphasize situations in which otherwise successful security controls are useless in the context of cloud computing. Thus, these challenges have exceptional relevance for further research related to cloud computing security.

Indeed, several present-day efforts-such as the development of certification schemes and security metrics, and the move toward full-featured virtualized network components-straightforwardly handle control challenges by permitting the use of such tested and tried controls for cloud computing.

### 3.8. THE BEST DEFENSE IN CLOUD NETWORK SAFETY

One of the most typical approach to safeguard on-site corporate networks from cyber-attacks is to incorporate the use of IT systems to prevent and detect unwanted efforts in a way to take an entry. Such efforts are dependent on the traditional view that the network of a company is like a castle inside walls (Figure 3.7).



**Figure 3.7.** *Analytics in cloud network.*

Source: Image by Oracle Blogs.

The castle is shielded by securing on more and more security measures in expectations of keeping attacker's miles away without rendering these networks so impermeable as to make them unfeasible.

Yet no such simply defensive tactical system can ever be strictly effective, particularly as companies digitize more and more aspects of their internal actions and external sources with the outside world.

Operational technologies are becoming too multifaceted to be safeguarded this way, and hackers will always be one step ahead in finding the vulnerability. The challenge calls for a completely distinct type of solution and that is where the role of cloud enters in.

Before going any further, it is worth noticing that not all cloud-based systems are identical. Some are more progressive than others. Some services billed as “cloud computing” do slightly more than imitate an on-premises connection in a network of interlinked computers. Currently, the major cloud providers include Amazon Web Services (AWS), Google Cloud Platform, and Microsoft’s Azure. These advanced cloud services demonstrate main investments in protections, interoperability, and ongoing innovation that permit off-premises enterprise IT to grasp its possibility.

From security perspective, cloud computing can provide almost limitless economic computational power, which is often required to ascertain the sorts of suspicious activity that reveal the hacker’s activities (what are their present and future course of action) and who they might be.

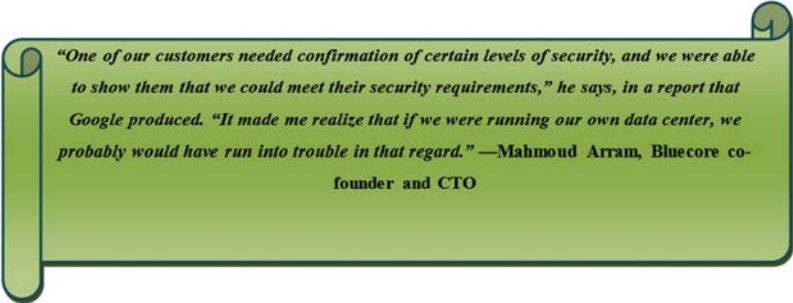
Without the cloud platform and its analytical power, it would be almost unbearable to identify such patterns, particularly when keeping an eye on high volumes of data, highly complicated and interlinked applications, and time interims as long as months or years.

Because cloud software is autonomous of specific hardware platforms, it is naturally “virtual”—code runs on other code, but not on devices. It made it easier to adapt, often instantly, to interruptions and other variations in the environment.

It is often seen that cloud also facilitate simplicity. It lessens the total points of vulnerability and makes it simpler to cope with the technological advancements—because companies can now dependent on the cloud services providers to build the hardware, cloud infrastructure, software, and services needed. It also permits companies to scale up their systems as per the requirement, to a level not conceivable with on-premises computing.

For example, Bluecore, a New York City-based start-up, provides about 100 high-end e-commerce companies with the ability to send customers emails in response to their online behavior. A shopper might make several purchases on a website, but then reach the shopping cart page, feel put off by the shipping costs, and fail to complete the transaction.

Bluecore’s app can detect that motive in the online behavior of the customer; it can also be set up to send an automated, personalized response that, say, offers to waive shipping costs. According to Bluecore cofounder and CTO Mahmoud Arram, the ability to track security was a critical factor in the company’s use of cloud computing—in this case, of Google Cloud Platform.



*"One of our customers needed confirmation of certain levels of security, and we were able to show them that we could meet their security requirements," he says, in a report that Google produced. "It made me realize that if we were running our own data center, we probably would have run into trouble in that regard." —Mahmoud Arram, Bluecore co-founder and CTO*

Most significantly, a cloud-based system proposes huge enhancements in a company's potential to counter cyber-threats because of its method to responds to incursion. A usual cyber-attack initiates with a hacker identifying a susceptibility in a company's network or systems that permits the interloper to send malware on a computing device.

It may be possible that the malware has never been seen before. It is extremely tough to uncover; the so-called command and control computer that organize it and obtains information from it could be detected anywhere across the world.

The malware is devised to convey through the IT systems of an organization, profiling their data structures and the information they accumulate, and then to eliminate any valued data it finds, conveying it to the command-and-control hardware.

By the time a cyber-attack is being identified in a typical computer system of an organization, the security technologies have now been unsuccessful in at least three ways.

The perimeter technology flopped to carry out the unauthorized activity; the network technology unsuccessful to identify the ongoing communications between the command-and-control computer and the infested endpoints; and the end-point technology flopped to look for the malware as well as the apprehensive behavior happening among the network, endpoint, and perimeter.

### **3.9. PRIVACY-PRESERVATION FOR SENSITIVE DATA IN CLOUD COMPUTING**

It is generally seen that over a period of time, organizations have collected key information about the people in our societies that contain sensitive information, for instance: medical information. Researchers need to analyze

and access such information with the help of big data technologies in cloud computing, while companies are needed to impose data protection compliance (Figure 3.8).



**Figure 3.8.** *Cloud computing privacy challenge.*

Source: Image by GeeksforGeeks.

It was observed that within the past few years, there has been progress witnessed on privacy preservation for sensitive data in both academia as well as industry context, e.g., solutions that develop tools and protocols for encryption or anonymization of data for discretion purposes.

This section classifies effort in context to this area with reference to distinctive privacy protection requirements. Although, these clarifications have not yet been extensively espoused by any organizations or cloud service providers. Pearson discusses a range of privacy and security challenges that are elevated by cloud computing.

Lack of user control, lack of expertise and training, complicated of regulatory compliance, illicit secondary usage, transborder data flow litigation and restrictions are among the challenges faced in cloud computing environments.

The privacy challenges of health-related data in the cloud embracing terms of services of cloud providers that are not advanced with a healthcare mindset, consciousness of patient to upload their data into the cloud without their approval, data monitoring, multi-tenancy, data accountability and security.

The concept of “outsourcing privacy” refers to a place where a database owner updates the database over regular intervals on untrusted servers. This definition takes into consideration that database clients as well as the untrusted servers are not able to grab anything about the matters of the databases without official access.

The authors execute a server-side indexing structure in order to create a system that permits a single database owner to efficiently and privately write data to, and numerous database clients to confidentially access data from, an outsourced database.

Homomorphic encryption is another privacy-preserving solution that is relied on the notion of computing over encrypted data without awareness that the keys belonging to distinctive parties. In order to privacy, the owner of data may encrypt data having a public key and accumulate data in the cloud.

When the process engine interprets the data, there is no necessity to possess DP’s private key in order to decrypt the data. During the time of private computation on encrypted genomic data, there is a need to propose a privacy-preserving model in a way to process genomic data using homomorphic encryption on genome-wide association studies.

Anonymization refers to another method which is widely used in order to ensure the privacy of sensitive data. SAIL offers discrete information on the accessibility of data types within a collection. Researchers are not able to cross-link (which is related to an equality join in SQL) data from distinctive outside studies, as the individualities of the samples are anonymized.

One of the other possible ways that can be adopted is an integration architecture to make the way to engage in aggregated queries over anonymized medical data sets from distinctive data providers. In such a scenario, data providers eradicate the data subjects’ identifiers and employ a two-level encryption with the help of PKI and hashing certificates.

The critical information and data will then be anonymized using an open-source toolkit and will be encoded granularly using the public key provided by the cloud service provider. ScaBIA is another widely used solution that is helpful in processing and storing anonymized brain imaging data in the cloud.

This tactic enables PKI authentication for manager roles to employ a PaaS middleware and outlines researchers as users in the Microsoft Azure cloud. Researchers are enabled with the opportunity to login by using

username and password to run statistical parametric mapping workflows within isolated generic worker containers.

The brain imaging datasets and associated outcomes can be shared by the researchers with the help of a RBAC model over secure HTTPS (hypertext transfer protocol secure) connections. The design and execution of a security framework for BiobankCloud, a platform that backs the secure administering and storage of genomic data in cloud computing environments, play an important role in preserving privacy.

The proposed framework is framed on the basis of cloud privacy threat modeling approach, which is used to outline the privacy threat model for handling contemporary sequencing data according to the DPD. This solution basically comprises of an RBAC access control mechanism and flexible two-factor authentication (2FA), along with auditing mechanisms to ensure that the necessities of the DPD are achieved.

### **3.10. CONCLUSION**

At the end, it is concluded that application safety in cloud network is one of the most important segments that should be taken into consideration by every organization. With the increase in the attacks and entrance into the cloud network by invaders, resulting in loss of sensitive data, it becomes more important to add an extra layer of security into the cloud network structure.

Nowadays, it is almost impossible to carry out all the organization operations offline, as the majority of the activities are now functioning online. Therefore, having the safety of cloud network is utmost important.

In addition, it is often seen that sensitive information of the company is stored online. This information is very critical from the perspective of the company. Compromising with this information would provide huge loss to the company, and if such valuable information will get into the hands of competitors, then it will not be good for the long-term survival of the company. Therefore, investing in the highly secure network is far better than feeling grave when data is sacrificed.

Furthermore, one cannot deny the fact that there is a lot of vulnerability in the cloud network. It is essential to engage in policy and decision making for the design of the cloud network structure in such a way in order to make it less vulnerable. With the speed at which advancement in technology is



going on, it is expected that the security of the cloud network will increase in the future.

But, at the same time, it is also possible that the ways and means adopted by the attackers will also be advanced, therefore looking for making they could network safe is a continuous process, and it will carry on till the trend of cloud network continues.



## REFERENCES

1. Archer, D., & Archer, T., (2016). *Safety in the Cloud*. [Online] Strategy+Business. Available at: <https://www.strategy-business.com/article/Safety-in-the-Cloud?gko=0ceeb> (accessed on 1 April 2021).
2. Assaraf, N., (2015). *Five Safety Concerns with Cloud Data Storage, Answered*. [Online] cloudHQ Blog. Available at: <https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/> (accessed on 1 April 2021).
3. Blog.avast.com. (2020). *Data Security Issues in Cloud Computing | Avast*. [Online] Available at: <https://blog.avast.com/data-security-issues-in-cloud-computing> (accessed on 1 April 2021).
4. Boyd, N., (2018). *Eleven Critical Cloud Security Vulnerabilities*. [Online] [www.sdxcentral.com](http://www.sdxcentral.com). Available at: <https://www.sdxcentral.com/cloud/definitions/11-critical-cloud-security-vulnerabilities/> (accessed on 1 April 2021).
5. Boyd, N., (2021). *Security Tips: How to be Safe in Cloud Computing*. [Online] [www.sdxcentral.com](http://www.sdxcentral.com). Available at: <https://www.sdxcentral.com/cloud/definitions/safe-in-cloud-computing/> (accessed on 1 April 2021).
6. Businessnewsdaily.com. (2021). *Eight Reasons to Fear Cloud Computing*. [Online] Available at: <https://www.businessnewsdaily.com/5215-dangers-cloud-computing.html> (accessed on 1 April 2021).
7. Check Point Software, (2016). *What is Cloud Security? Understand The 6 Pillars | Check Point Software*. [Online] Available at: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/> (accessed on 1 April 2021).
8. D'Silva, F., (2020). *Six Tips for Improving Cloud Computing Security*. [Online] Ntiva.com. Available at: <https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security> (accessed on 1 April 2021).
9. Hein, D., (2019). *Seven Cloud Storage Security Risks You Need to Know About*. [Online] Best enterprise cloud strategy tools, vendors, managed service providers, MSP, and solutions. Available at: <https://solutionsreview.com/cloud-platforms/7-cloud-storage-security-risks-you-need-to-know-about/> (accessed on 1 April 2021).
10. InfoQ, (2019). *Understanding Cloud Computing Vulnerabilities*. [Online] Available at: <https://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities/> (accessed on 1 April 2021).

11. Izvercian, M., Ivascu, L., & Radu, A., (2021). *Using Cloud Computing in Occupational Risks*. [Online] [www.researchgate.net](http://www.researchgate.net). Available at: [https://www.researchgate.net/publication/281068669\\_Using\\_cloud\\_computing\\_in\\_occupational\\_risks](https://www.researchgate.net/publication/281068669_Using_cloud_computing_in_occupational_risks) (accessed on 1 April 2021).
12. ManagedMethods, (2018). *What is Cloud Application Security? | Managed Methods*. [Online] Available at: <https://managedmethods.com/blog/what-is-cloud-application-security/> (accessed on 1 April 2021).
13. ManagedMethods, (2021). *What is Cloud Application Security? | Managed Methods*. [Online] Available at: <https://managedmethods.com/blog/what-is-cloud-application-security/> (accessed on 1 April 2021).
14. Rafter, D., (2021). *Cloud Security: How Secure Is Cloud Data?* [Online] [Us.norton.com](http://Us.norton.com). Available at: <https://us.norton.com/internetsecurity-privacy-cloud-data-security.html> (accessed on 1 April 2021).
15. Safety Net, (2021). *Cloud Services | Managed Cloud, Data, and IT Solutions*. [Online] Available at: <https://www.safetynet-inc.com/it-consulting-and-projects/cloud-implementation-services/> (accessed on 1 April 2021).
16. Zamora, W., (2018). *Should You Store Your Data in the Cloud?* *Malwarebytes Labs*. [Online] Malwarebytes Labs. Available at: <https://blog.malwarebytes.com/101/2016/04/should-you-store-your-data-in-the-cloud/> (accessed on 1 April 2021).

## CHAPTER 4

# Introduction to Internet of Things (IoT) Security and Its Open Challenges

## CONTENTS

4.1. Introduction.....	102
4.2. What Is IoT?.....	103
4.3. Security Role in the IoT Development.....	105
4.4. IoT Architecture .....	107
4.5. The Importance of IoT Security .....	108
4.6. Essential Focus Areas for IoT Security.....	109
4.7. How to Ensure Your IoT System Is Secure? .....	112
4.8. Trust, Data Confidentiality, and Privacy In IoT.....	113
4.9. Biggest Security Challenges for IoT .....	118
4.10. Future of IoT .....	123
4.11. Conclusion .....	126
References .....	127

IoT is nowadays one of the most popular areas gaining traction everywhere in the world. In this chapter, basic IoT concepts are discussed. The chapter also explains both the role of security in IoT development and IoT architecture. In addition to that, the chapter highlights the importance of IoT security. Several examples related of IoT security breaches are discussed. The chapter also provides practical and actionable tips to ensure that your IoT system is secure. Some relevant concepts that are explored in this chapter include trust, data confidentiality, and privacy. Furthermore, several biggest security challenges for IoT are also demonstrated. In the end, the possible future of the IoT is highlighted.

## 4.1. INTRODUCTION

IoT is an emerging technology that emphasizes on inter-connection between things or devices to each other and to users or humans in order to attain a common objective. IoT is driven by several prevailing technologies such as radio frequency identification (RFID) and wireless sensor and actuator networks (WSAN). The idea of IoT was first envisaged by Kevin Ashton of Auto ID-Centre MIT.

Because of the widespread of the internet availability across the world in the form of Wi-Fi, mobile data networks services (3G, 4G LTE), universal sensing has been already apparent. Consequently, it provides the opportunity for various devices to connect with each other and to the users that would eventually contribute to the smart cities in the future. It is expected that a present number of connected devices would likely to increase in the future to a greater extent, reaching between 50 and 100 billion by the year 2020.

This huge number of connected devices would yield universal sensing and extensive availability of services. In the IoT paradigm, the information and communication systems will be effortlessly integrated into our environment. Subsequently, processing, and sensing several physical phenomena and amassing the information on remote clouds. IoT is an integral part of creating smart homes, smart healthcare system as well as smart cities.

It is right to assume that IoT will be widely adopted if it successfully gained the trust of users by providing sturdier security and privacy.

In the present era, IoT security is a popular research topic and is gradually gaining more acceptance. Several researchers from all over the world are putting their maximum efforts and are collaborating on various platforms to address numerous security challenges in IoT.

However, IoT security is a significant challenge because of its complexity in nature. IoT is the combination of a variety of technologies, all of these technologies have their own set of security and privacy flaws that are need to be addressed with reference to the IoT.

It is important to note that the existing IoT infrastructure is significantly vulnerable to widely popular security attacks such as denial of service (DoS), Man in the middle, replay attacks, cloning of things, routing attack and eavesdropping are identified in. Atamli et al. categorized some IoT specific cyber-attacks such as privacy breach, device tampering, DoS, information disclosure, signal injection, Spoofing, and side-channel attack.

IoT devices are resource confined, and existing cryptographic security solutions cannot be executed to these devices, which makes it vulnerable to confidentiality and data integrity problems. In addition, with exposure to DoS attacks, the three security goals, i.e., integrity, confidentiality, and accessibility is inflexible to accomplish. The difficulties to traditional security solutions in IoT are conferred in this chapter in details.

Access control mechanism and device authentication is also a major security issue in IoT. Access control and authentication problems in IoT are because of a high number of digital devices and machine to machine (M2M) communication nature of IoT. There are some of the existing recommended techniques for access control and device authentication that are explained in detail.

It is important to note that IoT can be put into a variety of usage such as smart cities, smart home, smart healthcare system, connected vehicles, intelligent traffic control lights, smart grids, smart environment watching in industries, water network monitoring, smart metering, and smart logistics and many more. The IoT has wider scope and is not confined to the aforementioned applications. In this chapter, some of the security problems are discussed that can be applied to all application domains of IoT.

## 4.2. WHAT IS IOT?

The IoT concept was initiated by Kevin Ashton, a co-founder of the Auto-ID Centre at MIT, in the year 1998. The primary objective of that objects (“things”) is linked to each other, and thereby they create IoT in which each object has its distinctive uniqueness and can interconnect with other objects. IoT objects can differ severely in size from a little smart band to a cruise ship (Figure 4.1).



**Figure 4.1.** *Connected devices in IoT.*

Source: Image by Medium.

IoT is concerned with the transformation of common products such as buildings, cars, and machines into smart, digital, and connected objects that can interconnect with applications, people, and each other.

There are several definitions of IoT. The International Telecommunication Union (ITU) outlined the term IoT as “IoT will connect the world’s objects in both a sensory and intelligent manner.”

In the year 2014, the International Electrotechnical Commission (IEC) and the Joint Technical Committee of the International Organization for Standardization (ISO) outlined IoT as “an infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.”

At the IoT reception layer, sensors are placed between objects and devices in order to collect, evaluate, and record information about the physical environment, such as humidity, temperature, motion, or gas pressure. This information can be read, unified, and interpreted by higher IoT layers.

NIST uses two acronyms, IoT, and NoT (network of things). IoT is usually conceived as a subset of NoT because IoT has its “things” connected to the Internet. In contrast, some sorts of NoT only make use of local area networks (LAN), with none of their “things” connected to the Internet.

The IoT progress is compelled by commercial needs as part of enterprise digital transformation. According to a research conducted by Machina, it was estimated that the total number of IoT connections will flourish from 6 billion in the year 2015 to 27 billion by the year 2025.

It means a compound annual growth rate (CAGR) of 16%. In terms of market growth, the report by Berg Insight indicates that a surge of the global third-party IoT platform market from €610 million in 2015 to €3.05 billion by the year 2021.

IoT solutions not only comprise numerous technology domains such as cloud, mobile communications, data, telecommunications, security, and networking, but they also conducive to cross-industrial use of data (for instance, data produced in smart home and industrial applications can be applicable in the automotive domain).

It opens the pathways for founding corporate partnerships between vertical industries, such as car manufacturers, and horizontal industries, such as telecommunication operators, as new business models. Digital transformation of business empowered by IoT is much more than just using connected objects-it makes it probable to cultivate innovative business models that were difficult before.

### **4.3. SECURITY ROLE IN THE IOT DEVELOPMENT**

As outlined above, IoT is growing at a rapid rate across several industry verticals along with surges in the sum of interconnected devices and diversity of IoT applications. However, IoT technologies are not fully mellow yet, and there are several challenges that are need to be addressed. Security is the most critical of them.

It is worth noticing that there are billions of connected devices and sensors, and their numbers are rising at a greater rate. All of them demand reliable and secure connectivity. Hence, there is a need of elegant security IoT architectures by organizations and companies embracing IoT technologies.

Indeed, the threat in reference to the IoT threat is large and growing: the scope of attackers very huge, as any IoT device could be a probable attack target. Some IoT devices are positioned in untrusted areas, and attackers can get physical access to them and even can take full control of the device.

It is generally seen that majority of the IoT devices do not fulfill security finest practices requirements such as role-based or least-privileged access.

For instance, numerous smart-home IoT devices such as webcams, smart TVs, remote power outlets, home thermostats, home alarms, sprinkler controllers, door locks, and garage door openers establish communication with each other over the network without any form of encryption and do not provide the opportunity to the user to enable strong passwords.

IoT devices are resource-confined and are proposed with the aim to consume little power while in addition to this, ensures to provide all needed functionality at an economical cost. As a result, security is an after-thought, often positioned at the lowermost of the primacy list in the development lifecycle.

It is often seen that the vectors of IoT attack can target devices, SIM/cell, gateways, wearable, and transceivers, and can take benefit of weak passwords, backdoors, lack of encryption, etc.

The extensive diversity of IoT-specific operating systems, custom configurations, and firmware versions makes expansion of general IoT security solutions challenging. Patching and monitoring the diverse IoT OSes is a wonderful challenge. Furthermore, IoT security solutions should be tremendously scalable to pertain to an exponentially growing number of various IoT devices.

A rising variety of IoT applications throw potential security challenges. Apart from the traditional security domains such as secure communication, cryptography, and privacy assurances, IoT security also emphasizes on identity/trust management, privacy protection, and data confidentiality, etc.



## **4.4. IOT ARCHITECTURE**

It is well known that IoT will archetype the world in near future and will make the life of the human easy to a greater extent. Though, its security is very challenging and because of its wide deployment, heterogeneous nature, resource-restricted nodes and generation of massive amount of data every second. IoT network architecture comprises of four layers.

However, this is not a standard architecture for IoT, majority of the proposed architectures have these layers. Therefore, we take into consideration this architecture as our reference architecture for classifying and identifying diverse security problems in IoT. The different layers in IoT are:

### **4.4.1. Perceptual Layer**

This layer generally comprises of devices such as RFID and sensors that intellect any real-world physical phenomenon such as weather condition, RFID tags, and water level in the agriculture field. Actuator Networks and Wireless Sensor and RFID are the certain critical elements of this layer.

### **4.4.2. Network Layer**

This layer securely conveys the information assimilated by perceptual layer sensor devices to fog nodes, chief cloud or straightforwardly to another IoT node. Diverse technologies at this layer are Satellite networks, mobile networks, Wireless Ad hoc network, and many secure communication protocols used in these technologies.

### **4.4.3. Support Layer**

It is often seen that support layer offers an effective and feasible platform for IoT applications. Different IoT applications can be introduced on fog nodes or chief cloud and is manageable through internet by the resource reserved devices. It provides computing and storage power to the resource-constrained devices.

### **4.4.4. Application Layer**

This layer is basically concerned with ensuring that all the users will get IoT services according to their needs. Users are facilitated with several services using the Application layer interface. Different applications are smart

healthcare systems, smart homes, intelligent transportation, automated vehicles, smart agriculture, and many more.

## 4.5. THE IMPORTANCE OF IOT SECURITY

It is important to note that security affects more facets of an IoT system than several people recognize. It influences the strategy of each component and also raises privacy concerns that should be taken into consideration distinctly from security concerns (Figure 4.2).



**Figure 4.2.** *Importance of IoT.*

Source: Image by Information Age.

For instance, one can install a security system that is not possible to hack, but through standard usage of the system, users may be revealing their critical information and data.

Let us look at a smartphone as an example. It persistently tracks the location of a person and sharing that info to developers of both the owner of mobile phone companies and several apps that use your location. Everyone wants to keep their information safe and reluctant to share with anybody without their knowledge.

### 4.5.1. Examples of IoT Security Breaches

It is well known that Failure to appropriately address security in linked systems has already had grave real-life problems, and several examples that were relevant from this context are discussed as follows:

- Stuxnet is a widely known computer worm that focuses on SCADA systems. It's assumed to have tumbledown almost 20% of Iran's nuclear centrifuges in the year 2010. It infected more than 200,000 computers and caused almost 1,000 machines to physically degrade.
- At the German steel mill, installed systems were compromised by attackers who made it terrible to shut off the blast furnace, resulting in dramatic heat damage to equipment.
- Attackers gaining authorization to an oil rig at sea and tilted it drastically, positioning it out of commission. The owners had to bear huge downtime costs for restorations.
- In one of the most widely known security breaches, the Nissan Leaf car was compromised, permitting remote operatives to control the heating system of the car. It resulted in significant consumption of battery charge, potentially leaving drivers stranded.
- One of the biggest security breaches involving connected hardware devices was the Mirai botnet attack. It infected unsecured IoT devices (mostly IP cameras as well as wireless routers) with a perverse program that directed them to engage in a coordinated attack against a core part of internet infrastructure. This brought down highly busy websites including GitHub, Twitter, Reddit, and many others for substantial periods of time.

## 4.6. ESSENTIAL FOCUS AREAS FOR IOT SECURITY

It is important to note that a high proportion of these attacks could have been averted if the IoT systems in question had safeguarded the below given five effort areas.

Some of the critical areas in which security play a very important role while designing and building IoT systems (Figure 4.3).



**Figure 4.3.** *IoT in a smart home.*

Source: Image by 123RF.

#### 4.6.1. Device/Hardware Security

There are several attacks that can be initiated by the attackers if physical access to a device or piece of hardware is attained.

For instance, systems can be put down or offline, devices can be reprogrammed, destroyed, or enlisted in a botnet, and critical information can be pilfered. It is often seen that such types of attacks leave no trace but exposes a person to a subsequent attack based on the sensitivity of the data stolen.

### **4.6.2. Data Security**

Data security is basically concerned with ensuring that data is not conveyed from a device to the internet in its simple practice but is rather encrypted. It means that even the information is exposed to the attacker, it will be useless to them.

In addition, multi-factor verification can also be taken into consideration as it helps in providing an extra layer of protection for sensitive data transactions.

### **4.6.3. Network Security**

One of the widely known attack that can arise in this area is known as a 'man in the middle' attack. In this state, the attacker does not reveal their true identity. Instead, they interrupt communications between two users of a system and change those communications for their own advantage. In the interim, both original parties believe that they are communicating straightforwardly.

### **4.6.4. Operating System Security**

The remote servers that linked devices communicate with are most likely operating on popular systems such as Microsoft software or Linux. Because of their reputation, these operating systems are usually at the target attackers, keeping an eye on the vulnerability of the system.

Patches to these operating systems are disseminated steadily and should be implemented in a way to make sure that a system will remain secure for a certain period of time. Due to this, it is highly important for companies to prefer an IoT platform having OTA (Over the Air) update characteristics so that their clients do not need to eliminate all of their hardware from the field.

### **4.6.5. Server Software Security**

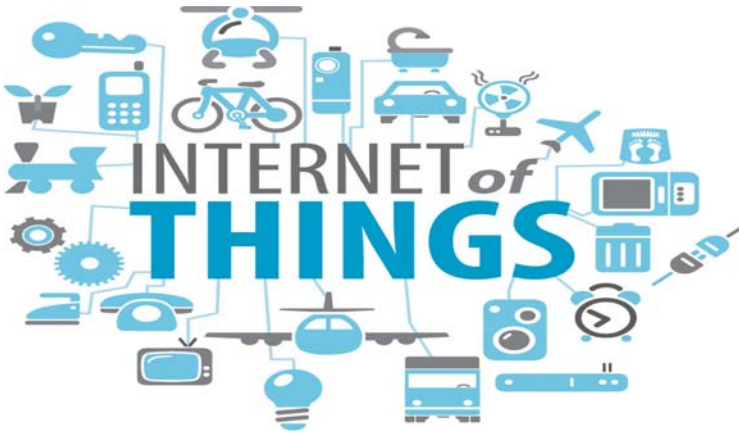
It is often seen the majority of the servers run on other software as well apart from their own operating system. For instance, they could be running a Linux operating system and a web server from an entirely distinctive software provider.

The same recommendation valid at operating systems is also applicable to any other piece of software operating on a server. It is imperative to apply

patches consistently to lessen the threat of security exposure. In addition, over-the-air OTA update facility make this process much simpler.

## 4.7. HOW TO ENSURE YOUR IOT SYSTEM IS SECURE?

It is often seen that the scope of attack in any software system is huge, and it only gets higher with the involvement of physical components into the picture (Figure 4.4).



**Figure 4.4.** *IoT security and privacy.*

Source: Image by Pinterest.

As far as the things that have observed so far, it was found that security can often be too greater an area for anyone business to entirely master themselves.

One positive news is that one can efficiently outsource several aspects of security to the equipment producers and service providers of cloud that one selects. It means that one should include security as a characteristic that can be taken into consideration while evaluating any service or product that is likely to play an imperative role in the connected system that one is building.

As it is well known that security is such a multifaceted topic, and one cannot make sure that no susceptibilities will ever arise. Therefore, it is always recommended to design and structure system in such a way that even it become compromised, then it's possible for one to recover without having to entirely redeploy all physical devices available.

For instance, whether it is needed to alter the password on a web browser with which a number of devices are connected. The best way is to never store that password on any internet platform or even in the devices themselves.

Software platforms such as Kosmos help managing credentials for situations like this and also provide OTA potentials for remotely renewing the code on a fleet of devices so that there is no need to physically touch the devices during the process of changing their behavior.

Lastly, when making buying decisions related to MCUs that have substantial market share and are used in several associated systems, make sure to alteration the default username and password that comes with them. It was an extensive failure to do so that contribute to the Mirai botnet attack stated previously.

## **4.8. TRUST, DATA CONFIDENTIALITY, AND PRIVACY IN IOT**

### **4.8.1. Trust in IoT**

It is generally seen that trust and security in IoT are based on credentials or tokens, postulated by a trust management infrastructure, which are rooted in and possibly shared between devices. These tokens can be digital certificates or symmetric keys.

They play a very vital role in deflecting external attacks inducted by entities that are not in control of credentials but collapse to avert internal attacks, where nodes or credentials that own credentials have been compromised.

Public key infrastructure (PKI) is the one which play a key role in generating and controlling certificates. In some security-sensitive environments, the trusted platform modules known as TPM are used, that facilitates a hardware-based root of faith and a high level of assurance that the identity attributes delivered belong to the particular device. As IoT is a dynamic system, processes to attest the reliability of IoT components throughout their existence are needed.

IoT devices are susceptible in many facets, so one can say that the trust management for them is a tough endeavor. A key setback associated with trustworthy firmware is that many entrenched processors (even if they function under a contemporary multitasking operating system) do not provide process encapsulation through memory virtualization.



As a result of, malicious code in a firmware image can attain and manipulate credentials used by other system processes to originate an internal attack. Hence, interpreting the credibility of firmware components independently is not adequate and the firmware image as a whole must be authenticated.

Devices with a static (“factory-flashed”) firmware image can sustain a greater level of credibility over time in comparison with the devices that are modernized gradually in the field through firmware download because the upload mechanism itself can have a prospective back door for attacks.

A secure device patching mechanism or firmware updating is a central element to conserve security. A network-wide update mechanism is required to embrace authenticity checks, robust integrity and curtail service outages, and permit for a type rollback if required.

Any trust management system for IoT deployments must have the ability to dynamically withdraw trust of individual devices. In a similar way, individual devices must be able to dynamically certify the reliability of other nodes they communicate with Secure Key Storage and Trust.

It is important to note that the robustness of trust tokens can be amplified by making use of keystores. A keystore – either a file (software stores) or a hardware device (hardware stores) – play a dominant role in providing storage for keys.

In the case of passive keystores that firmly recover and save credentials, operations related to cryptographic are fulfilled outside these stores by the CPU of the concerned device. In contrast, active keystores permit internal implementation of cryptographic operations through an application program interface (API), in order to make sure that credentials would never be exposed. Several categories of key stores are discussed as follows:

- **Hardware Stores:** The present-day cryptosystems make use of hardware security modules (HSMs). These specified tamper-resistant devices are made into use for handling cryptographic keys. General-purpose HSMs delivers a safe, secure, and usually configurable administration.

One of the major drawbacks of this is its lack of flexibility if rare token algorithms or setups are used. Cryptographic USB dongles and Cryptographic smart cards (embedded or otherwise) are economical HSMs. They are chiefly suitable for resource-restricted nodes or economical trust management infrastructures.



- **Trusted Platform Modules (TPMs):** TPMs, which is established by the Trusted Computing Group are committed microcontrollers or can be executed within devices such as memories.

Their primary goal is to guard hardware (by authenticating devices), booting processes, and so on. Secret data such as encryption keys are stored securely on the TPM by hashing. By ensuring the means to confirm that a platform will behave as it should, the TPM helps in establishing a hardware root of trust.

- **Software Stores:** The normal place for software keystores is in devices having low security necessities or economical embedded systems that have no necessities to tangibly interlink to hardware modules. There are a huge number of passive and active software stores that can be employed in IoT systems.

For instance, the homonymous public-key cryptography standard (PKCS) originally outlined by RSA Security (now part of Dell EMC) is used in PKCS#12 software stores. In principle, PKCS#12 outlines two categories of privacy/integrity modes; password-based and asymmetric cryptography.

Java stores are segment of a much extensive programming framework, the Java cryptography extension/Java cryptography architecture (JCE/JCA). This framework outlined a provider-based, pluggable architecture that embraces, among many other items, Keystore implementations.

- **Identity Management:** Current identity and access management (IAM) solutions in IoT are restricted in their potential to amend to storing entities and identities on a sizeable scale. This restriction has stemmed to a shortage of application integration layers for IoT-based applications. In the current scenario, there is existence of no overall framework that can help in discovering and managing IoT entities and their characteristics across distinctive solutions.

The distinctive approach is to deliver restricted access on the basis of an expected role instead of least-privileged access in conventional IAM systems. Consequently, authentication from a similar device may offer distinctive access potentials on the basis of how the user has validated to the device. IoT will require conventional IAM systems to embrace M2M entities. Overall, IAM platforms are required to be modified in a way to cover identity in IoT-based systems.

### 4.8.2. Data Confidentiality in IoT

The data a node receives or sends can be reliable if its integrity, optionally in amalgamation with data privacy via symmetric encryption (using the advanced encryption standard (AES) algorithm as a de facto industry standard), is guaranteed.

For instance, in a body area network, a wireless glucometer transmits glucose readings to an integrated insulin pump. This information should be safeguarded from intentionally tampering, or accidentally and patient privacy concerns necessitate the data to be encrypted.

However, there are several confronts of cryptography on devices with reserved resources, for instance, 8-bit microcontrollers with restricted RAM. Encryption is generally executed directly in hardware, while data integrity is delivered via cryptographic hashes or message authentication codes that are ascribed to the data payload.

For determining peer authenticity, a peer should be able to authenticate another peer's identity before establishment of a communication link. Coming back to the above case of an insulin pump, the pump should be able to authenticate that it essentially links to a trusted glucometer (and consequently receives data from it) and not to a malicious device.

Authorization proof provides a guarantee that a peer has the authority to (a) establish a connection with another peer and (b) engage in a certain course of activity. In our instance, a glucometer admits only data requests from an insulin pump (and not from the blood pressure monitor).

Moreover, both pump and glucometer must be from the identical manufacturer; and a reset command propelled to the glucometer sensor through the insulin pump (after a sensor reconfiguration) should only be implemented if the insulin pump fulfill the needed authorization level.

### 4.8.3. Privacy in IoT

It is often seen that ensuing privacy in IoT is still a major challenge. Privacy basically comprises of security of personal information as well as the potential to manage what happens to this information. Privacy issues with reference to the IoT systems are intricate because of the fact that a system is more than the computation of its parts.

Privacy considerations for low-level devices may vary from the distresses produced at data analytics or an application level. In addition, breach of privacy at any level in the system impact the entire system.

A huge amount of private information can be amassed from the smart devices. Making control of this information is a challenging task in an existing IoT techniques. In majority of the instances, data is collected inertly and due to some privacy breaches can go unobserved for a significant period of time.

The question about ownership of IoT data—who owns which data and who governs where data goes—creates chief concerns from ethical, regulatory, and financial standpoints. End users are of the opinion that they own all the data.

The original equipment manufacturers believe they own, or at least have the full rights to make use of the data generated from their side. The service providers in the majority of the instances opines they own the data, just like what application providers think.

Issues of data ownership become progressively complex as more heterogeneous IoT systems with more players from differing organizations are positioned. Neutralized conventional devices can still keep a lot of privacy-sensitive information and data sanitization should be done for them.

Apparently, cordial combinations of IoT data streams from several bases can endanger privacy. For instance, a user's toothbrush empowered with network might seize and convey harmless data about a person's brushing habits.

However, if user's fitness-tracking device transfers their activity data, the accumulation of these data streams provides a much comprehensive description and private information of the person's overall health. In few instances, the user might not be even cognizant that an IoT device is amassing data about him or his family members and possibly distributing it with third parties.

This kind of accumulation of data is becoming more rampant in consumer electronic/digital devices such as intelligent personal assistants and smart TVs. These devices have voice vision features or recognition that permit them to constantly listen to discussions or keep an eye on what is happening in a room and selectively transmit that data to a cloud service for administering, which sometimes comprises third party. People might be in the company of such devices without even conscious that their activities or conversation are being recorded or monitored.

It is generally seen that privacy-enhancing techniques are mostly deficient in data analytics and are swapped by non-technical means such as

SLAs and other customer agreements to ensure data processing in obedience with legal regulations that can have major regional disparities.

## **4.9. BIGGEST SECURITY CHALLENGES FOR IOT**

The global IoT market is expected to reach a value of USD 1,386.06 billion by 2026 from USD 761.4 billion in 2020 at a CAGR of 10.53%, during the period 2021–2026.

This increase in the popularity of IoT-connected devices will come along with a fair share of concerns and security challenges. As manufacturers will likely to compete to provide advanced and modern devices in the hand of consumers, very few of them are focusing on the security issues and challenges associated with data access and management as well as with that of the IoT devices themselves. But what is the chief security challenges presently troubling the field of IoT-connected devices?

### **4.9.1. Insufficient Testing and Updating**

Currently, there are almost 23 billion IoT connected devices across the world. It is expected that this number will likely to reach over 60 billion by the end of 2025. This huge wave of new digital devices does not come without a cost.

In fact, one of the major concerns with tech companies manufacturing these devices is that they are too casual when it comes to managing of risks related to device security.

It is often seen that many of these devices and IoT products do not get regular updates and security patches while, some don't even get any updates. This means that a device when it was initially purchased by a customer thinking that it is fully secure becomes insecure after some period of time and ultimately susceptible to hackers and other security issues.

Early computer systems faced such sort of problem, which was to some extent solved with automatic updates. However, IoT manufacturers are keener to manufacture and sell their devices as possible as possible without even thinking about security and update feature.

Unfortunately, Majority of the manufacturers offer firmware updates only for a shorter period of time, until the latest update model come into the market. Even worse, they use unsupported legacy Linux kernels. It resulted in propelling their trusted customers to the hands of potential attackers as a result of outdated software and hardware.

To protect the customers against these attacks, manufacturers are need to proper test each device before being launched into the market and companies should update them regularly before any mischief. Incapability to do so is worse for both the companies and their consumers as well, as it only takes a solo large-scale breach in consumer data to entirely devastate the company.

#### **4.9.2. Brute-Forcing and Problems with Default Passwords**

The Mirai botnet, used in some of the major and most troublesome DDoS attacks is conceivably one of the finest instances of the concerns that come with delivery devices with default passwords and not telling consumers to alter them as quickly as they obtain them.

There are certain government reports that provides recommendation to the manufacturers to note sell the IoT devices that come with default (read, hackable) credentials such as using “admin” as username and/or passwords. That said, these are nothing more than guidelines now, and there are not any legal consequences to encourage manufacturers to drop this unsafe practice.

Weak login password and credentials details leave almost all IoT devices susceptible to password hacking and brute-forcing in specific. One of the key reasons why Mirai malware was so popular is that it recognized susceptible IoT devices and made use of default usernames and passwords to log in and defile them.

Thus, any origination that made use of factory default credentials on their devices is putting both their company and its assets and the clients and their crucial data at jeopardy of being vulnerable to a brute-force attack.

#### **4.9.3. IoT Malware and Ransomware**

As the number of IoT connected devices will continue to surge in the coming years, so will the number of ransomware and malware used to exploit them.

While the conventional ransomware dependent on encryption to entirely lockout users out of distinctive platforms and devices, there is an ongoing hybridization of both ransomware and malware strains that purposes to combine the diverse types of attack.

The ransomware attacks could possibly emphasize on constricting or deactivating device functionality and embezzling user data at the same time. For instance, a simple IP camera is perfect for apprehending delicate information and data using a wide array of locations, including work office address, home address, or even the local gas station.

The webcam can then be protected and footage channeled to an infected web address that could abstract delicate information with the help of malware access point and demand payoff to unlock the device and return the data. The steadily increase in the number of IoT devices will give birth to instability with respect to the future attack permutations.

#### **4.9.4. IoT Cryptocurrency Botnets**

The heated mining competition, accompanied with the recent surge in cryptocurrency estimations, is proving too tempting for hackers wanting to cash in on the crypto craze. While the majority of the current blockchain platforms have robust cybersecurity measures, the potential attacks in the blockchain sectors have been continuously increasing.

The key susceptibility is not the blockchain itself, but instead the blockchain app development based on it. Social engineering is extensively being used by the hackers to obtain passwords, usernames, and the private keys, with which one can easily gain access to the account of a person.

All such methods to hack accounts of individuals will continue to increase in the future to hack blockchain-based apps. Open-source cryptocurrency called Monero is one such example of several digital currencies currently being mined with IoT devices. It was found that few hackers have even repurposed IP and video cameras to mine crypto.

Blockchain breaches, IoT botnet miners and manipulation of data integrity poses a major threat for flooding the open crypto-market and interrupting already unstable value and arrangement of cryptocurrencies. IoT applications, platforms, and structures dependent on technology need to be fully controlled and persistently scrutinized and updated if it were to avert any future cryptocurrency misuses.

#### **4.9.5. Data Security and Privacy Concerns (Mobile, Web, Cloud)**

It is important to note that data privacy and security will likely be the single largest topics in today's interrelated world. Data is persistently being transmitted, harnessed, stored, and handled by large companies using an extensive array of IoT devices, such as speakers, smart TVs, and lighting systems, HVAC systems, connected printers, and smart thermostats.

Normally, the user data is distributed between or even traded to several companies, disrupting our rights for Data security and privacy, and further

driving public distrust. There is a need to execute high standard privacy and compliance rules that anonymize and redact sensitive data before disassociating and amassing IoT data payloads from info that can be used to directly identify us.

Cached and unrequired needed data should then be disposed of securely. If the data is saved, then the greatest challenge agrees with various regulatory and legal structures. The same preparation should be used with web, mobile, and cloud services and applications used to manage, access, and process data associated with IoT devices.

Secure development of web-based IoT applications and mobile app can be rather challenging for small companies with restricted manpower and budgets. As discussed above, the majority of the manufacturers tend to emphasis exclusively on attaining the device and app on the market fast to entice even additional funding and start raising their user base.

Unless a person needs to take a risk of a major breach of security, which may result in ruining of a brand trustworthiness and authority, then one need to consider going through a directory of web development and mobile-based companies and find the adequate one to help one's in ironing out the kinks that come with multi-layered data management and its security.

#### **4.9.6. Small IoT Attacks That Evade Detection**

The largest IoT-based botnet 2-years ago was the Mirai botnet. In 2017, it was the Reaper, a drastically more hazardous botnet than the famed Mirai. As significant as extensive attacks can be, what we should be dreading in 2018 are the small-scale attacks that avoid out detection.

We are certain to see a large number of micro-breaches tumbling through the security net in the coming few years. Rather than triggering the big guns, hackers will most probable be using subtle attack meager enough to let the information leak out rather than just grabbing millions and millions of records at once.

#### **4.9.7. AI and Automation**

It is well known that IoT devices will continue to dominate a person's day to day life. In addition to it, as far as companies are concerned, they have to deal with hundreds of thousands, if not millions, of IoT devices.

Such a huge amount of individual data would be challenging to manage from the perspective of network and needs data collection.



AI tools and automation are now being used to scrutinize through enormous amounts of data and could one day help IoT network security officers and administrators to administer data-specific rules and perceive inconsistent data and traffic patterns.

Although, autonomous systems that helps in making autonomous decisions and that affect millions of functions across sizable infrastructures such as power, healthcare, and transportation might be too risky, particularly when it is well known that a single error in the code or a misbehaving algorithm is enough to put down the entire infrastructure.

These are just a few of the critical IoT security challenges that need to be taken into consideration while building an app based on IoT platforms in the following years.

As it is clearly visible that, most of them revolve around two things, keeping IoT secure against attacks and keeping the user-data protected against theft.

Both challenges can be resolute with strict regulatory and legal frameworks in reference to the manufacturers, with hefty fines and working limitation used for those who do not follow these stated frameworks.

#### **4.9.8. Home Invasions**

One of the scariest dangers associated with using IoT devices is home invasion. IoT devices are being used at homes and offices in the context of home automation.

The security of these IoT devices is a serious concern. For instance, IoT devices can accidentally reveal their IP address or the actual residential address of their owner.

The user data can be sold by the hackers to the interested parties, which are havens for criminal outfits.

Moreover, if a person employed IoT devices in its security systems, then there is a huge chance that they might compromise as well as leave one's house at a gigantic potential threat.

#### **4.9.9. Remote Vehicle Access**

Apart from the home invasion, remote vehicle access is also one of the potential threats brought by using IoT devices in our lives. Smart cars are becoming more and more popular and majority of them are controlled by connected IoT devices. As a result, a bad actor can take over the IoT device



and hijack the car that the device is linked to. This can be a scary situation because the perpetrator may use the car for various purposes, including committing crimes. .

#### 4.9.10. Untrustworthy Communication

There are a number of IoT devices that conveys messages to the network without any encryption. This is one of the major of IoT security challenge that still exists. In order to avoid this challenge, the best solution is to use transport encryption and standards, such as TLS. Another useful method is to use distinctive networks that segregates different devices.

One can also make use of private communication that guarantees that the data being transmitted is confidential and secure.

### 4.10. FUTURE OF IOT

Presently, systems and objects are endowed with network connectivity and have the computing power in order to establish the communication with related connected devices and machines. Intensifying the network potentials to all probable physical locations will helps in making the life easy and at the same time helps in saving money and time. In addition, linking to the Internet also means to enhance the vulnerability of potential cyber threats (Figure 4.5).



**Figure 4.5.** *Future of IoT things.*

Source: Image by Data mining.

Internet empowered products usually catch the attention of cybercriminals. The growth of the IoT market escalates the number of potential risks that can impact the overall productivity and the safety of the devices and thus our privacy. According to a report aimed at shadowing the frequencies of data breaches, it was found that it has increased considerably since 2015; 60% in the USA only.

Another survey conducted in Canada, Japan, Australia, the UK, the USA, and France revealed that 63% of the IoT consumers think these devices are unnerving because of lack of adequate security. Research findings also noted that 90% of consumers are not assured with respect to the IoT cybersecurity.

Recent research discovered several innovative techniques to lessen the degree of cyber-attacks and escalate privacy solutions. Some of the solutions recognized through the research are discussed as follows:

- **Implementing Encryption Techniques:** Enforcing updated and sturdy encryption techniques can enhance the overall cybersecurity. The encryption protocol executed in both the device and cloud environments. Thus, hackers would not be able to comprehend the unreadable protected data formats, reducing the likelihood of misusing it.
- **Constant Research Concerning Emerging Threats:** The security risks are evaluated on a daily basis. Device manufacturers and several associated organizations developed many teams for security research. These teams are concerned with interpreting the impact of IoT threats and foster accurate control measures via continuous evaluation and testing.
- **Increase the Updates Frequency:** It is required from the side of device manufacturers to develop small patches instead of substantial updates. This kind of strategy would help in minimizing the complication of patch installation. Apart from this, regular updates will help the users in circumventing cyber threats resources from diverse sources.
- **Deploy Robust Device Monitoring Tools:** The majority of the present-day research suggested to execute robust device monitoring techniques, resulting in controlling and tracking suspicious activities effortlessly. Many IT organizations initiated proficient device monitoring tools in order to identify the potential threats. These tools are significantly important for risk assessment that supports the organizations in producing sophisticated control

mechanisms.

- **Develop Documented User Guidelines to Increase Security Awareness:** It is often seen that a major proportion of the IoT attacks and data breaches are due to a lack of awareness among users. Generally, IoT security measures and guidelines are not stated on the receipt or manual of purchased devices. If manufacturers of devices clearly state the potential IoT threats clearly, users can evade these issues if not completely then at least to some extent.

Organizations can also propose successful training programs to improve security consciousness among their clients. These types of programs will guide users about how to create strong passwords and recommend them to update them regularly.

Apart from this, users are educated to update security patches on a daily basis. The users also requested and aware to escape from spam emails, third-party applications, or sources that can compromise with the security of IoT.

It is expected that by 2025 there will be almost 30 billion IoT devices. At first, people were aware of the benefits of IoT devices but their adoption was initially slow and challenging. However, later, IoT technology began to grow rapidly and now we have many IoT success stories, including smart home IoT devices, such as lighting and intelligent thermostats to conserve energy.

In the field of urban development, IoT provides new ways and opportunities to manage the growth of cities and communities. For instance, IoT devices can efficiently manage traffic so that it flows freely, safely, and efficiently. This leads to less crowding, lower pollution levels, and more safety.

In health care, medical services are becoming more and more expensive and the number of chronic diseases is on the rise. Now, we are still in the period when many people lack access to even primary health care services even though some of those people will desperately need those services.

Even though the technology is not efficient in preventing the population from aging, it can be helpful to ensure economical healthcare and simpler accessibility.

For example, by conveying routine medical checks from the hospital to the patient's home, patients get greater accessibility of services. Ensuring

real-time monitoring with the help of devices linked to the IoT is one such way of saving lives of many patients.

On-time alerts are very significant at the time of life-threatening circumstances, as many medical IoT devices will likely to be connected with each other to accumulate crucial data for real-time tracking. It will help in improving the lives of patients to a greater extent.

## **4.11. CONCLUSION**

To sum up, it can be said that the craze of IoT will continue to increase in the future. With more and more companies are setting their operations online and because of recent coronavirus pandemic, majority of the tasks, whether it is education sector or service sector, transformed online.

So, for this reason, the chances of vulnerability will also increase as all the devices and data are connected with each other. Attackers are always looking for the opportunity to taken an entry into the system of users, resulted in compromising of the data which is private and confidential.

Keeping this thing in mind, it is utmost important to ensure security of the IoT. In addition, as nowadays all the devices are connected with each other, entrance onto one device by attackers may result in compromise the security of all systems. Therefore, it is highly significant for companies to implement several layers of IoT security.

In the future, the means adopted by attackers to take an entry into systems of users will increase, and so on the security and advanced software to enhance the IoT security.

## REFERENCES

1. Arxiv.org. (2016). *Internet of Things Security, Device Authentication and Access Control: A Review*. [Online] Available at: <https://arxiv.org/pdf/1901.07309.pdf> (accessed on 1 April 2021).
2. Balbix, (2018). *Addressing IoT Security Challenges | Balbix*. [Online] Available at: <https://www.balbix.com/insights/addressing-iot-security-challenges/> (accessed on 1 April 2021).
3. Banach, Z., (2020). *The Challenges of Ensuring IoT Security*. [Online] Netsparker.com. Available at: <https://www.netsparker.com/blog/web-security/the-challenges-of-ensuring-iot-security/> (accessed on 1 April 2021).
4. Carson, J., (2020). *Understanding the Needs of IoT Security*. [Online] Securitymagazine.com. Available at: <https://www.securitymagazine.com/articles/92704-understanding-the-needs-of-iot-security> (accessed on 1 April 2021).
5. Corser, G., (2019). *Why IoT Security is so Important- and What to do About it-Internet of Things News*. [Online] Internet of things news. Available at: <https://iottechnews.com/news/2017/aug/04/why-iot-security-so-important-and-what-do-about-it/> (accessed on 1 April 2021).
6. Corser, G., Fink, G. A., Bielby, M., Bielby, J., & Nighot, R., (2018). *Internet of Things (IoT) Security Best Practices*. [eBook] Available at: [https://internetinitiative.ieee.org/images/files/resources/white\\_papers/internet\\_of\\_things\\_may\\_2017.pdf](https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf) (accessed on 1 April 2021).
7. Designrush.com. (2021). *Seven IoT Security Issues and How to Protect Your Solution*. [Online] Available at: <https://www.designrush.com/trends/iot-security-issues> (accessed on 1 April 2021).
8. Gloukhovtsev, M., (2021). *IoT Security: Challenges, Solutions and Future Prospects*. [eBook] Orange business services. Available at: [https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS\\_Gloukhovtsev-IoT\\_Security\\_Challenges\\_Solutions\\_and\\_Future\\_Prospects.pdf](https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf) (accessed on 1 April 2021).
9. Hajdarbegovic, N., (2015). *Are we Creating an Insecure Internet of Things (IoT)? Security Challenges and Concerns*. [Online] Toptal Engineering Blog. Available at: <https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things> (accessed on 1 April 2021).
10. Hossain, M., Fotouhi, M., & Hasan, R., (2015). *Towards an Analysis*

- of Security Issues, Challenges, and Open Problems in the Internet of Things*. [Online] Ieeeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/document/7196499> (accessed on 1 April 2021).
11. Intellectsoft Blog, (2018). *Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying*. [Online] Available at: <https://www.intellectsoft.net/blog/biggest-iot-security-issues/> (accessed on 1 April 2021).
  12. Kimera, C., (2019). *Top 7 IoT Security Challenges*. [Online] clutch.co. Available at: [https://clutch.co/cloud/resources/top-7-iot-security-challenges?\\_\\_cf\\_chl\\_jschl\\_tk\\_\\_=592973f00e06091e69fdcdaced7c6514704011a6-1612173837-0-AXWMhkDxa1gWLT8Yn8qPoYBmIX1B\\_qPtjqfPJSL7pGE-10RTnKLsZX-kktjO8yEidDhr5B7RFLvhox8iNSzgLuf\\_ZxXBYs9iF-A7i46q2Cgbb0zBt2a0lodTrDF3b3Y0mS5yxZAdLmb5fVNCRRttk3KFqboahfp\\_Cyg56H\\_IHsWB0ildlwxaBkCgnBPf5nW\\_mP30NrLSbd7Qb19T8QFqPJkynROG3VnfkPA7F-6TiTQRJu9330LC8RCFVkBZBMDHHhFARvJ2nwE3fVNgKCZzbIBhJl89\\_WvMG6GGP1kr2\\_FNLpv-d-NiTlUVWqqLDIbeq4Scoocv2rIwdkFYfIHVFxSpLWu4f-Updk\\_4pR06O5wNn7b\\_BVpX3jUDbZBDCih7kng](https://clutch.co/cloud/resources/top-7-iot-security-challenges?__cf_chl_jschl_tk__=592973f00e06091e69fdcdaced7c6514704011a6-1612173837-0-AXWMhkDxa1gWLT8Yn8qPoYBmIX1B_qPtjqfPJSL7pGE-10RTnKLsZX-kktjO8yEidDhr5B7RFLvhox8iNSzgLuf_ZxXBYs9iF-A7i46q2Cgbb0zBt2a0lodTrDF3b3Y0mS5yxZAdLmb5fVNCRRttk3KFqboahfp_Cyg56H_IHsWB0ildlwxaBkCgnBPf5nW_mP30NrLSbd7Qb19T8QFqPJkynROG3VnfkPA7F-6TiTQRJu9330LC8RCFVkBZBMDHHhFARvJ2nwE3fVNgKCZzbIBhJl89_WvMG6GGP1kr2_FNLpv-d-NiTlUVWqqLDIbeq4Scoocv2rIwdkFYfIHVFxSpLWu4f-Updk_4pR06O5wNn7b_BVpX3jUDbZBDCih7kng) (accessed on 1 April 2021).
  13. Klein, E., (2021). *The Importance of Security in IoT*. [Online] Logz.io. Available at: <https://logz.io/blog/the-importance-of-security-in-iot/> (accessed on 1 April 2021).
  14. Lerner, S., (2019). *Twelve IoT Security Challenges*. [Online] Enterprise digitalization. Available at: <https://www.enterprisedigi.com/iot/articles/iot-security-challenges> (accessed on 1 April 2021).
  15. Limbachiya, N., (2021). *Top 5 IoT Security Challenges to Expect in 2020 - DZone IoT*. [Online] dzone.com. Available at: <https://dzone.com/articles/top-5-iot-security-challenges-to-expect-in-2020> (accessed on 1 April 2021).
  16. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I., (2015). *Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures*. [eBook] Department of computer science and engineering. Available at: [http://faratarjome.ir/u/media/shopping\\_files/store-EN-1521022452-8019.pdf](http://faratarjome.ir/u/media/shopping_files/store-EN-1521022452-8019.pdf) (accessed on 1 April 2021).
  17. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I., (2015). *Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures*. [eBook] Available at: [http://faratarjome.ir/u/media/shopping\\_files/store-EN-1521022452-8019.pdf](http://faratarjome.ir/u/media/shopping_files/store-EN-1521022452-8019.pdf) (accessed on 1 April 2021).

- 2021).
18. Medium, (2019). *Why IoT Security is so Critical?* [Online] Available at: <https://theiotmagazine.com/why-iot-security-is-so-critical-381f4e7c29fc> (accessed on 1 April 2021).
  19. Peerbits, (2021). *Ten Biggest Security Challenges for IoT*. [Online] Available at: <https://www.peerbits.com/blog/biggest-iot-security-challenges.html> (accessed on 1 April 2021).
  20. Salah, K., & Khan, M., (2021). *IoT Security: Review, Blockchain Solutions, and Open Challenges*. [Online] [www.researchgate.net](http://www.researchgate.net). Available at: [https://www.researchgate.net/publication/321017113\\_IoT\\_Security\\_Review\\_Blockchain\\_Solutions\\_and\\_Open\\_Challenges](https://www.researchgate.net/publication/321017113_IoT_Security_Review_Blockchain_Solutions_and_Open_Challenges) (accessed on 1 April 2021).
  21. Shah, V., (2021). *Nine Main Security Challenges for the Future of the Internet of Things (IoT)*. [Online] [readwrite.com/](http://readwrite.com/). Available at: [https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/?\\_\\_cf\\_chl\\_jschl\\_tk\\_\\_=36b085957452970b3cb5f65d17046b14be7346db-1612173827-0-ASubT1SrQr5PXjq5EzKvurdMwTfhurfFP2AVlRTFI70CD9mRjgvcuS9H\\_PmcsHlFa4h9v9-6\\_II7\\_sjhvz9wY6cSb5wHgGkLxBpOTqY9dW6pmBeK70HsKNHd1yUS2sfVbWSaU2g5LfxIMvDpglMrTfGhjF7DtyTmuv2r6nXfF4EEUxi1Zb2FdZmmjfZDbipl-3nOupWGgBB77tLqcjPYK7e9eQ9G3mdLtYax8mOVJHXIYeZNAcXEgX9wNg4quaemHSzLclrDEkGP2YokfLHNBeN5rweUhn10y5PXW6ZDew-6bwAAuVzerHRW3MfGy6t3hPKQ5CgX\\_HfKPRjAss5MhYXyIXVUElbl7iAw3MMREceRPIVlKifjDOGKJCJbV3pZG4WJBnfiTa-FDA5gh3HGmhqXJVIjIHZBnJ9p6bpytSN8eKrP9pZot8yWBWasmS2Na4OQ-WqWIRzek51PAhdn5A1v3U-VluQPlu9Mpu6Pcqntu](https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/?__cf_chl_jschl_tk__=36b085957452970b3cb5f65d17046b14be7346db-1612173827-0-ASubT1SrQr5PXjq5EzKvurdMwTfhurfFP2AVlRTFI70CD9mRjgvcuS9H_PmcsHlFa4h9v9-6_II7_sjhvz9wY6cSb5wHgGkLxBpOTqY9dW6pmBeK70HsKNHd1yUS2sfVbWSaU2g5LfxIMvDpglMrTfGhjF7DtyTmuv2r6nXfF4EEUxi1Zb2FdZmmjfZDbipl-3nOupWGgBB77tLqcjPYK7e9eQ9G3mdLtYax8mOVJHXIYeZNAcXEgX9wNg4quaemHSzLclrDEkGP2YokfLHNBeN5rweUhn10y5PXW6ZDew-6bwAAuVzerHRW3MfGy6t3hPKQ5CgX_HfKPRjAss5MhYXyIXVUElbl7iAw3MMREceRPIVlKifjDOGKJCJbV3pZG4WJBnfiTa-FDA5gh3HGmhqXJVIjIHZBnJ9p6bpytSN8eKrP9pZot8yWBWasmS2Na4OQ-WqWIRzek51PAhdn5A1v3U-VluQPlu9Mpu6Pcqntu) (accessed on 1 April 2021).
  22. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M., (2019). *IoT Privacy and Security: Challenges and Solutions*. [eBook] Available at: <https://www.mdpi.com/2076-3417/10/12/4102/pdf> (accessed on 1 April 2021).
  23. The Temboo Blog, (2020). *IoT Security 101: The 5 Essential Focus Areas for Building a Safe System*. [Online] Available at: <https://blog.temboo.com/iot-security/> (accessed on 1 April 2021).





## CHAPTER 5

# IoT Architecture Security

### CONTENTS

5.1. Introduction.....	132
5.2. IoT Architecture .....	134
5.3. IoT Security Threats, Impacts, and Challenges.....	138
5.4. IoT Ecosystems Are Difficult to Monitor and Manage.....	144
5.5. IoT Ecosystems Can Be Inherently Insecure.....	144
5.6. IoT Standards and Regulations are Obscure.....	145
5.7. Security in IoT .....	146
5.8. Security Features at Various Layer of IoT .....	147
5.9. Software Defined Networks (SDN).....	148
5.10. SDN Based Architecture for IoT .....	152
5.11. Security Architecture Issues in the IoT.....	154
5.12. Insecure Access Control.....	155
5.13. Conclusion .....	157
References.....	158

In this chapter, concerns related to the security of IoT will be discussed by considering different factors related to IoT architecture security. As the internet is getting evolved with a rapid pace the network security threats are also ever-increasing. Every device that has networking capabilities are included in the internet of things (IoT), thus, the security of devices will be given special concern in this chapter. The devices with networking capabilities may include simple home sensors to nuclear reactors, other devices are cars, medical devices, airplanes, etc. The security threat related to any of these devices has the potential to risk human life. It has been a great concern since the number of cyber-attacks have been increasing day by day, and on the basis of data, these attacks increase a minimum of 50% every year in comparison with last year. Now in terms of security mechanisms traditional mechanisms have been implemented at the internet edge that includes intrusion detection and prevention system and firewalling. These mechanisms are capable of protecting the network over which the data transmission takes place in IoT devices from any external attack. However, in the next generation internet, these mechanisms are not enough to provide network security in IoT architecture. Apart from that, two other major concerns related to IoT are software verification and network access control that arises due to the borderless architecture of the IoT. All these issues will be discussed in detail in this chapter in different sections to allow the readers to have a better understanding.

## 5.1. INTRODUCTION

Over the past few years, IoT devices have become an essential part of human lives as every other device nowadays is connected to IoT technology. People are dependent on IoT technology as it has improved ease of living to a much greater extent. Some of the IoT-connected devices include cars, pacemakers, fitness trackers, and it also includes a control system that is responsible for delivering power and water supply to homes and enterprises.

It is also an undeniable fact that there are various benefits of the IoT technology related to ease of living, etc. But this also raises concern since the security of these devices are not at par and hence are vulnerable to external security attacks.

It is important for the IoT devices manufactures that they provide utmost security to its users, and there should not be any compromise to the security and privacy of the users. As the IoT devices are getting new innovations

every now and then, the security of these devices is not in pace with the innovations.

A few such examples of this are that in one case of automated vehicle operated with the help of IoT could be hijacked and operated remotely, this was the case of Jeep vehicles in 2015. In the next year, there was a much greater extent external attack called Mirai and Dyn that caused the Denial-of-access to websites such as Netflix and PayPal.

In the very next year, that is in 2017, IoT devices with security measures were compromised by BrickerBot, and in 2018, an attack called Z-downgrade was discovered by the researchers due to which over 100 million devices using IoT technology was left for unauthorized access. As per a previous estimate, the attackers were targeting IoT devices more, and cyberattacks targeting IoT devices were estimated to be 25% of total attacks by 2020.

In the case of IoT, when the business opportunities are found, then it is essential that the security-related risks are also present, and that is what security professionals look for and provide the information related to that to the business organization.

As per a study when asked about the two major security issues to the security professional that are related to the IoT devices, the major security threat was found to be possessed by email which as per 44.8% security professional is the major cause of cyber-attacks and IoT devices causing cyber attacks were considered by 44.3% as the major issue.

Apart from that Amazon Echo and chatbot devices were also considered to have a security threat to the business enterprise as per 99% survey respondents. The majority of these respondents were in favor of removing these devices from the enterprise.

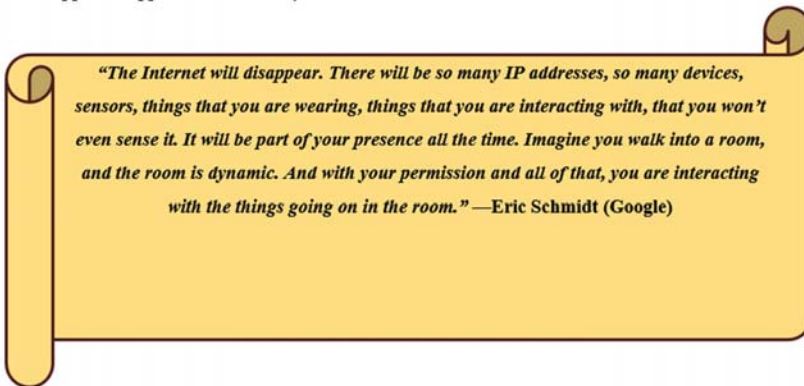
The result of the researches suggests that there is a great security threat posse by these devices, but to ban these devices from the working environment does not seems to be a feasible plan to defend from the issues.

Instead of using these tactics of removing the devices from the work a much effective solution would be to develop better security measures to be implemented in the IoT devices.

In order to deal with the IoT cybersecurity issues, the focus should be on developing secure IoT architecture involving the disparate hardware, software, and protocols for security. The IoT architecture and its processes should be different from the traditional network of the enterprise.

This should be done because if its devices are integrated into the enterprise network then and the enterprise needs to update their operational security strategies and they also will require new strategies for risk management since an additional entity has been added to the already working network of the enterprise where confidential data also gets transmitted from one section to the other section of the enterprise.

Also developing these strategies of operational security and risk management it will be use case dependent and also on the supported application criticality.



## 5.2. IOT ARCHITECTURE

### 5.2.1. Fundamental IoT Architecture Layers

There is not much difference between the architecture of IoT and traditional information technology that has multiple endpoints, which means if an organization has already implemented an IT architecture with multiple endpoints, then there won't be much hassle in implementing IoT architecture in that enterprise.

The major difference encountered is in the diversity and scale of the IoT endpoints. The IoT device security is not guaranteed by the enterprise as always, so in order to prevent any type of compromise, it is important that each of the four layers of the IoT architecture are set up after analyzing and understanding them properly as per the enterprise needs (Yelamarthi et al., 2017).

### ***5.2.1.1. Device Layer***

The device layer is commonly known to be the meeting point of the real world with the digital world. In this layer aspects of IoT are included such as IoT software, hardware, actuators, and sensors. The IoT devices are vulnerable to repudiation threats, information disclosure, elevation of privilege, theft, tampering, and spoofing.

In case if the IoT devices have suffered an external attack, then the damage can be done in the form of reputational damage to enterprises, extortion, privacy violation, mass service interruptions and data breach.

### ***5.2.1.2. Communication Layer***

The communication layer is important for the IoT system since it includes communication service providers required for providing IoT services to the users and business organizations, network technologies and communication protocols.

The communication layer also defines security mechanisms, such as X.509 certificates, and security protocols, such as data transport layer security (DTLS). Overall, the communication layer is vulnerable to issues such as denial of service (DoS), spoofing, information disclosure, tampering, and eavesdropping. The adverse impact of a communication layer-based attack would be in terms of operational and reputational damage, data breach and service interruptions.

### ***5.2.1.3. Cloud Platform Layer***

In a distributed IoT system, the role of the cloud platform layer is very important since it is the one that is responsible for ensuring consistency of data objects in the end-to-end semantic manner. Cloud platform layer provides description regarding how data is transmitted and store such as it describes how the data comes into and goes out of the system and how it is stored.

It is very important for business organizations to have a competitive advantage and the features and intelligence required for that is present in the cloud platform layer. The cloud infrastructure and web-based services are all included in the cloud platform layer, and this layer is vulnerable to external attacks like elevation of privilege, DoS, etc.

Thus, it is very important for any business organization to provide maximum security to the cloud platform layers since all the major data transmission takes place through this layer, and this layer is very important for them to have a better advantage over their competitors. Thus, any vulnerability to this layer will cause the organization to lose money and reputation as well (Ibrahim et al., 2019).

#### ***5.2.1.4. Process Layer***

In business organizations, the process layer for IoT architecture includes integration of IoT projects with management processes, operations, and governance along with the line of business systems. In the case of cybersecurity architecture, the weakest link is considered to be the people.

This is due to the fact that people working within an organization are often found to be neglecting the basic cybersecurity practices and policies that makes the entire system vulnerable to the cyber-attacks. The attacks often include sensitive information theft and repudiation, the sensitive information that gets leaked is often intellectual property (IP) and ends up resulting in lawsuits in many cases.

Due to the advancement in technology in a rapid manner making the people to enter the virtualized world in a more fast-paced way. This is sad due to the fact that smart machines are getting developed more and more with the help of artificial technology and as per a report by CISCO, the IoT population has crossed the human's population in 2016.

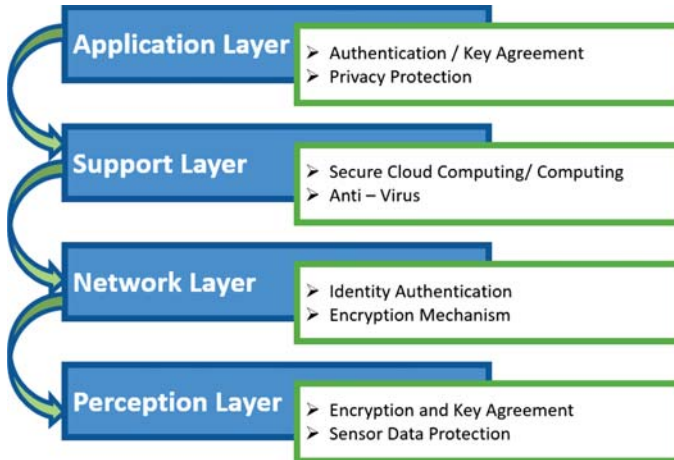
As per the recent trend the IoT devices are growing rapidly, and hence by the end of the year 2021, the number of connected devices over IoT may grow up to 60 million connected devices. Thus, in the research field and industry IoT sector hold a major position due to its promising growth.

In this chapter, the security features related to different IoT layers will be elaborated and discussed and a review will be provided in different sections of this chapter in which the current security measures taken for the security of IoT devices are sufficient or not for much more attention is needed to make this particular section more secure (Zhang and Qu, 2013).

Four main layers of the IoT Architecture identified are (Figure 5.1):

- Application layer;

- Perception layer;
- Networking layer; and
- Middleware layer.



**Figure 5.1.** *Layers of the IoT architecture.*

Source: Image by MDPI.

#### **5.2.1.5. Application Layer**

Application layer can be defined as the layer where all the IoT applications have been deployed, such as smart homes, etc. Application layer of IoT architecture has a major role to play in order to have a better IoT experience. The challenges related to the security and privacy in IoT remains a major hurdle for this technology to become one of the greatest technological leaps that happens once in every few years.

IoT is considered to be a revolution because it has who used the is of living to a much greater extent since all the devices connected over IoT are connected to each other as well and only way to for this device to not interfere with the working of each other is to have a secure and advanced level of security protocols (Zhong et al., 2015).

#### **5.2.1.6. Perception Layer (Sensing Layer)**

The major task of the perception layer includes collecting data from users in real-time with the help of sensors such as QR codes, barcodes, and RFID

technology. After collecting data from this layer, the data is sent to the application layer.

The RFID tags that are used over a device have all its information, and one this type can then the data of the device is received by the scanner. After the data is scanned from the tag then following the hierarchy is this data is sent to the networking layer where it is processed as per the requirement (Abd Aziz et al., 2017).

#### **5.2.1.7. Networking Layer**

After this layer, the networking layer is present in the IoT structure in which data transmission takes place. Once the sensing layer receives the data then it transmits it to the networking layer with the help of some networking protocol like the internet or with the help of any trustworthy layer of networking.

The data received from the sensing layer by the network layer using RFID tags can be transferred to the database so that the data received from scanning the tags can be stored properly.

#### **5.2.1.8. Middleware Layer**

In the middleware layer, the information processing takes place, and all the service-oriented processes are done. That means this layer is responsible for classifying the data and sending it to the relevant storage space.

Particular algorithms and techniques are used for classification of the data received by the middleware layer from the networking layer. The networking layer needs to be secured from any sort of malware attack so that the data is received over a secured channel.

### **5.3. IOT SECURITY THREATS, IMPACTS, AND CHALLENGES**

#### **5.3.1. Threats**

The threat of cyber-attack over IoT devices are rising rapidly, and they are very much more sophisticated than any other cyber-attack. In 2015 majority



of the cyber-attacks done on the IoT devices word to gain remote access over the internet-connected vehicles in which remote access were performed to enter the algorithm of the automated vehicles.

According to Rudresh (2018), in 2016 the problem of cyber-attack got even bigger and this time an IoT-based botnet wreaked havoc over the internet and many internet-based services works under the attack of these botnets. This problem of IoT based botnet attacks got even bigger in 2017 and 2018 along with the issues like crypto miners and malware attacks.

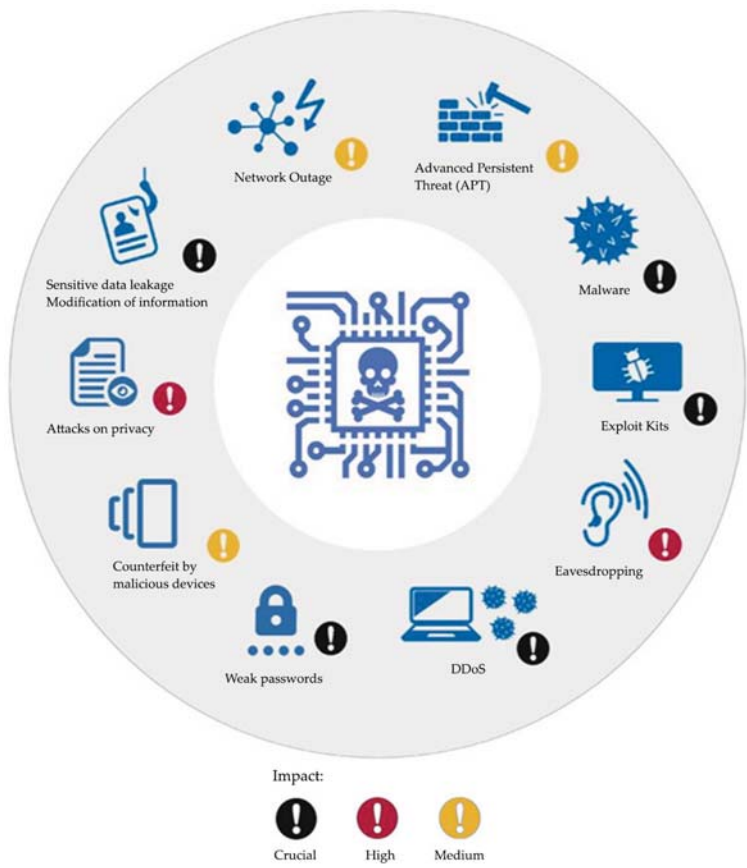
So, it would not be an easy task to list all the threats posed to an IoT ecosystem, but some of the major risk and attacks are malware (e.g., Mirai, Satori, Brickerbot, and VPNFilter), exploit kits (e.g., RIG), advanced persistent threats (e.g., Stuxnet), weak authentication mechanisms, poor password standards and due to weak cryptography algorithms, the attacks like protocol hijacking, session hijacking and man in the middle attacks becomes prominent (Hassija et al., 2019).

Cybercriminals exploit IoT devices so that they can instill operational or reputational damage to a business organization by introducing their online services and the services that are conducted through IoT-based systems; they can also steal sensitive data, extort, collate information, and eavesdrop (Delicato et al., 2013).

The attacks such as man in the middle attack are performed in order to gain access to the network over the data transmission that occurs for any organization that uses IoT-based systems. The hacker having unauthorized access to the network will be able to receive and send all the data that is being transmitted over the network.

The attacker can also manipulate the data received from the sender in between and then send this manipulated data to the receiver without the knowledge of the sender that sent data has been manipulated.

This problem, however, can be overcome using an advanced cryptographic algorithm that encrypts the data and anyone having unauthorized access to the data transmission can collect the data but without the appropriate he cannot understand but the information is being transmitted (Figure 5.2) (Ahmed et al., 2019).



**Figure 5.2.** *IoT threats with level of impact.*

Source: Image by Help Net Security.

In order to illustrate the threat landscape of the IoT Microsoft threat model that is straight will be used in this chapter, and the IoT threat model defined by Microsoft will also be evaluated. There are various threats identified in terms of IoT architecture, and hence these are required to be dealt with properly. Every year IoT devices suffer from various external cybersecurity attacks that cause loss of millions of dollars.

In most of the cases the attacks are of high level and cannot be overcome with the help of security measures but various cases have been identified that shows the cause of these attacks to happen, such as lack of knowledge of the employees related to the IoT architecture and hence making their company's IoT network vulnerable to external threat.

Implementing better security measures in IoT devices and network is one way to ensure security in the organization. Since there are various business organizations that run online and hence, they should not be vulnerable to external cyber-attack, since it will make them lose various customers. Different threats have been evaluated in this chapter so far, and some more will be discussed in the next section.

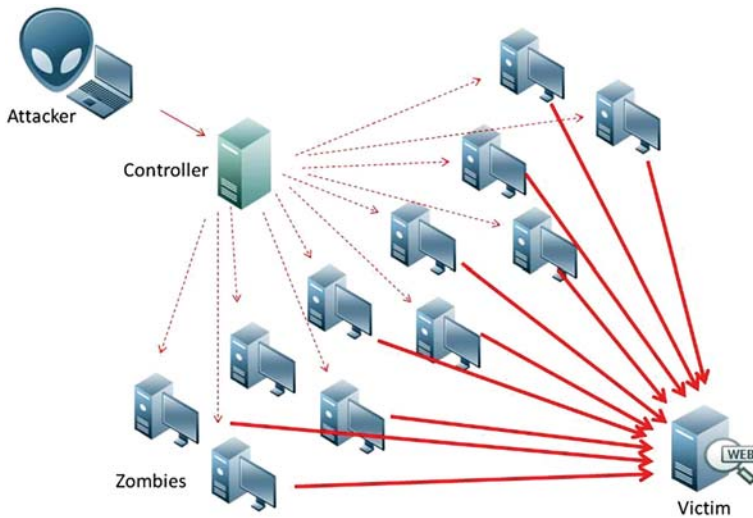
#### ***5.3.1.1. Spoofing***

Spoofing attack is caused when an attacker changes unauthorized access and pretends to be someone that they are not. The spoofing attack is done in order to gather essential data such as cryptographic keys from any device, which can be performed either at hardware or software level, and after that, the attacker can access the system with the help of a virtual device by using someone else's identity. An example of this is a remote control that can function on any TV. Spoofing is also considered as identity theft to gain user access.

#### ***5.3.1.2. Denial of Service (DoS)***

When an attacker gets access to any network over which the data transmission is taking place, then they can manipulate the services and gains the ability to deny the services offered over the network.

A device is made to stop working with the help of radio frequency interference or by any unethical means. This can be understood from the working of Mirai attack in which the network-connected cameras were targeted to make them stop functioning, and it also affected the poorly connected IoT devices (Figure 5.3).



**Figure 5.3.** *DDoS attack.*

Source: Image by Wikimedia Commons.

### 5.3.1.3. *Tampering*

In the case of a tampering attack, an attacker changes the capability of replacing the software running on the device in order to allow the replace software so that general identity of the device can be accessed and hence key data over the device can be collected.

In this attack, an attacker after extracting important data by replacing original software from the unauthorized one and after that the attacker can replace the original data over the communication path with the false data that has been made to show as original with the help of the stolen cryptographic key. This attack can also be conducted to manipulate data in servers and clients.

### 5.3.1.4. *Repudiation*

This is another issue of IoT in which someone performed an action and then did not claim to do it. This particular issue occurs in the case of credit card transactions. An attacker having details of the credit card of a user and then performs transactions on the user's behalf so the user will not claim that they performed the transactions. One such example of this is the email services in which a sender of an email can claim that they did not send that mail.

### **5.3.1.5. Information Disclosure**

If a device has been compromised, then it can leak data to unintentional receivers. For instance, if an attacker gets the information related to accessing the communication path then it can inject itself into the communication between device and cloud gateway, field gateway and a controller so that the information can be gathered from the internal communication of the organization.

These kinds of attacks are either done in order to have an unethical competitive advantage or by any malicious attacker for the purpose of extortion. In any case, information disclosure always has an adverse impact on the reputation of the organization in terms of securing user's data.

### **5.3.1.6. Elevation of Privilege**

In this attack, a device is exploited in order to perform the function other than what the device is supposed to do. For example, if a link is sent to provide limited information but by exploiting it, the same link acts as a gateway to the confidential data of the website. Another example can be a valve that is programmed in such a manner that it is supposed to open halfway, but it can be exploited to open all the way.

### **5.3.1.7. Theft**

This is a simple case of stealing a device or data from the device while the data is in transit or with the help of eavesdropping, essential information can be gathered.

## **5.3.2. Impacts**

In an IoT ecosystem, it is very important to understand what needs to be secured. That means the priority of information that should be secured at all cost needs to be identified at the initial stage. This ensures that even in case of an attack occurs then the confidential data is not lost.

This can be understood by understanding the risk associated with every layer of an IoT architecture and what are the corresponding impacts of each layer has on an enterprise.

## **5.4. IOT ECOSYSTEMS ARE DIFFICULT TO MONITOR AND MANAGE**

It is a known fact that managing and monitoring IoT ecosystems is a complex task. This is due to the fact that if an IoT environment is complex, then the IT administrators do not get required visible access over a few components of this structure.

One more issue in the inability to control and monitor the devices of IoT is that if the IoT devices are deployed over legacy infrastructures and non-IP based devices, then it becomes a major issue in monitoring these devices. In addition to that, in comparison to the traditional IT systems, it is found that lack of basic management functionalities is found in the IoT system due to their opaqueness and inflexibility (Li et al., 2019).

Considering a scenario to understand this issue is that direct access to an IoT system's operating system is not given to the system administrator, which does not allow them to reconfigure the operating system in order to get rid of the unwanted software and hardware capabilities.

This action however can cause hurdles to the intended functionality of the system, or it can completely break IoT devices. One more major issue faced by the IT administrator in order to manage the IoT ecosystems is that the employee in an organization do not follow basic security practices.

They are not supposed to connect their personal IoT devices to the company's IT network or while on the company network, they are not supposed to visit any malicious website, and at last, they should always keep their devices up-to-date to the latest software. This is due to the fact that outdated software has the risk of getting hacked easily.

## **5.5. IOT ECOSYSTEMS CAN BE INHERENTLY IN-SECURE**

There are multiple factors that cause IoT ecosystems to be insecure that includes lack of security by design expertise, poor implementation, or paucity of incentives to develop security controls. All these factors make an IoT device defenseless and vulnerable to cyber-attacks.

IoT devices suffer from the issue of lack of encryption of data during transit for their security. They also suffer from the issue that the software that hosts these devices lack mechanisms that ensure their security from malicious modifications (Harbers et al., 2018).

Other factors that work in favor of an attacker are that the IoT devices have little to no authentication mechanism, insecure update mechanism, and below-average physical security mechanism all these factors cause the IoT devices to be vulnerable to the external attack.

Apart from that, if the IoT devices are implemented over legacy infrastructure, then it becomes a major issue in protecting these devices because manufacturers no longer support the legacy infrastructure, and hence the problem of cyber-attacks increases to higher levels (Figure 5.4).



**Figure 5.4.** *IoT device vulnerabilities.*

Source: Image by Trend Micro.

## 5.6. IOT STANDARDS AND REGULATIONS ARE OBSCURE

The two major causes of barriers for the improvement of IoT security are a good amount of security issues and lack of mature security frameworks. At present for cybersecurity in IoT, no common approach can be found, and a common multi-stakeholder model is also missing for IoT cybersecurity.



This is the reason why most of the companies implement their own approach of IoT security as per the needs of their organization. This is the reason why the IoT security measures are undeveloped to be implemented over industry level.

That means since every organization and manufacturer have their own approach of IoT security implementation that is why a standard guide for IoT security measures is missing that can guide the IoT security manufacturers to have a common path while implementing the IoT security mechanism (Anwar et al., 2020).

There is also a tissue or a barrier to security in terms of regulation fragmentation this is due to the fact that no regulation can be found that has the ability to force security protocol at every level of IoT architecture, and another major problem is the unclear or liability.

In the case of a security incident there is a non-responsibility barrier is found among the stakeholders that are involved with the organization, and this barrier is both a legal and moral level. This arises a need that in the event of a security concern, the liabilities need to be clarified at every level of the IoT architecture.

## 5.7. SECURITY IN IOT

In terms of development, IoT has played a greater role in creating smart environments, smart devices, smart cars, smart homes, and smart cities. The role played by the IoT technology is of greater effect due to the fact that every case of developing of smart environment is related to IoT.

IoT has the greatest impact in terms of creating a smart environment, but there are a few other factors that are required to be given equal importance so that the experience of IoT is not different for every individual.

As per Kashyap et al. (2017), the major aspect that needs to be considered in terms of improving the experience of IoT is the security framework improvement for IoT. Although the development of the IoT framework has been considered and extensive work has been done in this regard but IoT security has not been given much importance since the beginning.

Since the IoT device are vulnerable to external attacks due to their compact size, easy access and less security thus, the basic security requirement in terms of IoT that is CIA known as (confidentiality, integrity, and availability) needs to be implemented in every IoT device.

The updating of the IoT architecture needs to be done on a regular basis



with improved security patches implemented which can ensure that the IoT devices are secured from attacks such as Hajime IoT worm which recently infected 3,00,000 devices, 8 DDoS attack in the application layer, Teddy bear data breach, Bricker Bot Malware attack which destroys unsecure IoT devices and many more such attacks need to be mitigated (Khan and Salah, 2018).

## **5.8. SECURITY FEATURES AT VARIOUS LAYER OF IOT**

There are various security issues lurking at each layer of IoT architecture that are required to be tackled properly so that the threat from external factors can be dealt with properly. Some of the security issues related to the IoT architecture have been discussed here in this chapter.

In order to resolve the IoT architecture security issue, various algorithms have been implemented, which will be discussed in the next section to understand how effective these algorithms are in order to provide the security to the IoT device (Ammar et al., 2018).

In the perception layer, the sensing and reading process of the data takes place with the help of different kinds of implemented sensors in that layer, thus, it is of high possibility that some of the sensors may read confidential data due to unauthorized access.

There are high chances that if an attacker has gained access to the perception layer and is reading the confidential, then they are able to manipulate it as well. There is also a chance that the intruder can pose a hurdle to the normal working of the system and can block the tags that can cause information loss.

An issue identified with the RFID tags is that they are visible and hence can be cloned easily, that is highly undesirable to any organization since they would not want their user's private information to go to some attacker's server (Mendez et al., 2017).

In the network layer, the data transmission process takes place with the help of a wireless communication network. The communication process is dependent on platforms such as Wi-Fi, cloud, and Bluetooth, etc.

The issue of network layer using these platforms is that the number of devices that can be connected over these platforms are higher so if the IoT

architecture is using one such platform for data transmission without much security measures than the chances of the IoT environment being vulnerable to the outside attack is higher.

Since the attacker can involve itself over one of the insecure networks using any of the platform over which the IoT architecture is present. Once getting into the network, the attacker would be able to gather or manipulate data over the network (Frustaci et al., 2017).

In the middleware layer, the services can be manipulated by the attacker due to the unauthorized access. Since the data storage takes place at the middleware level of the IoT architecture so, if the attacker gains access to this layer, then they are able to manipulate the stored data or may harm the system due to which some undesirable result may arise.

DoS can be considered to be one such attack, in which the middle ware level is attacked and the users are denied the services of some of the system functionalities. The Application layer architecture has to deal with the user end, and hence the security of the application layer needs to be priorities as well.

In the application layer, the attacker may pose as a genuine user and infect the system with malicious codes to harm the system. They can manipulate the program of the system by injecting malicious program into it and make the system to malfunction.

This overall issue reduces the user's trust over any organization when anything of this kind happens. Thus, for any organization dealing with the IoT system needs to have proper security measures taken at every level of the IoT architecture.

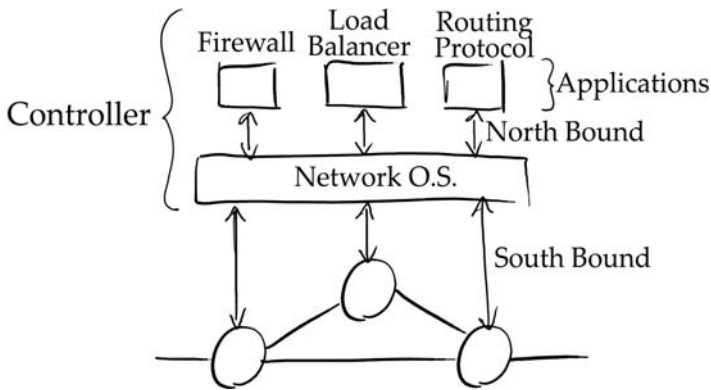
## **5.9. SOFTWARE DEFINED NETWORKS (SDN)**

With the advancement of technology related to IoT architecture have produced a new paradigm of technology that can be used for future communication known as software defined networks (SDN).

SDN is responsible for managing the users over the network and controlling their behavior in case any malicious activity is identified over the network. Network intelligence is logically centralized in the SDN and the data and control planes are decoupled (Dawood et al., 2018).

SDN controller has the ability to delete, update, and add flow entries in response to packets. In addition to that, security threats are acted upon first in the SDN network, and granular traffic filtering is performed and after

that deployment of dynamic security policies take place so that external cybersecurity threats can be occurred properly and in time (Figure 5.5).



**Figure 5.5.** *SDN components.*

Source: Image by Wikimedia Commons.

On the basis of SDN architecture, a security model for the information of technology can be proposed. The proposed model based on SDN architecture can help in securing both wireless and wired network infrastructure (Li, Romdhani, and Xu, 2017). Apart from that, an extension of this architecture will include network objects, such as smartphones, tablets, and sensors, and ad-hoc networks.

The main contributions of this model will be:

- This is the first attempt to tackle the security issues of IoT architecture with the help of SDN architecture;
- For IoT-based device's security, a secure architecture based on SDN is considered that is using security and network access control.

### 5.9.1. Software-Defined Networking Architecture

There are various benefits of the strategy of using software-defined networking that is SDN which includes network functionality improvement, IT cost reduction, innovative research is now enabled, and the hardware complexity is reduced to a much greater level with the help of SDN architecture. There are three layers present in SDN architecture that includes an infrastructure layer, a control layer and an application layer.

The infrastructure layer includes network devices such as wireless access points, virtual switches, routers, and switches. Controller of the control layer includes Floodlight, Beacon, POX, NOX, MUL, Open daylight, etc., and the application layer has SDN configuring aspects such as network management, energy-efficient networking, traffic, and security monitoring and access control (Qin et al., 2014).

SDN architecture's important feature includes security perimeter extending ability to the endpoint devices of the network access that includes wireless access points and access switches. A global network view is created by the SDN controller with the help of OpenFlow protocol in which security policy rules are built and set to the network devices, and the connection is established via OpenFlow switches.

The major issues identified with this global network is the presence of only a single controller that has been installed to control the overall network, and the issue is that if anything goes wrong with this controller, then the overall network will be at flaw and would not work properly. In addition to that security issues such as DoS is another major drawback of the system.

If in case of a cyber-attack can attack again access to the SDN controller then the entire network will be at risk as the attacker is now able to control the entire network. Apart from that, there is only a single controller system then software and hardware failures, which is a common issue, can also occur.

So, it is advisable to use a multi-controller system as it will provide fault tolerance and increase trustworthiness. In the multi-controller system if one controller is broken, then the system can be controlled by another SDN controller so that system failure can be avoided. Cluster-based high availability model is a very good example of a multi-controller system that can be used in the SDN architecture since this model is supported by open daylight controller.

### **5.9.2. SDN Architecture for Ad-Hoc Network**

Virtual switch is used over which every legacy interface is connected, and this virtual switch is controlled using a SDN controller that is integrated to a node. This system of virtual switch and node will reduce the risk of external threat to some extent this is due to the fact that operation of each node is carried out at equal interactions so it won't be an issue to other nodes that any single node is misbehaving due to the users that have been connected over them (Rawat and Reddy, 2016).

An embedded SDN compatible switch will be used for the connection of ad-hoc users with other nodes. At the same time, since there is another node in equal interaction over the SDN controller is present so it will take care of the security and connectivity between the nodes.

An additional advantage of this SDN-based ad-hoc network architecture is that it is compatible with SDN legacy network. Thus, in order to construct an SDN domain, the interconnection between legacy network and ad-hoc network can be done due to the fact that the nodes in the ad-hoc network have an SDN controller, and these nodes are embedded with SDN and compatible switches (Kalkan and Zeadally, 2017).

Further evaluating this system, it has been found that the limitation of the SDN domain is that the domain is limited to the network with infrastructure. Therefore, in this case, Ad Hoc users were required to connect with the help of other nodes such as network Gateway that are directly in connection with the SDN domain.

Since every Ad Hoc node has been provided with separate SDN controller so the management of every SDN virtual switch that is present on every ad-hoc device. When a new ad-hoc device is identified on the network or if a previous ad-hoc device leaves the network, then various messages are exchanged for the synchronization process (Ndiaye et al., 2017).

With the help of various controllers, fault tolerance and scalability are insured in a distributed SDN architecture. In order to ensure that process new controllers are added dynamically to the network area of the ad-hoc network and special nodes are given authorization for the control operation to run efficiently. However, the network global view is the same for the new controllers as well.

A small ad-hoc area is given for the domain of SDN management and its functionality to perform. In the SDN system, the software switches behavior required to be monitored at all times, and for that function to perform the same SDN and controllers are used as they are implemented at the user side.

In order to provide fast response whenever network change occurs, a distributed network access control architecture is used as it has been found to be working efficiently in case of network change. One more advantage of the distributed control architecture for network access is that it is able to react to the attacks that are performed over the SDN domain and that happens simultaneously performing that traffic load management by sharing this data with the root controller.

The control functions however are limited in case of the ad-hoc controllers as it works over the available resources that are present with the hosting ad-hoc device. This current SDN architecture can be extended to include smart objects like mobile vehicles, smartphones, and tablets, etc. This can be achieved by using open close software switches, and for that a Framework needs to be developed that can integrate this software into those devices.

## **5.10. SDN BASED ARCHITECTURE FOR IOT**

The traditional network protocols and traditional equipment lack the capability of managing higher levels of scalability, and these are also not sufficient enough to manage high amounts of traffic and mobility.

There have been a few IoT architecture models that have been proposed in which ETSIs M2M architecture can be exploited that can be done by making the device to negotiate the security parameters and the quality of service that it provides (Wang et al., 2017).

One more thing that can be done to make the system more efficient is that real-time information of Cloud Service connectivity can be accessed so that the information of how many devices and which devices connected to the network and when can be gathered.

The proposed IoT architecture model will be able to provide efficient services related to scalability, adaptability, and intraoperative ability of the IoT devices connected over the network. However, there are some previous solutions in this area that propose a software defined approach for this function to work efficiently for the IoT devices, but this solution lacks the capability of making the system of IoT network more secure.

These previous solutions one more focused on the integration of SDN and IoT and hence these were not sufficient enough for the security purposes. But the SDN based architecture for IoT devices that has Ad-Hoc networks and SDN control management performs the security measures as well, and it is efficient enough to deal with the external threats over the IoT devices.

Since the major issue identified with the IoT devices is in relation to the external cyber-attack that gains access to the network over which the data transmission related to IoT connected devices occurs.

This issue is dealt with using SDN based system for IoT architecture as the real-time data related to every device getting connected over the IoT network is gathered and any malicious behavior by any user is identified in

no time and as per the predefined rules if any rule is violated then that user is denied access to the network.

### **5.10.1. SDN Domain**

In IoT networks providing every device with a separate controller and switch of the SDN network will not be a suitable option. But it can be assumed that every device is connected to its neighbor node that has the SDN capability since the resources are limited.

There are two types of nodes identified in the SDN domain. A node that has enough resources is called a smart object, and if it does not have enough resources, then it is called an OF node. The traffic in a single domain is controlled by an SDN controller that is separately provided to every domain.

### **5.10.2. SDN Domain Interconnection**

For SDN architecture with multiple SDN and domains, it is assumed that every domain have either one or multiple SDN controllers. The devices present in the domain are only controlled by these SDN controllers. A data center on the enterprise network can be represented with the help of a single SDN domain.

In order to implement SDN systems in an IoT environment the heterogeneous interconnection needs to be established since the requirement of SDN domains is higher for the IoT devices network. Every domain is introduced with a new type of controller so that large scale interconnections of IoT devices can be maintained efficiently.

Since the interconnections became larger in the IoT network so it has been recommended that for optimization of the control functions, hierarchical architecture could be implemented that can perform control function distribution efficiently.

It has been proposed that instead of distributing the control functions over various controllers in the SDN and network, it would be beneficial that routing functions are distributed instead of control functions, and also every edge controller should be provided with the security rules with the help of the distribution process.

This process of interconnection establishment is a very complex process to follow since every domain in the SDN architecture has its own management strategy and security policies to follow. So, it is very important

that an optimized way to perform the interconnections needs to be derived which ensures the security of every domain as well.

## **5.11. SECURITY ARCHITECTURE ISSUES IN THE IOT**

### **5.11.1. Insufficient Authentication**

The authentication over the internet is provided with the help of login and password credentials in order to access any personal account, and the browsers are authenticated with the help of SSL or secure sockets layer protocol.

Any website that does not have an SSL certificate is deemed to be not secure, and hence users who visit these types of sites are provided with a warning before visiting this site. Similarly, in the IoT environment, every new device that is connected to the IoT network requires to be authenticated before giving access to the network in order to transfer data.

As per Olivier et al. (2015), it is required to be understood that since embedded devices are accessed by various users so authenticating every user every time is a time-consuming task, so authentication in embedded devices works on the basis of a stored set of credentials provided by the user. That means when the user first accesses the IoT environment then they are required to set a login and password to access the system every time.

These credentials are then stored securely in a storage area, and next time when the user tries to access the IoT network then they are asking for the credentials and after providing these credentials these are made with the stored credentials, and when the matching is perfect then only the user is provided with the access to the network or the IoT device (Marino et al., 2019).

### **5.11.2. Insufficient Device Authentication in IoT**

The devices in the IoT network suffer from insufficient authentication and hence they are vulnerable to the external attacks by the malicious user that contains unauthorized access over the IoT network.

In order to provide sufficient device authentication security tokens needs to be used the working of these should be in this manner: First security token should be for local gateway authentication in which in order to perform



some actions the IoT devices should be authenticated at the local gateway initially (Jose et al., 2020).

After that, when the data is getting forwarded, then the cloud endpoint authentication should be performed, and it should be given the next security token. All these tokens are getting collected from different actors, which in this case are our local gateway, cloud endpoint, etc.

One more actor here is the IoT application that is capable of rendering and analyzing the data stored, and hence these applications should also be properly authenticated. The working of security tokens will be as one actor authenticate the other with the help of security token obtained previously on the similar message.

Like in the beginning when the IoT devices is getting authenticated at the local gateway level then a security token is provided it to this message and this token is then authenticated at the cloud and point for authentication. This will help the IoT devices to be properly secure as the first actor is identified by the token, and it allows the second actor to make proper decisions related to further authorization process.

#### ***5.11.2.1. Authentication Tools***

OAuth 2.0 and OpenID Connect 1.0 these are the two authentication tools that supports the model described in the above section. These tools are able to provide enhance security and privacy control to the user with the help of using security tokens so that no unauthorized access can be done to the user's data for the purpose of malicious activities. The built-in registration and discovery process is helpful for the architecture scaling in the case of IoT architecture.

### **5.12. INSECURE ACCESS CONTROL**

Role-based authorization frameworks are considered to be the most exciting frameworks for online services and computer networks. In this framework at first the user identity is established and then as per their role in the organization the access privileges are given to them.

This enhances the control and the security of data in the organization since people who are required to have access to the confidential data can access it, and no one else is given access to it. The current network authorization systems and protocols such as SSH, RADIUS, LDAP, Kerberos apply the role-based framework.

The process of identifying individual users may be different as per the protocols implemented, but the process always involves the user identification in every case. After that access control and resource control of different types are applied (Cruz et al., 2018).

The role-based mechanism limits the privileges of device component in order to provide an extra layer of security for any insider threat and even if the system is compromised and any component that unauthorized access then the mechanism ensures that minimum access is provided to this component in order to secure the data.

### **5.12.1. Threats to Access Control, Privacy, and Availability**

In order to provide device security in this layer before it is at risk, the actions required to be performed are:

- Security standard implementation for IoT and to ensure that the specific security standards are met before the devices are given access to the IoT network.
- All the device components need to be reviewed and the data sensing system should be made to increase trustworthiness.
- User source should be traced forensically to identify them.
- At the end node of IoT, the software should be designed considering all the security measures.
- The Open Web Application Security Project's list of top 10 IoT vulnerabilities sums up most of the concerns and attack vectors surrounding this category of devices:
  - Insecure cloud interface;
  - Insecure mobile interface;
  - Insecure network services;
  - Insecure software/firmware;
  - Insecure web interface;
  - Insufficient authentication/authorization;
  - Insufficient security configurability;
  - Lack of transport encryption;
  - Poor physical security;
  - Privacy concerns.

### 5.13. CONCLUSION

In the last decade, the applications of IoT have increased exponentially, and now IoT-based devices and services can be seen everywhere. Cities are being converted to Smart City with the help of IoT technology and the houses are transformed into smart houses.

The vehicles are now smart vehicles as they are following commands with the help of IoT-based technology. Having this much impact in a very little time raises concerns related to its security. The security of the IoT devices is not very effective as every year IoT based attacks are increasing exponentially.

There are various security measures that have been implemented to the IoT devices, but still, the cybercriminals are able to access these devices from an ethical manner such as hacking. Still, cyber threats such as DoS and man in the middle attack are getting performed over the IoT devices all around the world.

It has been identified that due to the lack of redefine guidelines every IoT manufacturer and organization creates their own rules related to the security, which are in most cases and develop and hence make these IoT environments vulnerable to external attack.

The chapter discusses various threats related to IoT and the IoT architecture security has been evaluated efficiently. The evaluation of the SDN-based architecture to be implemented in the IoT devices has been done in this chapter, and it has been identified that this architecture provides an additional layer of security to the IoT devices.

## REFERENCES

1. Delicato, F. C., Pires, P. F., Batista, T., Cavalcante, E., Costa, B., & Barros, T., (2013). Towards an IoT ecosystem. In: *Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems* (pp. 25–28).
2. Kashyap, R., Bansal, P., Bharti, S., & Malyan, A., (2017). *Architecture, Features and Security Concern of IoT*. [Online] Ripublication.com. Available at: [https://www.ripublication.com/awmc17/awmcv10n5\\_26.pdf](https://www.ripublication.com/awmc17/awmcv10n5_26.pdf) (accessed on 1 April 2021).
3. Li, S., Romdhani, I., & Xu, L., (2017). *Securing the Internet of Things* (1<sup>st</sup> edn., pp. 1–137). Elsevier.
4. Li, X., Zhao, N., Jin, R., Liu, S., Sun, X., Wen, X., Wu, D., et al., (2019). Internet of things to network smart devices for ecosystem monitoring. *Science Bulletin*, 64(17), 1234–1245. Available at: [https://www.researchgate.net/publication/334370322\\_Internet\\_of\\_Things\\_to\\_network\\_smart\\_devices\\_for\\_ecosystem\\_monitoring](https://www.researchgate.net/publication/334370322_Internet_of_Things_to_network_smart_devices_for_ecosystem_monitoring) (accessed on 1 April 2021).
5. Marino, F., Moiso, C., & Petracca, M., (2019). Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems. *Computer Networks*, 148, 176–195.
6. Olivier, F., Carlos, G., & Florent, N., (2015). New security architecture for IoT network. *Procedia Computer Science*, 52, 1028–1033. Available at: <https://reader.elsevier.com/reader/sd/pii/S1877050915008996?token=BC6EB903DE648FD06F8711020A7E8E0B472C53171944893885BB21621E7A063DC1B9AA5F111E91BCC5B800C4B71E6DE2> (accessed on 1 April 2021).
7. Rudresh, V., (2018). *IoT Security Reference Architecture for the Enterprise*. [Online] Cdn2.hubspot.net. Available at: [https://cdn2.hubspot.net/hubfs/2539908/Resources%20PDFs/Whitepapers/IoT%20Security%20Reference%20Architecture\\_September-2018.pdf](https://cdn2.hubspot.net/hubfs/2539908/Resources%20PDFs/Whitepapers/IoT%20Security%20Reference%20Architecture_September-2018.pdf) (accessed on 1 April 2021).

## CHAPTER 6

# Security in Enabling Technologies

### CONTENTS

6.1. Introduction.....	160
6.2. Application of Tracking Technology.....	160
6.3. High-Reliability System Configuration .....	163
6.4. Privacy Concerns for 6LoWPAN .....	165
6.5. Security Concerns For 6LoWPAN.....	165
6.6. Challenges in Fog Computing .....	167
6.7. Temporary Stateless Addresses Auto-Configuration.....	169
6.8. Discussion of Security Framework for SDN.....	172
6.9. Conclusion .....	173
References .....	174

This chapter explores the security aspects in enabling technologies. Different applications of enabling technology and their security concerns will be evaluated. Similar as IoT-based systems, the major concern for the devices of embedded systems is related to the network security. Tracking technology will be discussed in the first section after that 6LoWPAN will be evaluated based on its privacy and security concerns. Fog computing has various security concerns and challenges that will be evaluated in the current chapter. The readers will also be able to get information related to the security framework used in the SDN.

## **6.1. INTRODUCTION**

Conventional access control systems are the systems that made use of a card reader to scan smart cards, or magnetic cards to validate the cardholder. Once a person's ID (identification) is authorized, the electric lock installed on the door is unlocked and the door can be opened.

This method is basically no different from the traditional use of a key. Against the backdrop of worries in context to social unrest and safety of business information, access-control systems should comply with the growing diversification of needs.

In order to ensure great reliability, smarter, and more competent access-control system (that is not merely an alternative of a key-based system), it is essential that users of facilities are not cognizant of using the system; in other ways, authentication should be executed while a person is obviously taking an entry a room. The key characteristics of the developed system is that it full this prerequisite by offering "hands-free" access control.

## **6.2. APPLICATION OF TRACKING TECHNOLOGY**

### **6.2.1. Hands-Free Room Access**

In order to attain the hands-free room access, a reception system and transmission making use of infrared radiation and long-distance-communication RFID was developed. When a person who is wearing the badge equipped with RFID stands in front of the room he or she wants to access, the system evaluates that person has the right to access (Figure 6.1).



**Figure 6.1.** *RFID technology can be used to track and manage inventory, assets, people, etc.*

Source: Image by Flickr.

In a scenario when an authorization is given to a person, the door automatically unlocks and the authorized person can now successfully access the room. This process consists of steps discussed as follows:

- An infrared emitter which is installed at each checkpoint (spot) constantly emits an infrared beam making a specific signal as a unique “position ID” for each spot.
- When a person wearing a badge enters through a spot, the badge picks up the infrared beam and obtains the position ID from it. The ID which is exclusive to that badge and the position ID are then merged, and the collective ID is transferred as an RFID signal.
- The controller obtains the joined ID and splits the specific ID and the position ID. By performing this, it can determine the specific badge that has entered any particular spot. It then checks the exact ID alongside the security level for the door in the spot in question.

If the controller verifies that the ID has the authorized access, it sends a command to open the electric door. The authorized person can then access

the approved areas easily in a “hands-free” manner and security checks will be done automatically without any disturbance.

### **6.2.2. Individual Authentication of Several People Entering Room at Same Time**

By offering a hands-free room access, some underlying security issues have now been addressed, namely, a distinct authentication of numerous people taking an entry into a room at the same time.

In relation to a conventional system, access is governed basically by means of smart cards, etc. Although in this case, it is probable that when the person who is standing in front of a door take an entry with his smart card, then a person who is standing behind him can also easily enter the room, even he does not have the smart card as the door will remain open for some seconds when the first person opens it.

On the contrary, in the present newly developed system, each person standing in the line can be authenticated individually.

### **6.2.3. Virtual-Gate Authentication**

The new access-control system also provides the opportunity to authenticate a person without even a need of physical gates. That is, an authentication system equipped with so-called “virtual-gates” can be set up as a security measure.

In this scenario, areas are polarized into zones by virtual gates that perform “soft” security checks (i.e., non-doorway checks) in a way to ensure a high level of access control. Even in door-less, spatial places such as corridors, virtual gates would work in a perfect manner as automatically authenticate a person who is passing through it.

If an unauthorized person or someone who is not wearing a badge is noticed, a warning message is given, and the complete picture of a person is clicked and recorded by a surveillance camera.

**Badge Security** The badge which is used in the developed access-control system offers a high level of security by making use of an RFID device and infrared radiation that generates a weak radio-wave signal.

Though this weak radio-wave output power is 1/10,000 of that of a standard mobile phone signal, or 1/100 of a PHS signal output, it can still offer a high level of security. By making use of such a badge, the new



system can be easily employed in hitherto difficult areas such as healthcare facilities, where use of such devices is limited.

### **6.3. HIGH-RELIABILITY SYSTEM CONFIGURATION**

Ensuring that a system have high reliability brings the two additional benefits that are discussed as follows:

- Even if the network or server is down, independent decentralized control ensures that access control is constant without any obstruction; and
- With a platform comprising of a cooling fan operating on a Linux\*1 operating system or an SH microcomputer without an HDD (hard disc drive) or the controller—the core of the access control—can provide long-term, stable operation.

#### **6.3.1. Installation of Security Centered on Dynamic-State Monitoring**

The developed access-control system can be employed at sensitive areas such as research centers in order to offer a high level of security regarding visitors and internal staff. Some essential features of the system are discussed as follows:

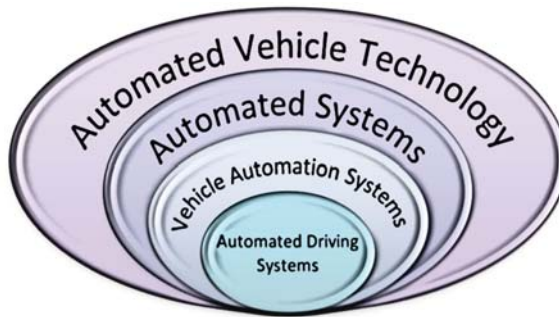
- Each area in the facility is stated systematically so that it is given a comprehensive security level.
- Organizations and outside people are outlined in groups according to lateral or vertical organizational hierarchy, and an “access level” for each location is provided to each stated group.
- Recording the entire data on room access for every location as well as movement of each individual or group are gathered.
- There is also employment of virtual gates in building passageways, and if an unauthorized person is passing through it, a warning signal is released, and an image of the interloper is shown on a real time basis. In addition, virtual gates set up in the offices gather records of the activities of authorized people. If an unauthorized person takes an entry through a virtual gate, a notification is sent to the administrator, and an image of the person is recorded concurrently.

### 6.3.2. Vehicle-Access-Control System

In this anticipated application, the developed access control system is employed to connect traffic signals and barriers for supervising the movement of vehicles in places like public and industrial facilities or delivery and distribution warehouses.

An RFID badge fixed in each vehicle facilitates the authorization or non-authorization of each vehicle perform its tasks at both the entry and exit gates as well as at “area” gates set up along internal roadways.

The gate barriers are then either opened or closed, and traffic signals are organized in reference to the authentication. It is an example of the access control system that are designed for vehicles to be run by people (Figure 6.2).



**Figure 6.2.** *Automated vehicle system technology hierarchy.*

Source: Image by Wikimedia commons.

Vehicles equipped with formerly registered badges and checking their authorization inevitably means that the drivers do not need to get out of their vehicles. This control system makes it possible to ensure the smooth passing of vehicle around the clock.

In comparison to the exiting ETC (electronic toll collection) system that is termed as “non-stop,” the proposed vehicle-access control system can be denoted to as “one-stop.” As this name suggests, the proposed system is not as suitable as the ETC system.

While on the other side, the system installation costs and the tag cost are also comparatively low, so it can be fit at any general business premises with economical price.

## 6.4. PRIVACY CONCERNS FOR 6LOWPAN

Among the security services, the encryption is concerned with ensuring confidentiality of the data that is exchanged over the network. The authentication and the integrity of the whole frame can be assured, but the confidentiality of information stored in the header remains unprotected.

It results in arising the concern of privacy. The header which is responsible for conveying information is called “metadata” and is used for “data mining.” They may enable tracking, as well identification, geo-localization as activity recognition or social links inference. In this section, the main area of focus is to describe how the private information included in the header can be protected (Wang and Mu, 2015).

## 6.5. SECURITY CONCERNS FOR 6LOWPAN

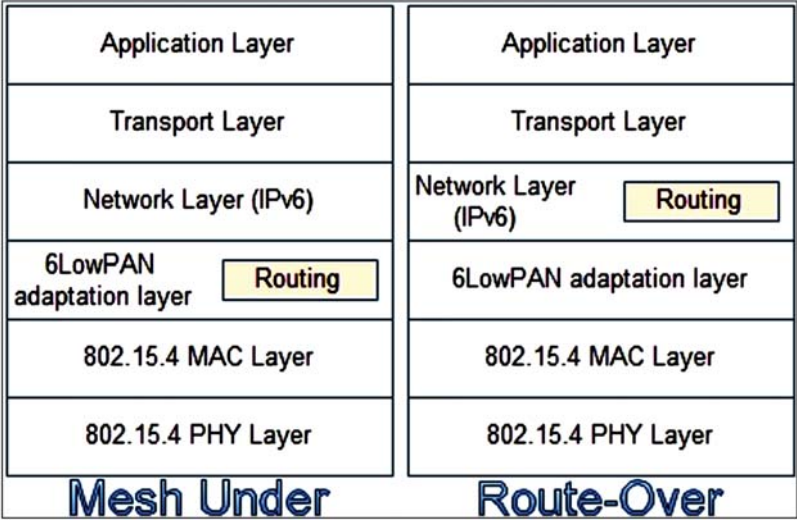
Wireless medium is secured with the help of link-layer security while to maintain the end-to-end security between two pairs upper layer security is used. The security requirements and the threads need to be understood properly in order to use against the right countermeasures.

Various attacks are countered in LoWPANs, including cryptography and other security measures. Due to the drawback of low power networks and devices, these tools are not deployed in parallel with each other.

In order to provide security to a network at a large scale, there are various challenges that need to be identified and solved for the deployment of such a large network can be done securely. Cryptographic keys management and deployment remains one of the most effective constraints in order to implement a secure network at large scale.

The resource provided by the node of 6LoWPAN becomes inaccessible in case of the threat analysis for this network, these threats include masking, relocation, and node destruction. There are various ways using which the cryptographic information can be accessed that includes using node programming, cloning, packet injection, replay attacks.

Denial of service (DoS) attack can be performed at the physical layer with the help of tampering the radio signal. At the link layer, the network flooding can be performed in order to occupy the entire bandwidth using large packets. Attacks such as packet injection can cause the packet loss and battery exhaustion issue. 6LoWPAN adaptation layer handles fragmentation attacks on “mesh-under” routing protocol (Figure 6.3).



**Figure 6.3.** 6LoWPAN routing

Source: Image by Wikimedia commons.

Since the first fragmentation has the information related to the destination address so next fragments can be flooded by the attacker. This will occupy the bandwidth entirely and the denial-of-service attack will be formed since no new service can be processed by the network.

One more attack of such type can occur in which the network bandwidth space is occupied by incomplete packets until saturation. Thus, network layer is vulnerable to various attacks and on routing there are several attacks that can be performed such as network service disruption using a compromised node inside network, Sybil attack, Sinkhole attack and Selective forwarding (Le et al., 2012).

A more dangerous attack can be performed called Wormhole attack in which it is not required to compromise a node the attacker can eavesdrops a packet and tunnels it to another node of the network. This can be launched at the phase of neighbor discovery.

Since there is no direct involvement of the attacker over the node so even if the compromised node detection cannot provide information of the attacker so that packets received by that user can be further blocked (Hennebert and Dos Santos, 2014).

## 6.6. CHALLENGES IN FOG COMPUTING

New challenges are bound to accompany any new organizational processes. Numerous factors, both known and unknown, are responsible challenges in the realm of fog computing that has developed in the era of cloud computing.

In a real-life scenario, the likely losses in the future are prevented as stimulator tools and simulation studies are helping to find those problems. Some of the challenges that have been identified in this field are given below.

### 6.6.1. Connectivity Challenges

Problems are bound to crop up in the system as fog computing is seeing an increase in the connectivity requirements owing to intermediate devices that are being used, which results in an enhanced requirement for communication amongst the varied levels of the system's hierarchy.

In order to forward the data, the time available to the ICO for connecting to the gateway device is quite limited wherein the gateway device discovers the ICO or ICO discovers the gateway device. To ensure that range is not passed by the gateway device before the discovery of the device and it's getting connected, the device needs to be discovered within a limited time in the most efficient manner.

To allow the availability of a sufficient amount of time for the transmission of data between them, it is essential that common grounds are found between them for faster and easier connectivity. Open network should be available during the entire period irrespective of its being the non-communication or communication phase in similar connectivity cases so that a lot of energy is wasted.

That all points of time the connectivity method needs to be kept 'ON' in either the ICOs or gateway devices. To help bring about efficiency and effectiveness in the process a technology needs to be developed that can help conserve the wastage of energy by providing the correct location and time to both the connecting objects.

### 6.6.2. Context Awareness

The fog devices used in fog computing need to be totally aware of the nearby situations that are going on as they are located near the end-user, and this is known as context-awareness. Only if the fitted devices have enough intelligence to assess this it can be possible.

To be context-aware, the fog gateway has to be intelligent which shall enable it to automatically self-modify within a short time so that the sensors provided data can be decoded semantically and then based on their capabilities they shall be able to provide or meet the condition-specific requirements within the context of the request.

Only with the local knowledge and the global data analysis gathered knowledge is coordinated and applied together can this be made possible. Fog computing applications face a major challenge due to the increased knowledge available to the device.

At the same time, the workload needs to be balanced by the smart devices. Through coordination and maintenance of the same with other ICOs and gateways, this is made possible. Further, wastage of resources can also be reduced by this.

Different devices within the system need to have interconnectivity through requisite techniques that shall need to be developed so that it can occur in real time conditions. “Cooperation and opportunistic sensing” are used to describe this.

### **6.6.3. Data Handling**

More and more places like the fog devices are processing and handling data even though in fog computing lesser data formation takes place. As a result, at all sites, data needs to be handled properly. System expansion becomes a necessity at times wherein for backup, temporarily the system is inserted with newer devices.

For this, it is essential that the infrastructure is such as to allow the devices with a higher compatibility to be easily inserted or removed. Data analytical components that are module-based need to be developed for dealing with this data handling challenge which in order to remotely control the system or in similar situations can be easily attached on a temporary basis to the fog gateway.

Devices with computational abilities that are restricted need to be developed so that they can be inserted remotely in the system that already exists as the gateway devices, and when the purpose is fulfilled, they can be removed.

Resource restrictions are placed on the gateway devices due to the manner in which they are designed. However, where the available resources on the device are not sufficient to enable completion of the processes, this

could actually hamper them.

As a result of this, certain data analysis processes cannot be completed in time as they cannot work on them, and unless this issue is resolved, fog computing shall continue to face a major challenge in its smooth functioning.

## **6.7. TEMPORARY STATELESS ADDRESSES AUTO-CONFIGURATION**

The use of a constant part in the address field is the foundation stone to route the packet over the network. Such sort of information can be easily concealed. Even when the payload is ciphered, the addresses comprised in the header are conveyed in well-defined text and can be eavesdropped.

The private information which is carried in the packet header should be concealed to data mining and avert tracking. IPv6 addresses can be categorized into two distinctive parts: the topology and interface identifier (IID).

The topology alters for mobile devices and transmits localization information. The IID remain persistent as it classifies a given device. “Data mining” techniques which associate the movement with the address are dependent on the IID tracking.

One of the best suitable approach with the auto-configuration of stateless addresses entails in adapting the IID over time. Thus, it becomes almost challenging to interrelate an activity with a device (or a person) even if the routing prefix doesn’t alter.

The document RFC2462 specifies a procedure for producing a temporary link-local address of a given IEEE 802.15.4 interface without even the requisite for a DHCP server. It also plays a very crucial role in addressing the extension of a temporary random stateless address to global scope tackling for outgoing message.

Pseudorandom sequence with IID is produced with a MD5 hash function from the IEEE 802.15.4 identifier and an unplanned component. A dedicated algorithm looks for determining that the generated IID has not been used already.

The connection of the 64-bits prefix with the 64-bits random IID forms a transient IPv6 address. When a new address is generated, the former one is automatically discarded in order to make sure that it would not use further.



Each application should be enabled with the preference to make use of public IPv6 address or the use of transient address in order to communicate with a given node (RFC3041). A UDP-based application could be exclusive to get the information about the addresses that are in use currently. In such a scenario, a heuristic would be helpful in deciding when the addresses are about to expire.

The APIs must be created in order to permit applications to signify their “privacy” needs with enough granularity. Auto-configuration, with the help of stateless addressing admits a host connecting to a network, forming its address, and instituting a communication with the other nodes without having been authenticated nor registered into a local subnetwork.

A great thanks to this technique as now it is possible for non-authorized users to establish connection to the network and use it. Now, several DoS attacks can be launched only because of the use of stateless addresses produced by auto-configuration (RFC4862).

The final user would be easily and independently activating the use of temporary addresses that defend its private profile while at the same time circumventing the access to some application or services (RFC4941).

The network administrator would be able to successfully deactivate the use of temporary addresses, for example in order to debug effortlessly or for a selected prefix. The use of transient addresses can troublesome applications that make use of private information.

Few servers refute communications which is conveying from clients whose IP address is not in accordance with the DNS name. In case, when there is an expiry of an address before the application has ended, it can also create bugs, resulting in stopping the application.

In addition, in case an application opens numerous sessions, it can assume the client would possess the same address for all sessions. This obligation cannot be ascertained with the use of transient addresses. If a node is using the identical prefix over a certain period of time, changing the IID will not be adequate to defend its privacy.

In order to obtain an efficient temporary addressing, the prefix should not be similar or static for a large number of nodes. Furthermore, the addresses may be spoofed. On a high-density network where transient addresses are generated a number of times, it would be almost challenging to determine between a spoofed address and a legitimate address composed of a non-existent IID and correct prefix. Although, even when the address is spoofed, the owner’s identity will remain safeguarded.



### 6.7.1. Cryptographically Generated Address (CGA)

Cryptographically generated address (CGA) is created with the objective to prevent against spoofed or stolen IPv6 addresses (RFC3972). It is dependent on the use of asymmetric cryptography dependent upon a couple of secret key/public key.

It relied on binding the IID of the address-produced with a cryptographic one-way hash function with the public key of the node. Such a scheme can be executed without any need of security infrastructure or certificate.

The public key of the device is cryptographically associated to its identity that is conveyed by its address. The owner of the address makes use of its secret key in order to sign the message and validate its identity to assure the authentication from its address.

By following this strategy, an attacker can generate a potential address based on a random prefix and its own public key making profit that the CGA is not certified. However, it is worth noticing that the attacker cannot steal the identity of a legitimate node.

There is another challenge that is associated with the use of CGA: There is presently no mechanism available that can validate whether an address coming from a CGA or not. It is usually seen that attackers possess the ability to intercept a CGA address and use it as a non-cryptographically signed address.

Nonetheless, they will face difficulties to generate profit of this hack because nodes provide preference only to signed addresses.

Two insignificant limitations of the use of this CGA for “privacy” are discussed as follows:

- Creating a new address demands huge computing power and consumes substantial energy. This is orthogonal with the demand to often renew the addresses; and
- The public key is disclosed in a “SeND” message. If the transceiver does not want to reveal its identity through the nodes used (multi-hop), they have to create not only a novel address but also a completely original public key. Although, the address is the exclusive identifier of the node at the level of the link layer. Thus, it will allow the node to retain the same public key as long as there is no change in the address.

The CGA scheme is dependent on an RSA cryptosystem. It is generally seen that the RSA cryptography is heavy in nature and is not customized for a use into LoWPANs.

In order to ensure high privacy protection over LoWPAN networks, it is essential to develop a cryptographic address generation scheme dependent on elliptic curve cryptography (ECC).

## **6.8. DISCUSSION OF SECURITY FRAMEWORK FOR SDN**

Several researchers in their studies done earlier have discussed a number of issues related to security. The challenges that crop in a cloud environment have been discussed. There is also a detailed insight into the various cyber based attacks that take place in cloud platforms.

A detailed analysis of the aspects involved in the security of both cloud computing and IoT has been the main focus of another study. The integration of cloud computing and IoT has also been the subject of the study.

It was concluded that a fog environment model can be provided for by cloud computing. An adaptive attribute optimization technique was not only developed but also implemented by the authors so that the prediction of disorders related to dengue fever risks could be efficiently optimized.

It was found out that optimum and positive results could be obtained with a number of parameters through the classification via the proposed algorithm. In order to classify different kinds of tumors, the authors implemented certain computation techniques that were biologically inspired.

The classification process used multilayer perception. Various security threats, along with the possible solutions as well as the characteristics of cloud computing that are important have been analyzed in depth. Presents the numerous vulnerabilities to the security in a categorization framework that is multilevel. The risk levels associated with several attacks as well as the possible attacks have been detected.

## 6.9. CONCLUSION

As discussed in the chapter, the enabling technology that includes IoT, cloud, and social networks as well has taken over in the normal day-to-day functioning of human beings. On the one hand, these technologies have improved the lifestyle and ease of life but the major threat of this is maintain privacy of the user. The security concerns identified and discussed in the chapter related to privacy issues are in need to get resolved so that the only hurdle that these systems have will be resolved.

## REFERENCES

1. Hennebert, C., & Dos, S. J., (2014). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet of Things Journal*, 1(5), 384–398, Available at: <https://hal.archives-ouvertes.fr/hal-03021091/document> (accessed on 1 April 2021).
2. Hitachi.com. (n.d). *Application of Tracking Technology to Access-Control System*. [Online] Available at: [http://www.hitachi.com/rev/pdf/2004/r2004\\_02\\_103.pdf](http://www.hitachi.com/rev/pdf/2004/r2004_02_103.pdf) (accessed on 1 April 2021).
3. Le, A., Loo, J., Lasebae, A., Aiash, M., & Luo, Y., (2012). 6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach. *International Journal of Communication Systems*, 25(9), 1189–1212. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.2356> (accessed on 1 April 2021).
4. Wang, X., & Mu, Y., (2015). Addressing and privacy support for 6LoWPAN. *IEEE Sensors Journal*, 15(9), 5193–5201. Available at: <https://ieeexplore.ieee.org/document/7118632> (accessed on 1 April 2021).

## CHAPTER 7

# Introduction to Social Network and Its Security Issues

### CONTENTS

7.1. Introduction.....	176
7.2. Social Networking .....	177
7.3. Historical Development of Social Networking Sites .....	179
7.4. Types of Social Networks .....	181
7.5. Popular Social Websites.....	183
7.6. Applications .....	185
7.7. Impact of Social Networks on Society.....	188
7.8. Some Security Issues In Social Network .....	190
7.9. National Security Issues .....	195
7.10. Recommendations and Countermeasures .....	197
7.11. Conclusion .....	202
References.....	203

Social networking is one of the most prominent topics nowadays given the increase in usage of internet and social media. In this chapter the basic concepts and historical developments in social networks are explored. The chapter also outlines several types of social networks. Some of the widely known social websites are also explained in this. In addition, real-life application of social network is also highlighted.

Furthermore, few security issues associated with social network, including national security issues, are also highlighted. In the end recommendations and countermeasures to make the social network more secure are brought forward.

## 7.1. INTRODUCTION

It is well known that social networks are one of the easiest and common way of communication these days. It basically outlays the social image of a person. Social networks have the potential to make a person live in a virtual world and make them forget about the actual real-world around themselves.

The network of social relations being developed during daily activity of life can be easily transformed onto one's "profile" and made available for the entire friends or family circle. Then there is a concept of "following" that can turn a nomad into a rock star. The number of pictures a person shares on a regular basis allows them to enhance their presence more on the internet.

It all looks so pleasurable that one would rarely think of goodbye this "world" and becoming an offline monk. But the more attached and comfortable people become with these sites, the more careless and casual they are to share personal details about themselves. It is usually seen that millions of people use a number of social networking sites (SNSs) that appear no less than a menu card in a restaurant.

For instance, Facebook, the world's prominent social networking site, has users far more than the combined population of so many countries. One cannot deny the fact that social networks have become a part of life for every internet user these days, and this trend is likely to increase at a rapid rate in the near future.

With the increase in the speed of the internet and surge in the use of mobile phone and computers, it is high likely that the presence of people on social sites will increase. However, such a large number of users are not aware of the potential risks and threats that arise by uploading sensitive information on the internet.

One of the key reasons why cyber-conspirators prey on these networks is primarily because of user's tendency to upload their personal and sensitive information on the internet that usually include their interests, pictures, social relationships, confidential information, and other useful and critical content, and spread this information to the entire world through SNSs that can be accessible easily.

Employees, too, naively disseminate large amount of personal information on SNS, thus leaving their company's information and data at a risk. The amount of and easily access of personal information present on these sites invited malicious and swindle people aimed at exploiting this information. Because of the sensitivity of this information available on SNSs, there is a need to engage in comprehensive research in the area in order to make this information more secure and safe.

Facts disclose that a large number of social media users generally post risky information online, uninformed of the security and privacy concerns. As the mono aim of SNSs is to gather as many people on their platform, resulting in making the job of the attackers easy and providing them a high rate of investment. The values at the core of networking sites-connecting, openness, and sharing with others-inappropriately are the very aspects that make way for cybercriminals to use such sites as a weapon for various crimes.

Without a vigilant security policy in place, the charming face of social networking could certainly be compromised on the social stature of an individual. The recent surge in such attacks clearly demonstrates that social networks and their millions of associated users need to do a lot of work in order to prevent themselves from organized cybercrime, or risk failing to identity scams, theft schemes, and malware attacks.

It became vital to have full awareness of these risks and challenges in order to avoid potential loss of personal and private information. It is the need of the hour to integrate social networking into the information security policy and user education.

## **7.2. SOCIAL NETWORKING**

Social networks refer to the groups of people, or communities, who share a common interest, background, beliefs, or perception. The social graph can be defined as the broad collection of people, interests, and places that makes

us individual. Nostalgia, one of the major factors and sensation that had directed SNSs a bigger bite of every day's meal. It allows people to get connected with their friends and preserve their memories (Figure 7.1).



**Figure 7.1.** *Social network.*

Source: Image by TheNextWeb.

There are many experts who are of the opinion that Facebook may morph into a “next-generation social operating system.” Many users log into Facebook and other social networks every day and it will only gain importance with time passes as its user base grows.

Social networking is the classification of individuals into specific groups, such as neighborhood subdivision or school community. The nature of online networking makes it easy to find people with similar interests, be they sporting, professional or other extracurricular activities.

The topics and interests are as wide and rich as the story of our universe. As far as online social networking is concerned, websites, such as Facebook, Twitter, or Clubhouse, are the ones that are commonly used for this purpose. These websites are known as social sites.

Social networking websites are basically act as an online community of internet users. This socialization may comprise getting access to the profile pages of other members and also have the facility to even contact



them. Another one of such benefits embrace diversity because the internet provides opportunity to people from all around the world to access to SNSs. This means that while a person living in India can make a friend with a person living in Denmark or United States.

Not only, it will help a person to make new friends, but also enable them to learn about cultures or new languages and learning is always a good thing. As stated, social networking usually comprises of grouping specific organizations or individuals together. While there are a large variety of social networking websites that emphasize on specific interests, there are others that do not.

The websites without a main focus are often indicated as “traditional” social networking websites and typically have open memberships. It suggests anyone can become a member without paying anything, no matter what their hobbies, views, beliefs, or perception are. However, once a person takes an entry into this online community, they can initiate their own network of friends and exclude members that do not share common goals, interests, or objectives.

### **7.3. HISTORICAL DEVELOPMENT OF SOCIAL NETWORKING SITES**

The first social network site, classmates.com, was introduced in the year 1995. The major focus this site was to attract audience from school, work, college, and military circles.

The second social network site was introduced in the year 1996 whose news was Bolt.com and emphasis of this site was broad-spectrum. In 1997, Asian Avenue and SixDegrees.com social network sites introduced and enabled with the features to allow their members to create profiles, list their friends and for community purposes.

Open diary, care 2, gapyear.com and fatki care was introduced as early as 1998 as social network sites. During the initial years of SNSs, friends of one person is not visible to another, but it was allowed firstly by classmates.com to appreciate with their high school or college, thus enhance their network base which is very important for a variety of reasons.

However, at that time, users could not create profile or list friends until years later. SixDegrees was the first one to come up with such qualities. From 1995 to 2001, a large number of community tools initiated supporting several arrangements of profiles and publicly communicated friends.

After this several sites permitted users to generate personal dating as well as professional profiles. After this, the sites provide the access of a person's friend's lists diary pages to others, and thus helping businesses leveraging their business networks. Table 7.1 is showing a complete historical record of social network sites.

**Table 7.1.** Timeline of Social Network Sites.

SL. No.	Launch Years	Names of Sites
1.	1995	Classmates.com
2.	1996	Bolt.com
3.	1997	sixdegrees.com, Asian Avenue,
4.	1998	care, gapyear.com, Open Diary, Fotki
5.	1999	Advogato, hr.com, Kiwibox, Cyworld, vampire.freak.com, MakeOut, LiveJournal, black planet
6.	2000	English, baby! friends Reunited, DXY.cn, hobo, writeA-Prisoner.com, deviant ART, maxi
7.	2001	Thinks, Fruhstuckstreff, cozy cot, party flock
8.	2002	Film affinity, fraudster, footslog, Last.fm, iWiW, hub culture, Travellerspoint
9.	2003	Couch surfing, hi5, LinkedIn, pure volume, WAYN, delicious, MySpace
10.	2004	Cob, Orkut, Facebook, Zoo.gr, flicker, Hyves, a small world, tagged
11.	2005	43 Things, Douban, Buzz net, focus.com, Ning, Biip.no, Bebo, Travbuddy.com, LibraryThing, Mocospace, Blogster
12.	2006	Anobii, PatientsLikeMe, Crunchyroll, Jaiku, Twitter, Vkontakte, Shelfari, Cafemom, GamerDNA, Goodreads
13.	2007	Flixster, Tylted, Quechup, Virb, Wiser.org, eToro, weRead, Geni.com, Elixio, Bigadda, Fubar, Fuelmyblog, Dailystrength
14.	2008	Cross.tv, Fetlife, Yammer, Busuu, gays.com, GetGlue, academia.edu, the sphere
15.	2009	Filmow, Skoob, DailyBooth, Foursquare, Fullcircle, Weibo, Sina
16.	2010	Audimated.com, Jiebang, Laibhaari, Blauk, Lagbook, MillatFacebook, Goodwizz, Termwiki, Diaspora*, Students Circle Network
17.	2011	Faces.com, Google+, Pinterest, playlist.com, Wellwer

Source: <http://www.iosrjournals.org/>.

## **7.4. TYPES OF SOCIAL NETWORKS**

There are a number of ways to categorized SNSs. We have chosen to follow, with some extension, the division developed by Digizen (2008), an institution which aims at promoting secure activities on the web.

### **7.4.1. Profile-Based Social Networks**

Profile-based social networks are one of the most popular social networks. Within the past few years, a large number of people across the world have created their profile on these sites. These profile-based services are mainly organized around members' profile pages. Some of the widely used ones are Facebook ([www.facebook.com](http://www.facebook.com)), Bebo ([www.bebo.com](http://www.bebo.com)), MySpace ([www.myspace.com](http://www.myspace.com)), Hi5 ([www.hi5.com](http://www.hi5.com)), and 9jabook.com are all good examples of this.

These sites are generally used for entertainment purposes and to increase the interaction and communication between people. After the arrival of these, people came closer as it allows them to connect to anyone, no matter how far a person is living.

### **7.4.2. Content-Based Social Networks**

Given the nature of these services, user profile plays a critical role in finding and organizing connections. Additionally, user profile may play a minor role in content posting. Photo-sharing site Flickr ([www.flickr.com](http://www.flickr.com)) is another example of a social networking service where groups and comments are revolved around pictures. Shelfari ([www.shelfari.com](http://www.shelfari.com)) is one of the existing brands of book-focused sites, with the members 'bookshelf' being a principal point of their membership and profile.

It usually works on the model of paying for the membership and then use the services for a particular period of time. Nowadays, on these websites, there are different types of membership, standard member at economical prices to premium membership, which delivers advanced services.

### **7.4.3. White-Label Social Networks**

These sites provide the opportunity to their members to create and join communities-this means that users can create their own 'mini-MySpace's,' small scale, personalized SNSs about whatever the initiator wants them to be about.

Some of the decent examples of these are WetPaint ([www.wetpaint.com](http://www.wetpaint.com)), Quora ([www.quora.com](http://www.quora.com)), Wikipedia ([www.wikipedia.com](http://www.wikipedia.com)), and WikiLeaks ([www.wikileaks.com](http://www.wikileaks.com)), which uses social wikis as its format to enable social networking.

#### **7.4.4. Multi-User Virtual Environments**

Gaming is one of the most important way for teenagers and youngsters for entertainment. Earlier, it was accessed by people using the device, which is a combination of hardware and software. Nowadays, with the increase in the speed of internet and highly advanced technological devices, online websites providing live and virtual gaming experience came into existence.

It allows their users to play games online along with their friends whether they are with them or living in another country, resulting in enhancing the gaming experience. Some of the popular gaming websites that are used for this purpose are RuneScape ([www.runescape.com](http://www.runescape.com)) and virtual world sites like Second Life ([www.secondlife.com](http://www.secondlife.com)).

#### **7.4.5. Mobile Social Networks**

It is important to note that many SNSs are now assisting mobile access to their services, allowing their user base to interact with their personal networks through their mobile phones. Two perfect examples of this are Bebo ([www.bebo.com](http://www.bebo.com)), and Facebook ([www.facebook.com](http://www.facebook.com)). Progressively, there are mobile-led and mobile-only-based communities emerging, such as MTN ToGo and Glo AfriChart all in Nigeria.

#### **7.4.6. Micro-Blogging**

Nowadays, there are several services that let users post their status on a regular basis, i.e., short messages that can be updated in a way to aware people about their mood, what there are feeling, where are they, or what they are doing. These types of networks make it easy for the users to be in constant touch with what their network is thinking, doing, and talking about. NairaLand ([www.nairaland.com](http://www.nairaland.com)), Twitter ([www.twitter.com](http://www.twitter.com)), and Wayn ([www.wayn.com](http://www.wayn.com)) are examples.

#### **7.4.7. Social Search**

Sites such as LinkedIn ([www.Linkedin.com](http://www.Linkedin.com)), Wink ([www.wink.com](http://www.wink.com)), and Spokeo ([www.spokeo.com](http://www.spokeo.com)) yield results by searching public profiles

of many individuals across the SNSs. It generally works by enabling their users to search for the people by their name, location, interest, and other information available publicly on profiles, allowing the creation of web-based ‘dossiers’ on individuals.

#### 7.4.8. Local Forums

Though these forums are generally not included in social network definitions, place-based fora such as Onsnet ([www.onsnetnueen.nl](http://www.onsnetnueen.nl)), Eastserve ([www.eastserve.com](http://www.eastserve.com)), and Cybermoor ([www.cybermoor.org](http://www.cybermoor.org)) provide a localized form of social networking, linking offline activity with online platform.

#### 7.4.9. Thematic Websites

Sites such as Netmums ([www.netmums.com](http://www.netmums.com)) also include a local dimension by putting mums in touch with others in their locality, where allows them to share recommendations, information, advice, information on schools, any news or event happening in their nearby place, and are able to network both at the local and national levels. In addition, there are also sites for people having a disability such as [www.deafgateway.info](http://www.deafgateway.info) that aimed at providing a place for deaf people to interrelate.

### 7.5. POPULAR SOCIAL WEBSITES

Major modern SNSs include Twitter, Facebook, YouTube, Google+, LinkedIn, and MySpace. All these are illustrated and discussed as in Figure 7.2.



**Figure 7.2.** Popular social websites.

Source: Image by Resort Development Organization.

### **7.5.1. Twitter**

Twitter was founded in 2006 by Odeo, Inc. It became a public network in 2006. It primarily aimed at providing a real-time, Web-based service that allows users to post short messages for other users and to comment on other user posts.

Tweets are extracted from Twitter. A tweet is basically referring to a small message whose total number of words cannot be more than 140 in order to communicate thoughts. This small limit of characters is to maintain its legacy by not making it boring.

After it came into existence, a large number of people created their accounts, and it has been continuously increasing. Microblogging is a newer blog option made popular by Twitter. Now, there are almost 340 million people on Twitter, which is more than the combined population of many countries.

### **7.5.2. Facebook**

Facebook was first launched in the year 2004 as a social networking site by a Harvard student, and only Harvard students are allowed to use it in order to communicate with each other. However, gradually it was opened to other universities and colleges as well, and after some time for all. In the year 2009, it became the largest social networking site.

It is till now the largest photo-sharing site. People do not have to pay anything to use Facebook. It is based on the model of generating revenue by charging companies who post their advertisement on Facebook in order to target or find their potential customers. Marketing strategists have found Facebook to be one of the most important platforms as it allows a range of personal and organizational interests.

### **7.5.3. YouTube**

YouTube is basically a video-sharing platform where countless number of people can discover, share, and watch user-generated videos. It is a website of participatory culture. Here, anyone living in any country can share their own videos, and anyone can watch it. It was first introduced in 2005, and after its inception, it becomes the most popular video-sharing internet website.

As YouTube is a part of Google, so there is a need to have a google account, and one can use YouTube with the help of a google account. Now

a lot of people have become an entrepreneur by creating their own YouTube channels and have millions of users.

It provides good income opportunities to the people who have their YouTube channel as it is based on the model of sharing revenue generated from the advertisement.

#### **7.5.4. MySpace**

This social networking site bases its existence on advertisers who are paying for page views. It provides a lot of opportunities to the users to do different things at the same time. MySpace are present in several countries such as Ireland, United Kingdom, and Australia.

#### **7.5.5. LinkedIn**

This is a professional network website that provides a platform to its users participate in networking with each other. It is basically for professions who used it to make contacts with other professionals either for looking for a job or for making business tie-ups.

By creating an account on LinkedIn, one can make an account with individuals that have similar interests. LinkedIn is now used as the most common and prevalent social networking site for companies to on-board new employees.

These are just a few of the social networking choices present on the Internet today. Others include Instagram, Friendster, China-based Renren, Vox, LiveJournal, Bebo, and Flickr. The impact of these modern social networks on health, social, economic, and political arenas has far exceeded the expectancies of many. Many experts see the future of social networking applications in lesser, custom-made, or specialized private systems.

### **7.6. APPLICATIONS**

Social networking applications have become one of the most critical services that stipulate Internet-based platforms for their users to intermingle socially. Common applications comprise computer-mediated social interaction, business, education, finance, politics, healthcare, religion, and crowdsourcing.

### **7.6.1. Social Interaction**

SNSs assist computer-mediated social interaction and provide the opportunity to make connect with the people having common interests and activities across economic, social, political, and geographic borders.

They are generally known for a modern form of entertainment. People usually make use of it use to meet new friends, look for old friends, identify people with similar background and interests, and keeping in touch with old acquaintances.

They also postulate an online environment for people to connect and exchange personal information for dating purposes. Some job seekers make use of social networks in order to find jobs, thus increasing their likelihood of getting job offers and finding lucrative employment.

### **7.6.2. Education**

Social networks are significantly impacting the way ways how educators and students engage in learning. They are now used for studying, content sharing, and educator professional development. Social media are also used by Scientific communities in order to exchange knowledge.

Librarians and Researchers generally make use of social networks steadily in order to maintain professional relationships and disseminate or spread ideas across different platforms. Social media can become learning and research networks.

Social networking media such as Twitter, Facebook, and Instagram are extensively used at many universities, with each university having at least a page on a site. Privacy, time-consumption, real friendship, and miscommunication are few challenges that the education sector faced through the social networking. While on the other side, flexibility, convenience, repeatability, and accessibility are the important benefits.

### **7.6.3. Business**

Social networking between businesses is another great application. It can be turned as an effectual promotional tool for entrepreneurs, businesses, musicians, actors, or artists. Companies make use SNSs in five major ways: to create awareness of brand among its existing and potential user, as an online reputation management tool, for recruiting, to learn about new competitors and technologies, and to intercept potential prospects.



SNSs are also very useful for businesses to advertise their products, recognize the needs of consumers, and congregate opinions on varied perspectives. Potential prospects for global finance are formed through the use of virtual currency in social networks.

Social networks provide the way for consumers to share their personal experience that allows early adopters to engaged in well-versed purchase decision and lessen the danger of buying a new product.

#### **7.6.4. Healthcare**

It is generally seen that social media provides several types of social connectivity among different stakeholders such as patients, doctors, and caregivers. Social networking is basically an effective tool for learning and teaching for nurses and doctors as SNS is used to provide new information from research and contribute in providing quality care to their patients.

It was observed that virtually all aspects of healthcare can be affected inherently by these technologies. Examples of health-related SNSs include Inspire, HealthChapter, ToolsToLife, DailyStrength, LiveStrong, Health Care 2.0, Everydayhealth, MyCancerPlace, Revolution Health, Planet Cancer, Prostate Cancer Infolink, No Surrender, SoberCircle, diabetic connect, Psych Central, and DailyPlate.

#### **7.6.5. Politics**

It is worth noticing that social networking seems to be impacting political movements and political life across the globe. It has persuaded voting and induced social changes, uprisings, unrest, and revolutions across the world. Social networking will make government to be more answerable and empower citizens to exercise freedom of speech.

It also provides the platform for people to engage in the democratic process and to motivate the younger generations involved in politics. For instance, Barack Obama positively assimilated social media in his campaign in 2008, active participation of people, empowering volunteers, and vastly increasing donors. Obama was the first US president who has a comprehensive understanding of the power of social media.

## 7.7. IMPACT OF SOCIAL NETWORKS ON SOCIETY

As social media aimed at fulfilling cognitive, personal, affective, and social needs, it is in turn impacting day-to-day life, including relationships, marriage, family, church, school, and entertainment. Like any other technology, the challenging use of social networking media and its opposing effects have become widespread (Figure 7.3).



**Figure 7.3.** *Effect of social network on society.*

Source: Image by Associations now.

Although there is a minimum age needed to create an account in social media networks, many children/students falsify their actual age and join these platforms. These students learn about privacy and safety issues in a chaotic way and suffer from training insufficiency.

According to various studies, it was found that the use of social networks among students, especially in developing countries, constitutes disturbances because students spend a significant proportion of their time on the networks.

In the past, some viewed social networking as an interruption and proposed no educational assistance for students studying in junior or high school.

So, jamming these social networks was cogitated a form of armor for students against addiction, wasting time, cyberbullying, sexual predators, and privacy theft. While others opine that the schools that block social networking services are blocking students from acquiring the critical skills needed in directing the digital world with conviction and consequently consider blocking SNSs as counterproductive.

Some have opposed that social networking is an impoverished version of traditional face-to-face social interactions, and it harvests negative consequences such as depression and loneliness for users who use the technology at a higher rate.

It is often observed that social networking services have been used for child pornography and bullying purposes. As there are no restrictions as to what individuals can possibly post online, people often post offensive pictures or remarks.

It resulted in causing a bad impact on the brain of children. As we know that there nowadays there are a lot of negativity around the world, which some evil people pose online in order to create polarization in the society. Such things significantly affect the brain of teenagers and sometimes may even trigger them to take some wrong steps in their life.

Privacy on SNSs is an important issue. For instance, third parties often use information (such as profile and personal information) posted on social networks for a number of purposes. Privacy may involve whether companies possess the right to keep an eye on employee's social network profiles. Privacy concerns vary from users to users based on their personality types and gender. It is usually believed by many that women often have more privacy concerns as compared to men.

Another dark side of social networks is that they are gradually becoming widespread tools for methods of ending friendships and relationships. There is a need to recognize that social network does not continue to be bastardized by bad influences that prey on the susceptible.

It is usually seen that culture plays a significant role on how people interact with each other on social networks as it outlines rules and norms on what is being acceptable and what is not. Culture can impose restrictions on people to whom a person can interact if they want to withhold their identity. For instance, a global culture has occurred in India as a consequence of the

SNS; the technological advancement has not only improved the quality of life but also the social architect of society.

## **7.8. SOME SECURITY ISSUES IN SOCIAL NETWORK**

It was observed that social media had been compromised from the security perspectives, resulting in posing a significant threat to the users with relation to their intellectual, personal, career property. In this section, the major area of focus is to outline the security, which are vulnerable to social media and its users. These security threats arrays from privacy setting threats, identity allied attack, anonymity attack, social attack, and information leakage attack.

Though few of such threats can be combed by solely edifying the users on the potential threats. For example, according to a survey, it was revealed that 25% of Facebook users don't worry about privacy settings (Bullas, 2014).

### **7.8.1. Malware**

Malware stems from malicious and software. It generally included viruses, worms, and Trojans. Survey shows that 36% of the companies have had to compromise with their systems once in their lifetime, and it was only because their system was infected with malware through social media 2009 while it has risen to 70% in 2010 (Vanheuanddy et al., 2010).

Some of the existing malware are Twitter Worm and Koobface. Koobface is a worm that can be disseminated via social media through Facebook. This type of worm can be blow-out via the messages that users send to their friends; this message could be in any form, whether it is a text message.

Video message or voice message. When a person receives these kinds of messages from their friend with an attached link for the video, the user if they click on the given link may be required to download or update the Flash Player. If they accept on the conditions to download the Flash Player, resulting in filling the computers with a lot of worms and viruses that can significantly damages the computer (Gunatilaka, 2011).

It is also important to note that the Twitter Worm is another attack common with users of the Twitter site. One type worm is Profile Spy worm, that provide the attacker to tweet link for downloading third party application call Profile Spy.

When the users click on this link to download the app, it will initiate a form to gather user personal information, and with these details, it will maintain posting malicious messages to the followers of the Twitter user. Another worm associated with Twitter is a worm that creates a fake invitation link that guides users to a malicious attachment comprising e-mail addresses from compromised computers and disseminated by making its copy into removable drives and folders (Qing, 2014).

### **7.8.2. Digital Dossier of Personal Information**

In this situation, an attacker collects the personal data of targeted victims on storage space and subsequently uses it for detrimental reasons on the victim's personality. As the majority of the social media websites provide search for user's profile, the attacker can mine out the potential victim into his storage system and then use it for affecting or damaging the reputation of the profile holder (Al Hasib, 2008).

### **7.8.3. Spam**

Spams are unsolicited or unwanted messages that are sent to social media or online e-mail account holders. The majority of the times, such kind of messages are malicious, though some have the objective to initiate advertisement.

The use of spam has been in existent for prolong period of time as it is into use on the Internet when it started, and they have developed with the advancement in the communication networks, not to augment it but as a sidestep the well-intended communication of the legal account owners.

According to a survey conducted in the first half of 2013, the growth of social spam media has risen to 35% just on typical account, indicating out that one of seven social posts comprise spam (Nguyen, 2014).

It is worth noticing that social spammers use different medium in order to entice the customers. It basically comprises of text-based, image or picture based and URL based. The social spam based on URL generally skips the text, leaving only the link for the user to view, thereby hiding the real purpose of the message in order to grab the innocent person.

Image-based social spams are also in existent nowadays, it basically works by showing the attractive images or advertisements with the strength of enticing the social network users to click it. It typically lures the user to use other's online computers that download Trojans into the computer. As

far as text-based social spam are concerned, they generally sent to the users with the object of phishing in mind.

The security measures that are relevant in this scenario is to use available message filtering functionalities that are been provided by the SNS that the user have created an account with. In addition, their third-party applications that sense chief social network security threat such as spam.

#### **7.8.4. Cross-Site Request Forgery and Cross-Site Scripting**

This type of attack usually happened when a malicious website, blog, e-mail, or program, opened on a user computer, making use of the victim browser to initiate connectivity to another website, and then uses login credentials (presented to a website that the legal user may have presently connected), of the unsuspecting user to engage in malicious attack on the website it has connected. An instance of cross-site request forgery can be attained through RESTful API. RESTful API has been engaged in recognizing the interconnection between social networks and applications.

Social network sites have provided APIs for these apps in order to recover user information. Mashup application such as HootSuite was used to gain access more than needed data from Facebook. When HootSuite was approved to connect to Facebook, it was able to get access to the basic information such as profile information, family information, relationship, friend list, and others (Zhang et al., 2013).

#### **7.8.5. SQL Injections**

Web application developers have had their database attacked by invaders via the use of SQL injection. SQL injection refers to a technical approach adopted by attackers in a way to gain access to database. Alleviating this attack is typically left to the developers of the social network, so that profile information of users of these social networks will be protected and secured.

Hackers are able to perform mischievous SQL query in contradiction of underlying databases of susceptible social network apps. According to a report published by Slow PC (2014), it was discovered that Twitter and Facebook were the sites that have underwent the highest number of SQL attacks in comparison to government websites.

### **7.8.6. Identity Theft**

Identity theft in social network has now the need of the hour in popular social networks with the increase in such thefts. The social network juggernaut, Facebook, and Twitter, users have constantly undergone this attack. Mali (2014) stated that 12 million people have become the sufferers of identity theft and fraud in 2012, and the expected monetary loss of these kinds of attack was pegged at \$21 billion.

Identity theft usually happens when attackers steal identifying data of other users such as profile picture, date, and place of birth, and then create another similar fake profile. These types of accounts are generally used for deceitful purposes.

### **7.8.7. Phishing**

Phishing is basically referring to a technique mostly used by the fraudsters to trick online users to give sensitive information such as password, to an illegitimate website. According to a report published by the Symantec Cooperation on internet security threat demonstrated that there was a plunge in the phishing attack witnessed usually by e-mail users from one in 299 e-mails in 2011 to one in 414 e-mails in 2012.

The major thing to notice in this is that this fall in such threats does not means that the attackers reclined, but they have changed the way of attacking by using social media. Wood (2013) had enumerated some safeguards that that should be taken by the social network users in s way to avoid the attack by phishers. The social network address must be tested to make sure that it is not a typosquatting site that is typically used to apprehend user's credential.

Additionally, users should also need to be fully aware and attentive by looking for the social website's certificate before using any website in order to make sure that the logging details are not revealed into the hands of scammers.

Although, users are from time to time being aware to make use of security software, they should also be vigilant by using different passwords across distinctive online accounts without giving them permission to browser to save the password for future usage.

### **7.8.8. Mobile Phone Attack**

It is worth noticing that out of the 6.6 billion people living on this earth, 5.9 billion people have access to mobile phones. From this, one can easily



estimate that how easy it is for attackers to target the large number of populations easily.

Nowadays, it is more common that people become the victim of the mobile phone attack. It is usually done by number of ways, either by sending text message to user's phone, or by calling or video message. It generally happens with those that have lack of awareness and they unintentionally click on some links that are being sent by invaders, resulting in compromising with the security of their mobile,

### **7.8.9. Stalking and Cooperate Espionage**

It is generally seen that the leakage of the cost organizations a significant amount of loss, both in monetary terms as well as at reputation front. Social networks will likely to perform as a platform to involve employees in unintentionally disclosing sensitive company data. Some of this information are emancipated to social network without knowing that they can be used for variety of purpose in contrast to the one for which it was intended for.

For instance, Scott McClellan, Hewlett-Packard vice president on cloud services, once slip up on his LinkedIn profile, when he revealed the comprehensive detail of HP's cloud computing platform. Although, before he was managed to destroy that information from his LinkedIn page, the news media took over it and disseminated it on different platforms, resulting in making Amazon and Microsoft to have a peep into HP's plan in this respect (Hill, 2011).

### **7.8.10. De-Anonymization Attack**

Anonymization in social network opens the ways for users to hide information that can make them known. Such information comprises of large amount of data from basic details such as names, address, pictures, to critical and sensitive data.

The reason for this concealment is to safeguard users from advertisers, data mining researchers and application developers who will infringe on user's privacy. Although, there have been some researches that have confirmed that this de-anonymization of online social network users is conceivable.

Wondracek et al. (2010) signified the use of public records such as birth date and marriage to de-anonymize an online user and even the membership group the user belongs to on the social network. In addition, chapter revealed



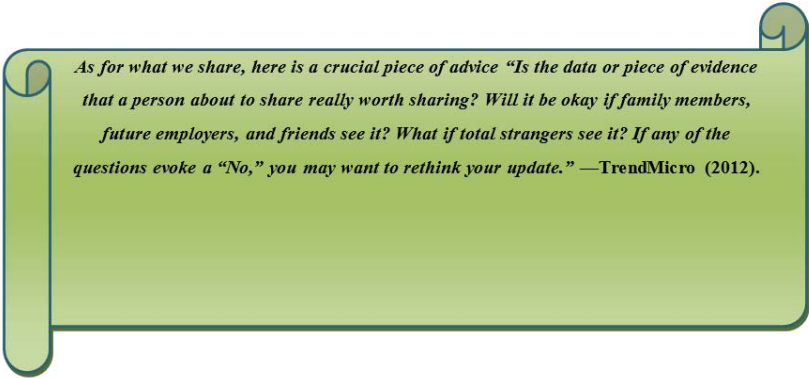
that an amalgamation of data can be produced from some social networks about an individual as a basis for deanonymizing the user. Hence, de-anonymization attack has become another hazardous tool on social network used by phishers in side-stepping user's privacy settings.

### 7.8.11. Awareness

There are personal and general security measures that a user must take, though this is only reliant on the awareness a user has access to. It is often seen that majority of the social network sites have their own security settings standard and information that potential users are supposed to read.

As a user, it is vital one should run through them and protected the best scenery that will provide them with needed privacy. Setting hard to predict password is also a good security measure from the perspective of the user.

When browsing social network sites, what the users contribute and sees or disseminate may be a loophole through which an attacker can advance ingress to attack. For what a person might be view, he or she should always be aware of the fancy story, URLs, and images. Consider the advantage versus the hazard of clicking links, text or images one does not trust.



*As for what we share, here is a crucial piece of advice "Is the data or piece of evidence that a person about to share really worth sharing? Will it be okay if family members, future employers, and friends see it? What if total strangers see it? If any of the questions evoke a "No," you may want to rethink your update." —TrendMicro (2012).*

## 7.9. NATIONAL SECURITY ISSUES

Experts are of the opinion that cyber-attack could come from anywhere—an individual or someone sitting overseas, any terrorist organization, or a country. But, within the past few years, it was observed that the number of cyber-attacks aiming at infiltrate national systems is on the rise—and the ever-magnifying web of SNSs could prove problematic for national cybersecurity (Figure 7.4).



**Figure 7.4.** *National security issues.*

Source: Image by WPBegginner.

Continuous updates of social networking technologies are posing significant potential threats for government in order to maintain their transparency and security. This is due to the fact that many agency employees use Facebook, Twitter, and similar social networking external sites.

Because of this, it would become difficult to keep an eye on each of them and check whether the information is leaked from which end. Keeping such kinds of problem in mind, many government officials at all levels are reconsidering their policies.

Information being disseminated on social network sites can be a critical resource for some, as targeted phishing attacks use authenticated information gathered from the web and identification checks used by legitimate sites.

The potential harm of placing too much private information online, especially on SNSs, was brought to light when the wife of the chief of the British secret service MI6 displayed extremely instructive details about their friends and residence on her Facebook page.

During the 2008 terrorist attacks in Mumbai, India, for instance, people on the scene sent Twitter updates, which includes the emergency contact number for the U.S. State Department's consular call center. The State

Department's Deputy Assistant Secretary for Public Diplomacy used Twitter postings to stipulate updates on her personal experiences.

Recently, in the Arab countries, people that have spent years under the dictatorship have risen up and said "no more." Few years back, in a way to manage an endurance movement to an oppressive government, one had to roam outside and look for the like-minded people (by cautiously not caught by the secret police) and find a safe and secure place to quietly discuss matters.

Even if one could get a noteworthy revolt in a dictatorship, he or she would most likely to be sent to jail or be killed. The only way to get a tyrannical regime to breakdown back in the "old days" was for the economy to go belly up, the soldiers not getting remunerated, consequently would no longer guard the dictator (The Masked Walnut, 2011).

But one should thank the God for the rise of internet SNSs. Now, it is possible to sit at home and gather the people of likeminded people to create a community in order to attain the common goal. With Twitter and Facebook or even 9jabook, one can now gather and organize thousands of people and mobilize them. The majority of these people will not have met tangibly until they are essentially at the protest.

A dictator can no longer "call out the tanks" because few minutes after they do their will be a live feed being broadcast on YouTube. If they are irrational enough to jerk shooting people, there wouldn't be ahead of a foreign government in their right mind not reproachful the actions.

If it can happen in Tunisia and Egypt, it can happen anywhere, and all governments on earth are careful and aware about this. So, it is the duty or responsibility of every government to be fully aware and remain cautious that online social networking institutes great danger to national security!

## **7.10. RECOMMENDATIONS AND COUNTERMEASURES**

### **7.10.1. Encourage Awareness-Raising and Educational Campaigns**

Nowadays, given the increase awareness of privacy and security settings on social networks, it becomes important to educate users by using contextual information on a real-time basis. This is already the case in some situations but it should be encouraged as best practice. In addition, there

are efforts to publish user-friendly community guidelines instead of “terms and conditions”, which can be quite intimidating to read for non-technical audience.

Such guidelines should use accessible language in order to make sure that the users can easily understand the rules of the site. The clearer the guidelines are, the more likely the users will abide by them:

- To help improve performance, websites and apps store frequently used data, such as user profiles, to cache.
- A person should be recognizable in pictures similar to the way they are recognized in the real world.
- The nature or size of the audience which has access to content may not be as probable in an offline circle of friends.
- It is also important to note that a person should not accept the friend requests from untrusted users as it could lead to phishing and spam.
- Images that embrace information and which can be used to identify a person or pinpoint location.
- Images can also give away private data about other people, chiefly when labeled with metadata.
- Images may also comprise of embedded data that can recognize the device used to shoot them and thereby implicitly identify the owner.
- There may also be the presence of profile information in some search results even if one believes that it is private.
- The probable exploitations of information posted on social network sites (e.g., when it comprises location data) for the objective of stalking.

While the majority of the social network sites already confine users from posting location data, it is nearly difficult to avert users from posting it unintentionally in messages and posts on comments areas or on public notes.

Many social network sites are already banning certain data types (e.g., zip codes). Best practice as to banned data types on SNSs should be well-defined and endorsed on all sites. At a minimum, users should be motivated to abstain from public disclosure of real-world contact information (e.g., Landline or mobile-phone number and residential address).

### **7.10.2. Review and Reinterpret Regulatory Framework**

Social networking sites present numerous instances, which were not predicted, when present legislation (particularly data protection law) was formed. One can interpret from this is that certain issues could not be able to clarified. In certain scenarios, the present legal framework could not be extended or altered. The regulatory framework which is responsible for governing social network sites need to evaluated and, were crucial, altered.

Some of the specific issues that should be taken into consideration which reviewing and reinterpreting regulatory framework are discussed as follows:

- What is the legal position if the content generated by the users are deleted by the service providers if it is categorized as SNS spam?
- What is the legal position in case the image is tagged by the third parties?
- Who is responsible for finding flaws in security, resulting from user-generated scripting or mark-up?
- How should users be aware or communicated about the privacy policies of embedded third-party widgets?
- What exactly composes personal data in an SNS environment?
- What is the legal position in case of profile-squatting?
- Should the sharing of some classes of data by minors (location data) be made illegal?

### **7.10.3. Increase Transparency of Data-Handling Practices**

There is need to enhance the transparency of data handling practices of social network sites in relation to the existing data protection law and best practice is recommended. For instance, European data protection law, needed explicit and clear notice to be given to data subjects of:

- The objective for which the data is being used (including the secondary usage of data).
- Any third-party receivers of the data.
- The existence of a means of rectification and access. The accuracy and transparency of data handling statements, particularly in relation to third party widgets including survey responses and mood indicators from recognized individuals, should be inspected since existing language is often uninformative and vague.

- Users should be given precise information on what is done with their data before and after the closure of account.

#### **7.10.4. Discourage the Banning of SNSs in Schools**

It was observed that a large number of schools are restricting or banning the use of social network sites in schools. Therefore, it is highly advisable that education policymakers and schools should carefully examine the likelihood of banning SNSs since this acts as a deterrent to the reportage of bullying.

It also means that adults and teachers are less likely to acquire the skills required to monitor and mentor young people in this area. Finally, it also means that an esteemed educational resource is lost.

SNSs need to be used in an open and controlled way (i.e., not discouraged or banned), with coordinated campaigns to educate teachers, children, and parents. This would have a wider knock-on effect as many of the susceptibilities defined in this chapter can be tackled solely by fostering awareness and as children in turn educate their teachers and parents.

One cannot toss the entire blame on technologies for bullying behavior, but it is the individuals who misuse them. Because of this reason, education, the modeling of the positive use of technology by teachers, peers, and adults and community self-regulation are all critical areas in fighting cyberbullying.

#### **7.10.5. Provider and Corporate Policy Recommendations**

It is generally seen that the strength of authentication chosen in SNS environments varies on the social network sites. Many social network sites get the advantage from the potential to subterfuge as another persona, and therefore this is not suitable.

The advantage can comprise educational profiles, safety through harmless and anonymity experimentation. Virtual worlds are actually a display of this type of network. Although, in certain types of SNS, both social service providers and their clients can extract the advantage from sturdier authentication and the vaster validity this lends to claims made on SNSs.

Examples comprise so-called white-label SNSs such as Academy and more professional networks, such as LinkedIn that can made into use for professional purpose. On all networks, authentication methods which can distinguish bona fide fellows from spammers are also beneficial.

It may also be probable that, if stronger authentication process were made more user-friendly, it would not act as a deterrent to enrollment. In fact, it may result in having the contrasting effect by enhancing the trust positioned in others on the network.

There are a variety of added authentication factors that SNSs could use to augment their offer by lessening the level of troublesome and fake memberships. These range from simple e-mail verification through CAPTCHAs and recommendation-only networks (in which a person can enrolled only if he or she is invited for the same) to physical devices such as identity card readers and mobile phones, where these have been organized (e.g., as part of a wider eID pilot).

Each method has its own characters with relation to the ease of usage, strength of authentication and extra privacy risk (e.g., some users would likely to feel that it is invasive to have their profile associated with a government-issued identity number; while others may not likely to reveal their phone numbers), so there is improbable there will be a single solution.

### **7.10.6. Implement Countermeasures Against Corporate Espionage Using SNSs**

One of the important factors in circumventing the social engineering attacks is employee security awareness. Sadly, there is no silver bullet for distinguishing an attack before it results in greater damage. It is well known that every company has its own vulnerabilities and characteristics.

Just as a social hacker needs to acquaint themselves with these peculiarities, protective measures have to be personalized to a company's explicit necessities in a way to be effective. Protection can be achieved only by ensuring that staff would be able to recognize the difference between defined processes and requests that diverge from these definitions.

This, of course, demanded exhaustive security awareness among employees. The following steps are suggested for the stoppage of social engineering attacks which is caused by the dissemination of information on SNSs:

- It is important to aware employees that they need to be as aware and as cautious as they are in their real life.
- Establish a security policy comprising the use of social network sites.
- Promote the idea that the more the information is being

disseminated, the more likely they are vulnerable. At a minimum, social network service provider should needed a membership of a network before enlightening its members or their relationships. This is especially critical as no single member of the network (e.g., Barclays Bank) is liable for such a privacy setting.

### **7.10.7. Maximize Possibilities for Reporting and Detecting Abuse**

Policies and systems for managing illegal action and activity that halts terms and conditions should be erected into the design of the application. For example, if a member of the public an offensive image on a certain page or group, there should be a clear and transparent procedure for how this will be dealt with, integrating protection against bogus reports and, where applicable, using reputation aggregation systems to engage in decision making. Similar policies and systems should be in place for concerns related to law enforcement.

## **7.11. CONCLUSION**

Social networking is nowadays significantly popular with the increase in the internet usage. It is now severely under attack and appears likely to be at the target of the attackers as its popularity grows. The degree at which it is vulnerable depends upon the users how they implement and react measures to ensure privacy and security.

What happens to security measures on the national level? Governments will play an active role in order to make the social network secure and they need to take significant efforts to crack down on existing cybercriminals and discourage new hackers from joining the dark side.

These efforts need to be applied at both the global and national level to ensure that criminals and crimes cannot be abetted and harbored by rogue nations ignoring global regulation. There is a need to make new laws and ensure transparency and provide protection from criminals in order to ensure secure behavior by those entrusted with sensitive data—who will undoubtedly continue to disclose information in ever-greater amounts, as it was observed throughout the past decade.



## REFERENCES

1. Abdulhamid, S., Ahmad, S., Waziri, V., & Jibril, F., (2021). *Privacy and National Security Issues in Social Networks: The Challenges*. [ebook] Available at: <https://arxiv.org/pdf/1402.3301.pdf> (accessed on 1 April 2021).
2. Abhipedia.abhimanu.com. (2021). *Social Media and Security Challenges Issues and Analysis @ Abhipedia Powered by Abhimanu IAS*. [Online] Available at: <https://abhipedia.abhimanu.com/Article/IAS/NDM5MAEEQQVVEEQQVV/Social-Media-and-Security-Challenges-Security-Issues-IAS> (accessed on 1 April 2021).
3. Accan.org.au. (2019). *Introduction to Social Networking*. [Online] Available at: <https://accan.org.au/files/Tip%20Sheets/ACCAN%20Basics%20of%20Social%20Networking.pdf> (accessed on 1 April 2021).
4. Assaad, W., & Marx, G. J., (2016). Social network in marketing (social media marketing) opportunities and risks). [eBook] *International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)* (2<sup>nd</sup> edn.). Available at: <http://airccse.org/journal/mpict/papers/0911ijmpict02.pdf> (accessed on 1 April 2021).
5. Bhagwat, S., & Goutam, A., (2013). *Development of Social Networking Sites and Their Role in Business with Special Reference to Facebook*. [eBook] Available at: <http://www.iosrjournals.org/iosr-jbm/papers/Vol6-issue5/B0651528.pdf> (accessed on 1 April 2021).
6. Bozkurt, A., Karadeniz, A., & Kocdar, S., (2019). *Social Networking Sites as Communication, Interaction, and Learning Environments: Perceptions and Preferences of Distance Education Students*. [eBook] Available at: <https://files.eric.ed.gov/fulltext/EJ1161784.pdf> (accessed on 1 April 2021).
7. Das, D., & Shankar, S. J., (2018). *Social Networking Sites: A Critical Analysis of its Impact on Personal and Social Life* (14<sup>th</sup> edn.). [eBook] Available at: [https://www.ijbssnet.com/journals/Vol.\\_2\\_No.\\_14%3B\\_July\\_2011/25.pdf](https://www.ijbssnet.com/journals/Vol._2_No._14%3B_July_2011/25.pdf) (accessed on 1 April 2021).
8. Hogben, G., (2021). *Security Issues and Recommendations for Online Social Networks* (3<sup>rd</sup> edn.). [eBook] Available at: <https://ifap.ru/library/book227.pdf> (accessed on 1 April 2021).
9. Robert A. Hanneman, Introduction to Social Network Methods. (2019). [eBook] Available at: <http://www.analytictech.com/networks>.

- pdf (accessed on 1 April 2021).
10. Kumar, A., Kumar, G. S., Kumar, R. A., & Sinha, S., (2013). *Social Networking Sites and Their Security Issues* (3<sup>rd</sup> edn., p. 5). [eBook] Available at: <http://www.ijsrp.org/research-paper-0413/ijsrp-p1666.pdf> (accessed on 1 April 2021).
  11. Nations, D., (2021). *What is Social Networking?* [Online] Lifewire. Available at: <https://www.lifewire.com/what-is-social-networking-3486513> (accessed on 1 April 2021).
  12. Obiniy, A., Oyelade, O., & Obiniyi, P., (2018). *Social Network and Security Issues: Mitigating Threat Through Reliable Security Model*. [eBook] Available at: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.800.510&rep=rep1&type=pdf> (accessed on 1 April 2021).
  13. Senthil Kumar N., Saravanakumar K., Deepa K., On Privacy and Security in Social Media: A Comprehensive Study. (2015). [eBook] Available at: <https://core.ac.uk/download/pdf/82396532.pdf> (accessed on 1 April 2021).
  14. Rathore, S., Sharma, P., Loia, V., Jeong, Y., & Park, J., (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, [Online] 421, 43–69. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0020025517309106> (accessed on 1 April 2021).
  15. Regina, R. S., & Ramesh, K. S., (2014). *Security and Privacy Issues in Social Network Services: An Overview* (2<sup>nd</sup> edn.) [eBook] Available at: [https://ijireeice.com/wp-content/uploads/2013/03/IJIREEICE4J\\_a\\_raji\\_security.pdf](https://ijireeice.com/wp-content/uploads/2013/03/IJIREEICE4J_a_raji_security.pdf) (accessed on 1 April 2021).
  16. Sadiku, M. N. O., Omotoso, A. A., & Musa, S. M., (2019). (PDF) *Social Networking*. [Online] ResearchGate. Available at: [https://www.researchgate.net/publication/333695257\\_Social\\_Networking](https://www.researchgate.net/publication/333695257_Social_Networking) (accessed on 1 April 2021).
  17. UKEssays.com. (2019). *The Security Issues with Social Networks Media Essay*. [Online] Available at: <https://www.ukessays.com/essays/media/the-security-issues-with-social-networks-media-essay.php> (accessed on 1 April 2021).

## CHAPTER 8

# Cyberspace Security in Digital Age

## CONTENTS

8.1. The Start of Cybersecurity .....	206
8.2. Importance of Cyber Security in the Digital World? .....	208
8.3. Why Cyber Security is Critical for Companies? .....	208
8.4. The Importance of Cybersecurity In Digital Transformation .....	209
8.5. Why is Cybersecurity Lagging In Digital Transformation? .....	211
8.6. How Can Cybersecurity Ensure Successful Digital Transformation?.....	214
8.7. Overcoming Paralysis by Analysis When it Comes to Cyber Risk and Cyber Security .....	216
8.8. Embedding Cybersecurity Into Digital Transformation .....	217
8.9. Security in the Digital Age .....	218
8.10. Cybersecurity Best Practices .....	220
8.11. Cybersecurity's Dual Mission During the Coronavirus Crisis .....	222
8.12. Vulnerability Discovery Models (VDMS) .....	229
8.13. Conclusion .....	233
References .....	235

Currently, cybersecurity is one of the major concerns since most of the business organizations have shifted their work online. All the data related to their customers and their business functionality stored in cloud storage. Also, cloud computing services are used by individual users as well, and they store their personal data over the cloud space. Apart from that its users also have their respective accounts on social media platforms and the IoT technology getting more and more advanced is being provided to the general public more and more. All these are getting affected due to a less secure online environment. In this chapter, cybersecurity concerns have been discussed, topics such as the importance of cybersecurity in digital transformation have been elaborated so that proper understanding of cybersecurity in the digital world can be provided.

## 8.1. THE START OF CYBERSECURITY

During the early 70s, Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts, realized that a computer program can effectively move across a network and leave a small trail wherever it went. Then, he created the first computer “worm,” named as *creeper*. It could replicate itself over multiple computer systems.

Ray Tomlinson, the inventor of e-mail also worked for BBN Technologies. In turn, he developed the first antivirus named *Reaper*, a program that could replicate itself while moving across computer networks and, thus it found copies of *creeper*. The *Reaper* solution would simply log *creeper* out of the system.

After the development of Creeper and Reaper, cybercrime in various forms became more extensive as computer software and hardware continued to evolve. As the development of software and protection methods progress, hackers endure to find vulnerabilities and thus, cybercrime has evolved in parallel.

### 8.1.1. Cybersecurity Today

At present, technology is not just limited to software and hardware. Many modern organizations are making effective use of IoT, blockchain, data analytics, and mobile computing. All these provide a more seamless and easier way to conduct business on a regular basis.

As technology sustains to improve workflow as well as business processes, cybercriminals are also getting more advanced in their attacks

or threats, and businesses have proven to be the key priority. As per the McAfee's 2017 State of Cloud Adoption and Security report, a total of 93% of the organizations make effective use of cloud services in some form. Out of these, 74% agreed that they store some or all of their sensitive data in public clouds.

Nevertheless, the report also shows that 52% of the security experts felt that there is always a chance of getting a malware infection from a cloud app. Also, 49% of the survey respondents said they slowed down the adoption of cloud usage because of the lack of cybersecurity skills.

All around the globe, the amount of data going across various networks endures to increase, and if not safeguarded, this could cause organizations tens of thousands to millions of dollars. During the initial days of the cybersecurity industry, the inherent vulnerabilities in such networks were not exploited easily, but with time, hacking skills and the consequent damage has rapidly increased (Figure 8.1).



**Figure 8.1.** *Cybersecurity alert.*

Source: Image by Pixabay.

## 8.2. IMPORTANCE OF CYBER SECURITY IN THE DIGITAL WORLD?

Digital world is complex and with unlimited offerings. This, unfortunately, also applies security breaches. Security attacks are not limited to stealing or compromising personal, financial, and complex business data; they can cause a threat to national security. As the digital platforms are developing at a rapid scale, so are the methods of protecting the information security.

Below given are multiple factors that are associated with cybersecurity:

1. **Data Security:** It is put in place in order to avert unauthorized access to the database of different organizations. In addition, data security is also considered as an aspect of IT security.
2. **Mobile Security:** It is also called wireless security, which functions to secure smartphones, laptops, and all other types of portable computing devices from threat.
3. **Network Security:** It is considered as a broader process where software as well as hardware technologies are utilized in order to protect or secure the computer networks.
4. **Application Security:** The security features are put inside of the application so as to make sure that they are safe from any kind of cyber-attack.
5. **Endpoint Security:** The connectivity of wireless devices like phones and laptops too possess risk, and these are secured by endpoint security.
6. **Identity Management:** Accessibility to networks, systems, and applications is checked by using a detailed and established procedure.
7. **Disaster Recovery:** In order to keep unplanned events in check, a security plan is laid out by the companies well in advance.

## 8.3. WHY CYBER SECURITY IS CRITICAL FOR COMPANIES?

Not only nations and governments need to be on the lookout for cyber-attacks these days, the corporate sector is also a major risk and thus, needs to ensure that it is not at risk to any kind of cyber threats. This is the key reason why organizations are taking enough as well as apt steps to put a good security check-in place.

In addition to that, it is not only the big corporations but business of all sizes is putting up strong security in the face of cyber threats. As the future is not predictable, it is always better to have a good plan of action that can protect or secure the sensitive data or information that is vital for the company before any major damage happens.

## 8.4. THE IMPORTANCE OF CYBERSECURITY IN DIGITAL TRANSFORMATION

### 8.4.1. What Is Digital Transformation?

Digital transformation occurs when digital technology is integrated into processes, products, and different assets of a business for the aim of optimizing the overall operational efficiency, improving customer experience, growing or expanding into new markets, and last but not the least, managing risk.

For some of the organizations, digital transformation can be tough. Although, the gradual increase in the use and application of digital technologies like IoT, cloud, big data, AI, and mobile in almost every area of business and society have proven that digitalization is the one and only way to move further if companies or organizations want to grow and have competitive advantage.

However, digital transformation is mainly discussed in context to businesses, so all kinds of organizations are required to evolve so that they can adapt to the changing landscape of businesses.

### 8.4.2. What Are the Benefits of Digital Transformation?

- **Operations have Become More Customer-Centric:** The key issue related with digital transformation is having the ability to make effective use of technology to improve customer experience. Digital transformation aids the organization to pay more attention to the needs or desires of customers since service becomes consistently improved across all channels.
- **Operations are More Consolidated:** Novel technologies aid to streamline the workflows of businesses and overhead that are mainly linked with the outdated solutions are eliminated.
- **Customer Strategy is Improved:** With the aid of new technologies, organizations become capable of acquiring, retaining, and assisting their customers.



- **Digital Transformation Provides Universal Customer Experience:** When enterprise-wide systems and technologies are linked together, the customer experience becomes simplified and universal irrespective of when, where, and how customers prefer to interact with a specific brand.
- **Digital Transformation Drives Data-based Insights:** Digitalization makes companies enable to combine all of the data from all customer interactions, allowing them to enhance their processes and strategies to aid them attain better results.
- **Costs are Ultimately Reduced and Sales Increase:** Organizations are required to spend more on new technologies at the initial phase of digital transformation. Nevertheless, operations have become focused on customers and tasks become more effective. Consequently, the workforce is much more productive. When the customers are satisfied, they do more business with the brand, and there are high chances that they will refer the company to others.

These benefits clearly show that digital transformation is important for organizations, and for this reason, the senior management in different organizations in various industries has put this a priority. Though, management must also realize that there are effective benefits to digital transformation, as well as a number of risks are also involved.

Technology enhances the operations of a company, and this eventually results in improved customer experience. At the same time, this may also leave organizations open to cyberattack.

According to a report by Cybint, 230,000 new malware samples are being launched on a regular basis. Additionally, there happens a hacker attack in every 39 seconds, and this affects one in three individuals in the U.S. alone.

Since the year 2013, there have been 3,809,448 records stolen from data breaches that occurred on a regular basis. That means, 158,727 records per hour, 2,645 per minute and 44 every second of every day. Also, the report states that approximately \$1 trillion is expected to be spent all around the world on cybersecurity from 2017 to 2021.

As per, “The State of Cybersecurity: 2016” study conducted by ISACA (formerly known as the Information Systems Audit and Control Association), about 82% of organizations feel that their board of directors is concerned about cybersecurity. Though, as the aforementioned statistics show, there



appears to be gaps between what many organizations want related to cybersecurity to what they actually do about it.

## **8.5. WHY IS CYBERSECURITY LAGGING IN DIGITAL TRANSFORMATION?**

All organizations know better that cybersecurity is important, however few people like to be challenged with this requirement:

- With the advent of technology, user experience, agility, and performance are important. Of course, security is also very critical. Nevertheless, to several users, having to go through other methods to make sure that network systems are protected, make them uncomfortable. Consequently, security has become built-in everywhere.

There has to be a change in outlook. The aim of digital transformation in most of the organization has been on speed, optimization, automation, innovation, and some other transitional goals. In addition, digitalization should focus on compliance and cybersecurity. Instead of considering cybersecurity as a cost, companies must consider it as a basic requirement.

- Many seem to believe that cybersecurity slows down digital transformation. Digital transformation mainly comprise change, speed, connectivity, agility, improved service, enhanced customer experience, etc. Though, when cybersecurity is added into the mix, many find it boring due to the rules and regulations, training, and every other thing that is the part of security implementation.

In terms of marketing, a lot is going on within the framework of digital transformation, however cybersecurity is hardly mentioned when a company draws up plans of increasing its sales. Actually, a lot many users do not desire for speed, connectivity, performance, and customer experience to be impacted by the security solutions.

Well, this is not the case with novel technologies anymore. At present days, the security solutions can be done even in the cloud. Inappropriately, a lot many organizations do not involve their security team at the start of the process. Basically, they are called in too late.

- Some organizations do not seem to have a sense of urgency to implement security in new technology. As per the survey conducted by Dell, around 97% of the respondents said they have

been investing largely in digital technologies that will eventually transform their respective businesses, including mobile phones, cloud infrastructures and its applications, and IoT. Nevertheless, only 18% out of total confirmed that security has been involved in all of their initiatives related to digital transformation.

The same survey, surprisingly showed that 85% of the survey respondents admitted that if the security teams are involved from the start of the project, then those initiatives could have been better enabled by the security.

- Cybersecurity is not a simple process. To potential cyberattacks, cybersecurity is not an easy fix or solution. It needs developing a strategy that entails prioritizing the most important processes along with the systems within the organization, and also recognizing and securing potential causes of attacks or vulnerabilities.
- Making a business case for cybersecurity can be difficult. Different from other aspects of the business when it can be projected what it can bring into the business such as increased sales, improved customer experience, etc., it cannot be predicted that how much attack will impact the company or business. Even if one can factor in potential losses if cybersecurity is not implemented in an effective manner, then he or she will only know when an attack has occurred accurately.
- Mobile technology has changed security parameters. Technologies like IoT and mobile has made security parameters even more complex. The perimeter of cybersecurity is practically all over the place. As there are numerous channels by which attacks can occur, firewall, and anti-virus solutions are no longer enough for the mobile user of today's world.
- Data and information are undervalued. Often the organizations do not give much value to data and information. These are the spirit of the businesses these days and a source of revenue as well as new business models. However, this is not much reflected in the cybersecurity initiatives of various organizations.

### **8.5.1. How Can Organizations Address These Issues?**

In total, a change of mindset in context to cybersecurity is highly required. Security must be involved from the very beginning of the digital transformation in an organization. Cybersecurity required to be embedded in to the network of companies.

It needs to be treated as an asset or strength which is really critical for the growth and success of the company instead of considering it as additional cost. In addition, it is also very significant to have the CISO or any other executive in charge of cybersecurity to be a part of the team.

For a successful digital transformation, cybersecurity is vital. In order to ensure that the network of an organization is well secured while going through the transformation process, cyber experts need to be consulted.

Netswitch has been named by the industry analysts such as Gartner as one of the leading managed detection and response (MDR) Services globally. The company delivers progressive threat detection by security analytics, with 24/7 monitoring and alerting, and remote incident investigation and response incorporated in the end-to-end service.

How is technology evolving life, societies, and organizations, and how does it impact digital transformation?

In today's society, the role that technology plays in human life is becoming a progressively urgent topic of discussion. Considering the pace of nature of technological change, and how different it is now versus earlier eras is informative (Figure 8.2).



**Figure 8.2.** *Ransomware attack.*

Source: FileCloud.

Looking back 220 years ago, the Internet, or World Wide Web<sup>1</sup>, was primitive and essentially just for play. Several companies like AOL, a web portal and an online service provider, governed supreme as the one-time mogul of the media, the CD was the king of recorded music, Nokia unveiled the first-ever monochromatic display cell phone of the world and the cloud was the only know as what people saw in the sky.

At present, there are more than 4.1B internet users, more than 1.8B websites and more than 337B GB worth of Internet traffic previous year alone (2020)-of which 52% was generated only through mobile phones. According to Paul Daugherty, Chief Technology and Innovation Officer at Accenture, distributed ledgers, AI, extended reality, and quantum computing are the next big technology catalysts for change that are seeing adoption cases this year.

The advancements in technology are very rapid, which is apparent as more and more data becomes available. As technology continues to adapt and evolve at a rate that appears to outpace culture and institutions, organizations without considerations of cybersecurity in their digital transformation strategies are at a risk, as stagnancy leads to uncertainty and instability.

As the drive towards digital transformation endures to gather momentum ceaselessly, this is an apt time for the organization to pause and reflect on their security strategies, for a moment. For most of the human history, the world didn't change all that much in a single lifetime. In a clear way, that's no longer the case and rapidly advancing technology is the reason why.

*"We discovered in our research that insider threats are not viewed as seriously as external threats, like a cyberattack. But when companies had an insider threat, in general, they were much more costly than external incidents. This was largely because the insider that is smart has the skills to hide the crime, for months, for years, sometimes forever."*—Dr. Larry

**Ponemon**

## 8.6. HOW CAN CYBERSECURITY ENSURE SUCCESSFUL DIGITAL TRANSFORMATION?

The capability of digitally reimagining processes as well as functions is determined mainly by a clear digital strategy which is supported by the

leaders of different organizations who foster a culture to encourage change and reinvent the old.

Even though the transformation insights are consistent with the evolution of prior technologies, now what is different in digital transformation is that taking risks is a kind of cultural norm as the digitally advanced companies target new avenues of competitive benefits.

In the current technological climate, the confidence or assurance gathered from a competitive benefit or advantage can be largely attributed to data stewardship and cybersecurity to make the most out of the digital environment.

In the current time of analytics and intelligence, competing in a data-driven world is quite tough. Today's business environment has become super competitive, and those organizations which are not reinventing their businesses continuously with the data at its core will eventually fall off the tracks, watching from the sidelines while their market is disrupted.

Though, as growing digital natives were made for analytics, legacy companies have to do the hard work of changing or overhauling the existing systems. It is not always simple and easy to redesign to a stage of data-driven decision making, mainly while accounting for the cybersecurity implications.

Some of the companies have heavily invested in technologies but not yet changed their respective organizations to make the most out of those investments. A lot many people are struggling to develop the effective business processes along with organizational muscle to get real value from cybersecurity and analytics. However, this value is not assured.

As technology gets advanced, so does the level of chances of cyber risk that organizations should navigate. According to a report published by Deloitte, analysts estimated that the cyber risk all around the world "could slow the pace of technological innovation by as much as USD \$3 trillion in lost economic value in 2020."

Organizational vulnerability to cyber-attacks can be declined by the development of a strong cybersecurity strategy, which is specific to the company, in order to manage the cyber-attacks or cyber threats with confidence. Good investments in cybersecurity allow different organizations to better understand their level of cyber resilience depending upon the

critical business assets, their threat landscape as well as the maturity of their cyber capabilities.

In addition to that, integrated dashboards permit organizations to check or monitor the level of cyber resilience and can also be customized for an operational, executive, and managerial audience. Operative implementation remedies organizational imbalance and presents a complete picture of the cyber-protected enterprise by addressing security standards, increasing cooperation and information sharing, policies, and practices, and enhancing collaboration between partners.

## **8.7. OVERCOMING PARALYSIS BY ANALYSIS WHEN IT COMES TO CYBER RISK AND CYBER SECURITY**

It is very much evident that the financial costs of a cyber-attack could be huge enough to cause severe changes in small and medium-sized businesses. Along with having negative financial implications, brand equity is equally destroyed when consumers see their privacy as being violated, consumer trust being violated and long-term brand reputation.

The number of data breaches as reported by UK financial services firms to the Financial Conduct Authority (FCA) increased 480% in the year 2018 to 145, up from just 25 in the year 2017. Organizations are struggling hard to keep up with the cybercriminal community.

Digital transformation such as SD-WAN, cloud adaptation, and IoT, along with adaptation of various emerging technologies, is creating as well as expanding new and unexpected means of attack.

According to Forbes, those enterprises who are prioritizing cybersecurity are developing a challenging competitive benefit over their peers, as the typical U.S. based enterprise will lose an average of \$7.91M from a breach, almost double the global average of \$3.68M according to IBM's 2018 Data Breach Study.

Digital natives are rapidly becoming more and more comfortable with the emerging technology, and are giving away personal data more than ever, in spite of growing risks and severe consequences. An Experian study revealed that 70% of consumers all around the world "are willing to share more personal data with the organizations they interact with online, particularly when they see a benefit."

Another survey conducted by the Centre for Data Innovation came to almost similar conclusion, concluding that 58% of consumers are “willing to share their most sensitive personal data” (i.e., biometric, medical, and/or location data) in return for using different apps and services.

Consumers, these days, are putting trust in organizations in order to manage as well as protect their private data. In turn, organizations should become well-equipped with an effective cybersecurity strategy to do so. The predominant challenge and need to overcome as well as prepare for cyber threats are to include security in their core strategic vision.

Another mandatory step is to develop the right and most effective business processes along with building capabilities, including both talent as well as data infrastructure. It is not simply enough to layer potential technology systems on top of the current business operations. All of such aspects of the digital transformation require to come together to realize the complete potential of cybersecurity.

## **8.8. EMBEDDING CYBERSECURITY INTO DIGITAL TRANSFORMATION**

It is really crucial for organizations to make security the beginning point, and not a kind of afterthought. In spite of the abundance of the data breaches all around the world, security remains an afterthought for a great majority of digital transformation activities endured by current businesses like mobility, cloud services, and customer experience programs.

Unfortunately, security is considered as slowing down a project instead of something that enables success. However, it is understood that along with time pressure to get a project running efficiently, the lack of sensible security considerations is a key issue for several organizations striving for cyber resilience and vigilance.

It is evident across today’s digitized climate that with a gradual increase in frequency as well as publicity of cyberattacks getting much more complex, businesses should realize that their customers are aware of certain cyber issues than ever before. At this point of time, embedding a cybersecurity strategy is an important competitive benefit.



According to a survey done by IT and security professionals, just 18% of the organizations agreed that their security team had been effectively involved in all of their digital transformation-related projects, and other 76% agreed that security considerations were added very late in the project, at last resulting in projects being delayed because of being retrofitted after major decisions had been made. In the same survey, 85% of respondents agreed that the security team could have done a much better job if they had been included much earlier in the project.

The main challenge or issue and overall aim for the security team is to reinsure the organization that their IT infrastructure is resilient and secure. Nevertheless, at current times, it is vital for organizations to understand that no digital transformation project should always begin without understanding its security implications.

Organizations which can harness such capabilities in an effective manner will eventually be able to create important values and differentiate themselves, while others will find themselves mainly at a disadvantage. More than ever, people are now relying largely on the emerging digital economy.

As different organizations, government agencies, and critical infrastructures move to such an ever-evolving digital model, a key security event could have catastrophic results for everyone. Also, it is important to remember that cybersecurity events do not care about social, economic, and political borders. When an infrastructure or economic system is brought down and compromised, everyone suffers.

## **8.9. SECURITY IN THE DIGITAL AGE**

Every day, much more than 2.5 quintillion bytes of data is created or developed, which is highly enough to fill up 10 million Blu-ray disks on a regular basis. With the digitization of such a huge information database, the security needs or requirements of different companies or organizations are changing rapidly. While the requirement for physical security has not reduced, the demands for keeping all of such data secure or protected is of high importance.

The increasing number of data breaches are a perfect indication that companies are highly susceptible to exposure of their private data, in spite of all of the efforts they make to keep their information safe and secure. Though no one may ever see data breaches getting disappear completely, there are certain practices that can be utilized in order to improve data security as well as keep private data as it is intended to be private.



According to Bruce Schneier, a security expert “encryption is the most important privacy-preserving technology we have.” The process of keeping data safe and protected begins with the use of encryption across an organization.

It is considered to be most effective when it is pervasive at a company, which means documents, e-mails, and other data is all encrypted. Data encryption is regarded as the first step in guaranteeing that data, even if interpreted or stolen-is more difficult for those having bad intentions to use.

Data stored in the cloud can always be accessed by the remote users logging on to extract or upload information. In such environment, it is really significant that individuals as well as companies use secure passwords. Hackers, these days are much capable of using brute force tools to guess at passwords, and users having common passwords are the most vulnerable to experience cyber threats.

A strong password is considered to be a front-line defense which aids in ensuring the security of data. Krebs on Security, an authoritative source for information on data security, has gathered some best practices for passwords that users can utilize to keep their digital information secure.

Another best practice that organizations can make use of is ensuring that all of their software are updated. At times, digital criminals look for exploits in software in order to access the private data. Once such vulnerabilities are discovered, the level of threat rapidly increases.

In general, the software providers react instantly by providing software patches. The end users must execute these fixes as early as they become available to prevent hackers from taking effective benefits of the exploits.

When looking at a cloud service provider, certain security measures that the provider provides must be considered. In addition, physical security plays a vital role in keeping data safe and secure. These days, organizations employ various physical security measures in order to ensure that data stored is only accessible to authorized personnel.

This basically includes the use of multi-factor authentication as well as biometrics for access control, alarms, video surveillance throughout the facility, along with several other physical measures that eventually help in ensuring that data cannot be accessible by unknown personnel.

Making sure that information stays safe and secure appears like common sense, but there are cases of breaches every day. Passwords and encryption

are not necessarily new concepts, though employing best practices will aid in ensuring data safety.

### **8.9.1. Security as the Enemy of Digital Transformation**

Digital transformation is all about agility, change, connectivity, speed, customer expectations, real-time economy, disruption, etc. It is about rules, regulations, defense protection, awareness, training, and a layer that some believe slows down the initiatives related to digital transformation.

The security experts know this quite well that the users do not look for experiences affected by the security solutions. In digital transformation projects, security tends to get called a bit late. Reasons being executives are scared that their digital transformation efforts could be blocked by the intervention of security. Well, this is not like a valid excuse, at least not with today's security solutions and certainly not by pretending security isn't that important.

### **8.9.2. Security and the Technologies of the Digital Transformation Economy**

There is a great correlation between emerging technologies and security. Initiatives in the space of IoT are usually amongst the most obvious one. At present, people are largely investing in digital technologies like mobile, cloud application, IoT, and infrastructures, and security has been involved in all mobile, IoT, cloud, and self-service initiatives.

## **8.10. CYBERSECURITY BEST PRACTICES**

- All data in transit and at rest should be encrypted. As cybercriminals continue to develop different ways to steal data in small and large businesses, it is now become mandatory to both the data in transit and data at rest to be protected. As a result, using proactive measures like identifying data at-risk and executing effective data protection for both data at rest and in transit is needed.
- Always use two-factor authentication (2FA). Earlier, logging on to online accounts just by using a password used to be an effective security measure. But now, a password has been proven to be the weakest form of security. On a regular basis, there is a news related to passwords being stolen through social engineering or using

some electronic ways. Hackers can easily guess the passwords and also, they can capture it by software keyloggers (Figure 8.3).



**Figure 8.3.** *Encryption process.*

Source: Image by PixaBay.

- Applications should have embedded security controls by default. In spite of asking the users or customers to choose security set-ups, the security features must be built into the apps in advance in order to provide the highest level of security and protection.
- Perform routine system back-ups.
- Immediate upgradation of company systems with any new developer patches along with software updates.
- Research and consider proactive security management systems by making use of advanced technologies such as:
  - Behavioral analytics;
  - Continuous reporting of risk assessment;
  - Automated IP blocking based on real-time threat data;
  - Incident response and remediation service contracts.
- Consider looking for a professional asset and risk assessment, including a penetration test, performed by a respected cybersecurity company.

At present, an IT team is mainly responsible for the cybersecurity of organizations. This IT team or cybersecurity team can be in-house or third party. However, their scope in protecting the networks of the company requires to be more proactive as the traditional network-perimeter security becomes more vulnerable to attacks of threats. Netswitch provides modern cybersecurity solutions to various kinds of organizations to keep the data of company safe and secure from cyberattacks.

## **8.11. CYBERSECURITY'S DUAL MISSION DURING THE CORONAVIRUS CRISIS**

The efforts of various companies and organizations in order to protect or secure the workers as well as serve the customers during the time of the COVID-19 pandemic have unluckily increased their exposure to cyberattacks. Adoption of work from home technologies on a large scale, greater utilization of online services, and heightened activity on customer-facing networks all present fresh openings, that cyber attackers have been very fast to exploit.

The predominant issue for the cybersecurity teams will be protecting their organizations while aiding operations to go on without interruption. For instance, cybersecurity teams at organizations that provide web-based services to consumers should adjust their security programs to match scaled-up operations while protecting a huge shift to work-from-home tools.

Addressing such diverse as well as competing requirements at once won't be easy. However, certain governing principles are aiding the organizations to deal effectively with such conditions. Some of those principles are focusing on critical needs of operation, testing plans for managing security as well as technology risks, balancing protection with business continuity and monitoring for new cyberthreats.

### ***How the response to COVID-19 has increased cyber risk?***

As people and organizations have cut down travel and gatherings, they have shifted activities into the digital realm. These days, workers and students are staying home, mainly using video conferencing, collaboration platforms, and various other tools in order to complete their businesses and schoolwork.

During free time, people go online to shop, chat, read, stream, and play. All such tasks eventually put a huge stress on the control and operations of cybersecurity, and as a result, key vulnerabilities stand out such as:

- Working from home has opened multiple vectors for cyberattacks. A major shift towards work-from-home arrangements has increased the long-lasting cybersecurity issues, today. Such issues can be unprotected data transmissions by people who are not using VPN software, a very weak implementation of risk-mitigating behavior, and both physical as well as psychological stressors that require clients to bypass the controls for getting things done properly.

The more that people working from home struggle to access data and systems in an easy way, the more they will try and use risky workarounds. The teams of cybersecurity will require to protect the systems of those employees who are working from home, test, and scale VPNs along with incident response tools. Also, they may try to revisit access-management policies so that the employees can easily connect to the infrastructure through personal devices or some other open, internet-facing channels.

- Social-engineering ploys are on the rise. In the case of social engineering strategies, attackers try to acquire valuable details or information, money, or access to secured systems just by tricking the users. Many companies have observed malware-laced email-phishing campaigns that steal the identities of health, aid, and some other benevolent organizations.

Scammers behaving as the part of corporate help-desk teams ask employees or workers for their security credentials by using text phishing and voice phishing. Email fraudsters try to get executives to move money in order to fund vendors, operations, and virus-related response activities.

- Cyber attackers are using websites with weak security to deliver malware. With the creation and development of new domains and websites to effectively spread the information, and the resources to deal with coronavirus, attackers are mainly taking advantage of weak security controls on various sites so as to spread malware through drive-by downloads. In one case, an attacker targeted a public-sector entity just by incorporating malware in a pandemic-related document and concealing it as an official communiqué from another part of the government.

After it gets installed, such a nasty application steals the confidential data of the user, like personal information, bitcoin wallet keys and credit

card information. Some of the malware applications launch ransomware attacks that lock the system of the user until he or she pay a definite amount of money to the attacker.

- Public-sector organizations are experiencing acute pressure. In North America, a large government organization suffered from a distributed denial of service (DoS) attack that was targeted at disrupting the services and spreading misinformation to the public.

In Europe, a major hospital was hit by a cyber-attack that consequently forced it to suspend all of its scheduled operations, shutting down IT network and moving acute-care patients to another facility. A department of local government also had its website encrypted by some ransomware which eventually prevented officials from posting necessary information for the public and employees from accessing some of the critical files.

As the COVID-19 pandemic progressed, it somehow changed the functioning of socioeconomic systems. So, in order to remain effective and vigilant, cybersecurity teams require all new approaches to deal with hackers or attackers.

### 8.11.1. Cybersecurity Tactics for the Coronavirus Pandemic

The COVID-19 pandemic has made it a bit harder for several companies to effectively maintain their security practices and continuity of their businesses. However, the new tactics can positively aid cybersecurity leaders to protect their organizations:

1. **Securing Work-from-Home Arrangements at Scale:** The widespread adoption of work from home tools has largely put considerable strain on the cybersecurity teams to protect and secure those tools without making it hard or impossible for employees to work. In Asia, Europe, and North America, the cybersecurity teams are safeguarding new work from home arrangements by implementing some critical changes in some areas-technology, people, and processes.
2. **Technology: Make Sure Required Controls are in Place:** As companies roll out new technologies that make employees able to work from home to maintain business continuity, the team of cybersecurity experts are taking actions mentioned below mainly to mitigate the cybersecurity risks:

- **Accelerate Patching for Critical Systems:** Shortening patch cycles for VPNs (virtual private networks), cloud interfaces and end-point protection systems. These systems are important for remote working and will benefit the companies in eliminating the vulnerabilities just after their discovery. Patches that can secure the remote infrastructure deserve special attention.
- **Scale-Up Multifactor Authentication (MFA):** Employees who are working remotely from home must be required to make use of multifactor authentication (MFA) to access critical applications and networks easily. However, scaling up MFA can be somewhat challenging-the protection it will add actually calls for a flow in short-term capacity.

Various practices make the MFA rollout much manageable. One is to arrange users who have raised privileges like domain and sysadmins, and application developers, and work with critical systems, for instance, money transfers.

Targeting users in pilot rollouts of modest scale will consequently allow the team to learn from the experience and make efficient use of that knowledge to shape extensive implementation plans. Cybersecurity teams can benefit from using MFA technologies like the application gateways provided by different cloud providers that are combined with the current processes.

- **Install Compensating Controls for Facility-based Applications Migrated to Remote Access:** Certain applications like cell-center wikis and bank-teller interfaces are only available to users working onsite at their organizations' facilities.

To make sure such kind of facility-based applications are available to remote workers, organizations are required to protect those apps through special controls. For instance, the companies might need their employees to activate VPNs and then use MFA to reach facility-based assets while allowing them to use MFA alone when accessing other parts of the corporate environment.

- **Account for Shadow IT:** At various companies, employees use so-called shadow IT systems. Employees set up these shadow IT systems and administer without formal approval or support from the IT department. Extended work from home operations will eventually expose those systems because the business processes



that depend on the shadow IT in the company will break down once the employee find self-unable to access the resources.

IT teams along with security teams must be prepared to support, transition, and secure the business-critical shadow assets. They should always keep an eye out for new shadow-IT systems that can be used by employees or can be created to make work from home easy, or to compensate for in-office capabilities which the employees can't access, or to get around obstacles.

- **Quicken Device Virtualization:** Cloud-based virtualized desktop solutions can make it easier for the employees to work from home. Reason being-many of them can be implemented more rapidly than on-premises solutions. Though, new solutions will require strong authentication protocols such as a complex password, along with a second authentication factor.
- **People: Help Employees Understand the Risks:** Employees working from home should exercise good judgment in order to maintain information security, even with stronger technology controls. People feel added stress, and this can make them much prone to social engineering threats.

Employees working from home, at times, get engage in certain practices that consequently opens them to other threats or attacks, like visiting malicious websites that office networks do not give access to employees. Building a “human firewall” will help to ensure that employees who work from home do their part to keep the enterprise secure and protected.

- **Communicate Creatively:** A very high volume of crisis-related communications can drown out the warnings of cybersecurity risks. Security teams will require to utilize a mix of approaches to get their messages across.

These might consist of setting up two-way communication channels that let users post as well as review questions, report, and share best practices; posting announcements to pop-up or universal-lock screens; and inspiring the innovative utilization of the existing communication tools that compensate for the loss of informal interactions in hallways, break rooms, and other office settings.

- **Focus on What to do Rather Than What Not to do:** Security teams should explain the benefits, for example, security and productivity, of using approved messaging, file-transfer, and



document-management tools to do their jobs. Further, to encourage safe behavior, the cybersecurity team can promote the utilization of approved devices like-by providing stipends to purchase approved software and hardware.

- **Increase Awareness of Social Engineering:** COVID-19-themed phishing, campaigns have surged. Cybersecurity security teams must prepare the employees of the organization to avoid being tricked. These teams should not just alert users that attackers will exploit their fear, stress, and uncertainty but correspondingly consider shifting to crisis-specific testing themes for phishing campaigns.
- **Identify and Monitor High-Risk User Groups:** Some of the users, for example, those who are working with personally recognizable information or some other confidential data, stance more risk than others. High-risk users must be identified and then monitored for their behavior, that can specify the security breaches.
- **Processes: Promote Resilience:** Some of the business processes are designed in such a way to support work from home extensively, and thus most of them lack the right embedded controls. For instance, an employee who has never done high-risk remote work and has not set up a VPN might not find it possible to do so due to in-person VPN-initiation requirements. In such kind of cases, complementary security-control processes can alleviate risks. Such processes of security include these:
- **Supporting Secure Remote-Working Tools:** Security and IT help desks must add capacity while a large number of employees are setting up and installing basic security tools like VPNs and MFA. It might be practical to organize security-team members at all of the centers in order to provide added frontline support.
- **Testing and Adjusting IR and BC/DR Capabilities:** Validating remote communications and collaboration tools, even with increased traffic allows companies or organizations to support incident-response (IR) and business continuity (BC) or disaster recovery (DR) plans. However, the companies might have to regulate their plans to cover conditions related to the current crisis. To find weak points in plans, it is recommended to conduct a short IR or BC/DR tabletop exercise with no one in the office.

- **Securing Physical Documents:** In the office, employees usually have ready access to digital document-sharing mechanisms, as well as shredders and secure disposal bins for printed materials. In work from home conditions, where employees might lack the resources, subtle information can end up in the trash. Setting norms for the retention as well as destruction of physical copies, even if that means waiting until the organization resumes business as usual.
- **Expand Monitoring:** Increasing the scope of organization-wide monitoring activities, especially for data and endpoints is critical for two reasons. First is, cyberattacks have increased. Second is, basic boundary-protection mechanisms, like web gateways, proxies, or network intrusion-detection systems (IDS) or intrusion-prevention systems (IPS), won't protect users working from home, off the enterprise network, and not connected to a VPN.

Based on the security stack, organizations that do not need the use of a VPN or need it only for accessing a limited set of the resources might go highly unprotected. To increase monitoring, security teams must update security-information-and-event-management (SIEM) systems with new rule sets and discovered confusions for new malware.

In addition, they should also increase the staffing in the Security Operations Center (SOC) in order to aid compensate for the loss of network-based security capabilities, like end-point protections of the non-company assets. If in case, network-based security capabilities are found to be disrupted, teams should always expand their IR and BC/DR plans.

- **Clarify Incident-Response (IR) Protocols:** When cybersecurity threats or attacks happen, SOC teams should always know how to report them accurately. The leaders of cybersecurity teams should build options of redundancy into response protocols so that the responses do not stall, if in case decision-makers can't be reached or if the normal escalation pathways are somehow interrupted due to people working from home.
- **Confirm the Security of Third Parties:** Almost all of the organizations make effective use of contractors as well as off-site vendors. Also, most of them integrate IT systems and share the data with contract as well as non-contract third parties, for example, tax or law enforcement authorities.

When different organizations assess which kind of controls should be extended to the employees in order to protect or safeguard new protocols of working from home, they must do the same for third-party users and connections, who are expected to be managing similar kind of shifts in their operations as well as security protocols.

- **Sustain Good Procurement Practices:** Fast-track procurement proposed to close the major security gaps related to arrangements of work from home must always follow standard due-diligence processes. The main need for specific security and IT tools may appear urgent, however, the poor vendor selection could do more harm as compared to good.

## 8.12. VULNERABILITY DISCOVERY MODELS (VDMS)

Most of the research in the field of cybersecurity considers software vulnerabilities as a random variable and thus performs fitting as well as estimation exercises with the help of distributions. Consequently, there is a clear lack of understanding regarding specific vulnerability discovery process and it has eventually led to particular forms of stochastic models which can explain the software vulnerability discovery (Amin et al., 2013).

Vulnerability discovery models (VDMs), in a way, are used to estimate as well as predict the count of future vulnerabilities that have been affecting a software application, in history. Alhazmi and associates (Alhazmi and Malaiya, 2005, 2008; Alhazmi et al., 2007) present several studies on VDMs. Alhazmi and Malaiya (2008) proposed VDMs for Microsoft and Red Hat Linux OS, Woo et al. (2006) analyze VDMs for Apache and IIS Web Servers.

Models with time-dependent functionality with linear as well as non-linear behavior are thermodynamic (Anderson, 2002), logistic (Alhazmi et al., 2007), quadratic (Rescorla, 2005), Weibull (Joh et al., 2008) and sigmoidal (Ruohonen et al., 2015).

Another contemporary study in the field of cybersecurity tries to analyze the growth of data breach as well as attacks via statistical distributions- Negative Binomial (Sen and Borle, 2015), Gamma (Johnson et al., 2016), logistic (Guo et al., 2016; Mitra and Ransbotham, 2015).

However, a well-known software product or platform is much more appealing to the attackers as compared to other contemporary products available in the market.

Often, a popular software product or platform is more alluring to attackers than other contemporary products in the market. Ruohonen et al. (2015) show the presence of distinct lifecycle phases of a software product deriving from the product lifecycle theory proposed by Bass (1969).

### 8.12.1. Types of Attacks in the Application Layer

Most of the programs make use of the application layer for the purpose of network communication. For communication purposes, the data is condensed in the application layer and then passed on to the transport layer. Some of the very common attacks in security application layer are trojan horses, DNS cache poisoning, and DoS attack.

- **Trojan horses:** A trojan horse is a malevolent computer program which can hide its extension and then seem as a regular file. After that, it is used to access the target computer illicitly. Unlike viruses and worms, it cannot spread itself.
- **DNS cache poisoning:** A domain name system (DNS) server converts the given URL address to the corresponding IP address when browsing the Internet. In DNS Cache Poisoning or Spoofing, the cache information on the DNS server is conceded. It degrades the data of the cache, and consequently, the DNS server returns incorrect IP addresses. In this way, an attacker can divert authentic traffic to its computer and attain sensitive information.
- **DoS attack:** The application layer is compromised, in DoS attack. It is basically attained by flooding the targeted resource or machine with some kind of unnecessary traffic which ultimately makes it impossible for the resource or computer to serve legitimate or authentic requests and thus affects the availability metric of the server.

While, distributed DoS (DDoS) attack is a category of DoS outbreak where the malevolent agent typically sends requests from various IP addresses and thus, making it impossible to stop such kind of attacks (Badve et al., 2016). According to Ginovsky (2014), DDoS attacks on application layer constitutes around 20% of total DDoS attacks.

### 8.12.2. Types of Attacks in the Transport Layer

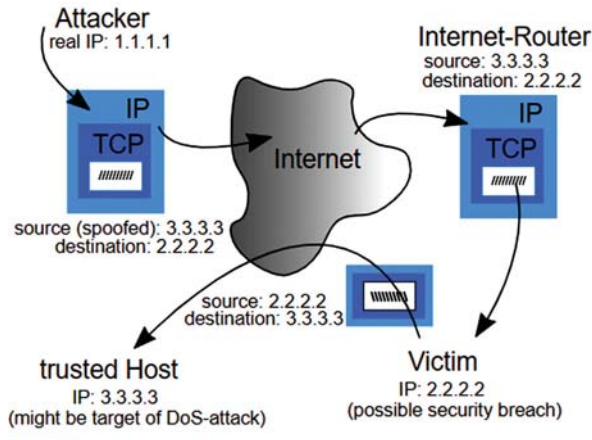
The transport layer executes end-to-end data transmission together with error control, fragmentation, and flow control. Some of the alarming attacks on transport layer are session hijacking and port scanning:

- **Session hijacking:** This is also known as cookie hijacking. It occurs during an established session in order to access the information or services of a computer in an illegal way. Source-routed IP packets are mostly used for session hijacking. The attacker interrupts the conversation between the client and server by influencing them to send the pertinent IP packets through the attacker's machine.
- **Port scanning:** The attacker transmits the access requests to a specific series of IP addresses on the target machine so as to find active ports depending on which the attacker can get an idea of what services are running and also about the operating system installed on the device.

### 8.12.3. Types of Attacks in the Internet Layer

The Internet layer basically regulates the best path via the network. The most common attacks on the Internet layer are packet sniffing, SYN flooding and IP spoofing.

- **Packet sniffing:** It is a process of seizing packets which flow through the network. Then the attacker analyzes the packets in order to acquire sensitive information. In general, it is an attack on the confidentiality service.
- **IP spoofing:** The attacker in this attack creates IP data packets that are marked with spurious origin IP addresses so as to hide his own identity. At times, the intruder can also make use of an authorized IP addresses in order to break the IP address-based authentication and access information. It is generally used in executing DoS attacks (Figure 8.4).



**Figure 8.4.** *IP spoofing.*

Source: Image by Wikimedia Commons.

- **SYN flooding:** a SYN flood is a DoS attack, which aims to make a server unavailable to legitimate traffic by consuming all available server resources.

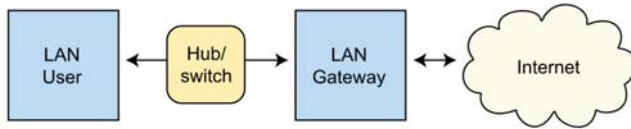
#### 8.12.4. Types of Attacks in the Host-to-Network Layer

The Host-to-Network layer is largely responsible for the transfer of data between different network entities. Common security attacks on this layer are MAC address spoofing and Address Resolution Protocol (ARP) cache poisoning.

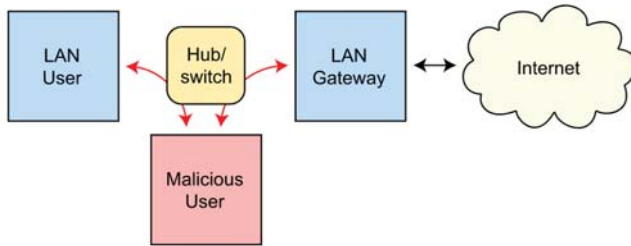
- **MAC Address Spoofing:** MAC address is seared on every network interface card (NIC) in order to recognize them in a network, exclusively. The attacker in this attack masks the MAC address of a NIC to change its identity. In this manner, one machine can get the data of another computer in a LAN.
- **ARP cache poisoning:** This is also known as ARP spoofing and represents a Man-in-the-Middle attack that allows attackers to intercept communication between network devices. The attack works as follows: The attacker in this attack sends the ARP messages to the LAN to link its MAC address with the IP address

of a legitimate user. ARP is usually used to find the media access-control address equivalent to an IP. Through this attack, the attacker can seize the data, amend data or avert regular data flow on the network (Figure 8.5).

Routing under normal operation



Routing subject to ARP cache poisoning



**Figure 8.5.** *ARP cache poisoning.*

Source: Image by Wikimedia Commons.

### 8.13. CONCLUSION

Cybersecurity has become a major research area due to the security concerns on the internet. Various business organizations, whether small-scale or large-scale businesses, and individual users are using online services on a day-to-day basis.

The data stored or transferred over the internet every day is related to user's personal information or transactional data both if reach wrong hands can cause trouble to the users and organizations as well. As it becomes very essential that online service providers such as social media platforms and the cloud computing service providers need to have better security measures taken to ensure the security of the data of its users.

In this chapter, various major concerns related to cybersecurity have been discussed, and what security measures that need to be taken have also been elaborated. The conclusion that can be made from this chapter is that

not only the services need to be developed for its users, but the security measures need to be improved as well. As the technology is improving every day, so are the ways to exploit it. Thus, for this manner cybersecurity becomes a very essential factor to provide data security over the internet.



## REFERENCES

1. Agrawal, D., Wang, H. and Gupta, B., 2018. Computer and Cyber Security. [online] Available at: <[https://www.researchgate.net/publication/329921021\\_Computer\\_and\\_Cyber\\_Security\\_Principles\\_Algorithm\\_Applications\\_and\\_Perspectives](https://www.researchgate.net/publication/329921021_Computer_and_Cyber_Security_Principles_Algorithm_Applications_and_Perspectives)> [Accessed 11 May 2021].
2. Boehm, J., Kaplan, J., & Steen, T., (2020). *Cybersecurity Tactics for the Coronavirus Pandemic*. [Online] McKinsey & Company. Available at: <https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-tactics-for-the-coronavirus-pandemic> (accessed on 1 April 2021).
3. Cybersecurity in a Digital Era. (2021). [eBook] Digital McKinsey and Global Risk Practice. Available at: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf> (accessed on 1 April 2021).
4. Hgsdigital.com. (2021). *Cyber Risk and Security in the Era of Digital Transformation | HGS Digital*. [Online] Available at: <https://www.hgsdigital.com/blogs/cyber-security-in-the-era-of-digital-transformation> (accessed on 1 April 2021).
5. Info.cloudcarib.com. (n.d). *Security in the Digital Age*. [Online] Available at: <https://info.cloudcarib.com/blog/security-in-the-digital-age> (accessed on 1 April 2021).
6. i-SCOOP. (n.d). *Cybersecurity and Cyber Resilience-Security and Cybercrime*. [Online] Available at: <https://www.i-scoop.eu/cyber-security-cyber-risks-dx/> (accessed on 1 April 2021).
7. Kaplan, J., & Boehm, J., (2020). *Cybersecurity's Dual Mission During the Coronavirus Crisis*. [Online] McKinsey & Company. Available at: <https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis> (accessed on 1 April 2021).
8. Kaushal, N., (2019). *Significance of Cybersecurity in the Digital Age*. [Online] Torontosom.ca. Available at: <https://www.torontosom.ca/blog/significance-of-cybersecurity-in-the-digital-age> (accessed on 1 April 2021).

9. Kedrosky, E., (2018). *The Importance of Cybersecurity in Digital Transformation-Security Boulevard*. [Online] Security Boulevard. Available at: <https://securityboulevard.com/2018/05/the-importance-of-cybersecurity-in-digital-transformation/> (accessed on 1 April 2021).

# Index

---

## A

Accountability 27  
advanced encryption standard (AES)  
21, 116  
Airavat 69  
Alibaba 39  
Amazon 32, 39  
Amazon Web Services (AWS) 93  
Anonymization 96  
Application layer 136, 137, 148  
Application programming interfaces  
(APIs) 49  
Application Security 16, 208  
asymmetrical searchable encryption  
(ASE) 68  
audits 11, 27  
Authentication 26  
authenticity checks 114  
Authorization 26  
Autonomic computing 7

## B

backdrop 160  
blockchain 120  
business intelligence (BI) 34

## C

classmates.com 179  
cloud access security broker (CASB)  
76  
Cloud application security 65  
cloud application security platforms  
(CASP) 76  
Cloud Audit Data Federation  
(CADF) 44  
Cloud computing 2, 4, 7, 9  
cloud data management interface  
(CDMI) 45  
cloud security 9, 10, 12, 13, 16, 26  
Cloud Storage Security 16  
communication layer 135  
communications 105, 111  
compound annual growth rate  
(CAGR) 105  
computer emergency response team  
(CERT) 73  
Confidential Data 15  
control system 132  
Conventional access control systems  
160  
cookie hijacking 231

**Corrective Controls 12**

cryptocurrency 120

cryptography 80, 82, 86, 87

cyberattacks 212, 217, 222, 223,  
228

cybersecurity 47, 57

**D**

data analytics 206

databases 2

Data breach 72

Data encryption 56

Data recovery vulnerability 83

Data security 50

data transmission 132, 136, 138,  
139, 141, 147, 148, 152data transport layer security (DTLS)  
135

de-anonymization 194, 195

Denial of Service (DoS) 47

Detective Controls 12

Deterrent Controls 12

Digital transformation 209, 211,  
216, 220

Disaster Recovery 208

domain name system (DNS) 230

DoS attack 230, 232

**E**

e-administration 64

eavesdropping 135, 143

economic denial of sustainability  
(EDoS) 75

Encryption 116, 124

Encryption techniques 47

Endpoint Security 208

enterprise 67, 93, 99

**F**Facebook 176, 178, 180, 181, 182,  
183, 184, 186, 190, 192, 193,  
196, 197, 203

financial analysis 37

**G**

glucometer 116

Google 32, 33

Google Cloud Platform 93

**H**

hardware 32, 33, 37

hardware security module (HSM)  
84

high-performance computers 5

Homomorphic encryption 96

Hybrid cloud 5

**I**Identity and access management  
(IAM) 44

Identity Management 208

Identity theft 193

information disclosure 135, 143

Information Life Cycle Manage-  
ment 15Information Security Society Swit-  
zerland (ISSS) 9

Infrastructure as a Service (IaaS) 3

Intel chip 6

intellectual property (IP) 47

International Telecommunication  
Union (ITU) 104

internet 32, 33, 47

intrusion-detection systems (IDS)  
228intrusion-prevention systems (IPS)  
228

IoT infrastructure 103

## K

Key-logging 48

keystores 114, 115

## L

LinkedIn 180, 182, 183, 185, 194, 200

## M

Malware 190

managed detection and response (MDR) 213

Micro-Blogging 182

Microsoft 32

middleware layer 138, 148

mobile computing 206

multifactor authentication (MFA) 225

MySpace 180, 181, 183, 185

## N

National Institute of Standards and Technology (NIST) 32

network bandwidth 166

networking 2, 4

network interface card (NIC) 232

Network Security 208

## O

Open Cloud Consortium (OCC) 45

open security alliance (OSA) 9

Open Virtualization Format (OVF) 44

order-preserving symmetric encryption (OPSE) 68

Organizations 37

## P

pacemakers 132

Phishing 193

Platform as a Service (PaaS) 3

Preventative Controls 12

private cloud 4

Private Data 15

Profile-based social networks 181

protocol hijacking 139

public cloud 4, 10

Public Data 14

public-key cryptography standard (PKCS) 115

Public key infrastructure (PKI) 113

## Q

Quora 182

## R

radio frequency identification (RFID) 102

ransomware 119

remote servers 33

Repudiation 142

risk analysis (RA) 12

robust integrity 114

## S

Security and system development life cycle (SDLC) 70

security architecture 9, 10, 13

security-information-and-event-management (SIEM) 228

security management 10, 12, 13

Security Operations Center (SOC)

228  
 security risks 35  
 Selective forwarding 166  
 Sensitive Data 14  
 service-oriented architecture (SOA) 43  
 session hijacking 139  
 Sinkhole attack 166  
 social networking sites (SNSs) 176  
 Social networks 176, 177, 186, 187, 194  
 software 2, 3, 4, 9, 10, 15, 16, 17, 22, 24, 26, 32, 33, 34, 37, 44, 49, 52, 53, 57  
 Software as a Service (SaaS) 3  
 software defined networks (SDN) 148  
 software patches 219  
 Spams 191  
 Spoofing 141  
 SQL injection 192  
 standard development organizations (SDOs) 42  
 Storage Networking Industry Association (SNIA) 44  
 Sybil attack 166  
 symmetric searchable encryption (SSE) 68

## T

tampering 135, 142  
 tele management (TM) Forum 11  
 trojan horse 230  
 Trusted Platform Modules (TPMs) 115  
 Twitter 178, 180, 182, 183, 184, 186, 190, 191, 192, 193, 196, 197  
 two-factor authentication (2FA) 220

## U

utility administration 64

## V

Virtual-Gate Authentication 162  
 virtualization 33, 43  
 virtual machines (VM) 44, 64  
 Vulnerability discovery models (VDMs) 229

## W

Web2.0 43  
 WetPaint 182  
 wireless sensor and actuator networks (WSAN) 102

## Y

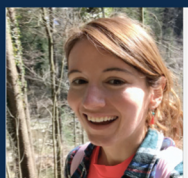
YouTube 183, 184, 185, 197



# Security Designs for the Cloud, IoT, and Social Networking

Currently, the world is facing rapid technological advancement in every field. Unarguably, the most affected area is digital technology. The use of digital devices has increased to a much greater extent in the last decade. In this book three major aspects of digital technology data, social media, cloud computing, and internet of things (IoT) are discussed. This book thoroughly examines the issues and vulnerabilities of IoT services. Due to the low cost of cloud services, almost every organization is storing their data in the cloud. This causes a big chunk of users' personal data to be saved in the cloud, which can be a target for hackers who are always trying to get access to cloud storage. Apart from that, IoT security and its open challenges have been thoroughly discussed in this book. We assume the readers have little previous knowledge of IoT and cloud computing. The first three chapters focus on the cloud and its security aspects. The encryption standards, such as AES and RSA algorithms, are considered in Chapter 1 to understand the working of encryption algorithms for securing data over the cloud. In Chapter 2 the basic definition of cloud computing is discussed along with risk issues and security challenges in cloud computing. The vulnerabilities and threats associated with cloud computing are also discussed. Chapter 3 discusses the roles and responsibilities of the cloud service providers in terms of the security of the user's data. The major focus has been placed on the analytics and its importance for cloud security. In Chapter 4 the IoT and its concepts are discussed along with the discussion of the threats and vulnerabilities of IoT. Specifically, cyber attacks taking place on IoT devices are becoming more prevalent and are increasing by up to 50% every year. In Chapter 5 the IoT aspects of security, such as network access control and software verification, have been evaluated. In Chapter 6 embedded systems have been discussed along their security aspects. Chapter 7 explores different types of social networks. Finally, in Chapter 8 various cybersecurity aspects are examined.

I hope that this book has the potential to be referred by the scholar for their work. It provides them with the up-to-date knowledge on security designs for cloud, IoT, and social networking.



Adele Kuzmiakova is a computational engineer focusing on solving problems in machine learning, deep learning, and computer vision. Adele attended Cornell University in New York, United States for her undergraduate studies. She studied engineering with a focus on applied math. While at Cornell, she developed close relationships with professors, which enabled her to get involved in academic research to get hands-on experience with solving computational problems. She was also selected to be Accel Roundtable on Entrepreneurship Education (REE) Fellow at Stanford University and spent 3 months working on entrepreneurship projects to get a taste of entrepreneurship and high-growth ventures in engineering and life sciences. The program culminated in giving a presentation on the startup technology and was judged by Stanford faculty and entrepreneurship experts in Silicon Valley. After graduating from Cornell, Adele worked as a data scientist at Swiss Federal Institute of Technology in Lausanne, Switzerland where she focused on developing algorithms and graphical models to analyze chemical pathways in the atmosphere. Adele also pursued graduate studies at Stanford University in the United States where she entered as a recipient of American Association of University Women International Fellowship. The Fellowship enabled her to focus on tackling important research problems in machine learning and computer vision. Some research problems she worked on at Stanford include detecting air pollution from outdoor public webcam images. Specifically, she modified and set up a variety of pre-trained architectures, such as DehazeNet, VGG, and ResNet, on public webcam images to evaluate their ability to predict air quality based on the degree of haze on pictures. Other deep learning problems Adele worked on include investigating the promise of second-order optimizers in deep learning and using neural networks to predict sequences of data in energy consumption. Adele also places an emphasis on continual education and served as a Student Leader in PyTorch scholarship challenge organized by Udacity. Her roles as the Student Leader were helping students debug their code to train neural networks with PyTorch and providing mentorship on technical and career aspects. Her hobbies include skiing, playing tennis, cooking, and meeting new people.