AWAZ NAAM SALEEM CYBERSECURITY ISSUES IN SOCIAL MEDIA NEU 2021

CYBERSECURITY ISSUES IN SOCIAL MEDIA

A THESIS SUBMITTED TO THE INSTITUTE OF GRADUATE STUDIES

OF

NEAR EAST UNIVERSITY

By

AWAZ NAAMAN SALEEM

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2021

CYBERSECURITY ISSUES IN SOCIAL MEDIA

A THESIS SUBMITTED TO THE INSTITUTE OF GRADUATE STUDIES OF NEAR EAST UNIVERSITY

By

AWAZ NAAMAN SALEEM

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2021

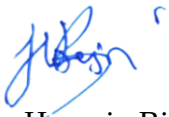
AWAZ NAAMAN SALEEM: CYBERSECURITY ISSUES IN SOCIAL MEDIA

Approval of Director of Institute of Graduate Studies

Prof. Dr. KEMAL HÜSNÜ CAN

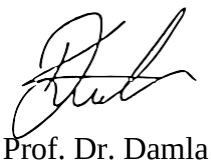
We certify that this thesis is satisfactory for the award of the degree of Master of Science in Computer Information Systems

Examining Committee in Charge:



Prof. Dr. Huseyin Bicen — Committee Chairperson, Computer Education and Instructional Technologies, NEU

Prof. Dr. Fezile Özdamlı — Department of Computer Information Systems, NEU



Assist. Prof. Dr. Damla Karagözlü — Supervisor, Department of Computer Information Systems, NEU

I hereby declare that all material and information in this paper were collected and presented in accordance with academic rules and ethical standards. I also declare that as required by these rules and behavior. I have thoroughly cited and referenced all material and findings that are not original to this work.

Name, Last name: Awaz Naaman Saleem

Signature: 

Date: 6/23/2021

ACKNOWLEDGEMENTS

This dissertation would not have been achievable without the assistance, co-operation, and encouragement of my supervisor; my appreciation and gratefulness go to my supervisor's Assist. Prof. Dr Damla Karagözlü. For her continuous motivation and guidance. She guided me throughout the whole process of writing my thesis. This work would not have been achievable without her clear and inspiring guidance.

I would like to express my heartfelt thankfulness to Prof. Dr. Fezile Özdamlı and Prof. Dr. Nadire Çavuş. Their experience, understanding, and commitment to the highest standards have encouraged and guided me in the right direction. I would also like to thank the academic and administrative staff of the Computer Information System Department for their motivating and consistent service.

My most profound thankfulness and appreciation to my beloved and wonderful family with unending truthfulness and sincere love, for they believing in me and supporting me throughout my life. And a heartfelt thanks to my parents appreciate their unconditional and limitless love, consistent and unwavering support throughout my academic career. Furthermore, I would like to thank my brothers and sister for their assistance and encouragement. Finally, I also have a list of friends I would like to thank who have helped me from the beginning of my studies till the last words. Thank you all for all the encouragement and support you have given me; I wouldn't be here without your partnership in my journey, and this dissertation would not be achievable without your being.

To my parents…

ABSTRACT

Social media (SM), in the modern environment, offers a powerful medium for illustrating expressions, emotions, viewpoints, and interactions among individuals from different aspects of life. SM sites in 2020 have more than 3.6 billion global active users. The growth of SM sites has drawn billions of people to interact and exchange information on these platforms. The presence of large amounts of data and information causes various security threats to these platforms. Therefore, cybersecurity is a significant problem in modern technology ecosystems. Cybersecurity emerges as a critical need to provide a safe and sustainable environment for Internet users. This study aims to conduct a systematic review and analysis of the literature to provide understanding of cybersecurity issues in social media. In addition to many positive aspects of the internet in our lives, there are also some negative aspects. Cases of social engineering, phishing, cyberbullying, malware, etc., because of a lack of awareness and training, SM users can't protect themselves from becoming victims of cyberattacks. The study presented various types of cyberattacks, factors that lead to SM users vulnerable, some recommended methods to gain awareness and knowledge about cybersecurity, and prevention techniques from cyber threats. The study's findings will help SM users, organizations, companies, and regular people. where understanding cybersecurity enhances the safe use of SM and its platforms.

Keywords: Cybersecurity; cyber safety; cyberattacks; social media; social networking site; vulnerability

ÖZET

Sosyal medya (SM), farklı bireyler arasındaki ifadeleri, duyguları, bakış açılarını ve etkileşimleri göstermek için güçlü bir ortam sunmaktadır. 2020 yılında SM sitelerinin 3,6 milyardan fazla küresel aktif kullanıcısı bulunmaktadır. SM sitelerinin büyümesi, milyarlarca insanı bu platformlarda etkileşime girmeye ve bilgi alışverişi yapmaya teşvik etmiştir. Büyük miktarda veri ve bilginin varlığı, bu platformlara yönelik çeşitli güvenlik tehditlerine neden olmaktadır. Bu nedenle siber güvenlik, modern teknoloji ekosistemlerinde önemli bir sorun haline gelmiştir. İnternet kullanıcıları için güvenli ve sürdürülebilir bir ortam sağlamak açısından sibergüvenlik kritik bir ihtiyaç olarak ortaya çıkmaktadır. Bu çalışma, sosyal medyada siber güvenlik sorunlarının analizine yönelik sistematik literatür taraması yapmayı amaçlamaktadır. İnternetin hayatımızdaki birçok olumlu yanlarının yanısıra neden olduğu bazı olumsuzluklar da mevcuttur. Sosyal mühendislik, kimlik avı, siber zorbalık, kötü amaçlı yazılım vb. vakalar, farkındalık ve eğitim eksikliği nedeniyle SM kullanıcıları kendilerini siber saldırıların kurbanı olmaktan koruyamazlar. Çalışma, çeşitli siber saldırı türlerini, SM kullanıcılarının savunmasız kalmasına neden olan faktörleri, siber güvenlik hakkında farkındalık ve bilgi edinmek için önerilen bazı yöntemleri ve siber tehditlerden korunma tekniklerini sundu. Çalışmanın bulguları SM kullanıcılarına, kuruluşlara, şirketlere ve sıradan insanlara yardımcı olacaktır. Siber güvenliği anlamanın SM ve platformlarının güvenli kullanımını geliştirdiği yer.

Anahtar Kelimeler: Siber güvenlik; siber güvenlik; siber saldırılar; sosyal medya; sosyal ağ sitesi; güvenlik açığı

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAA:	Authentication, Authorization, and Accounting
CIA:	Confidentiality, Integrity, and Availability
CPNI	Centre for the Protection of National Infrastructure
DDoS:	Distributed Denial of Service
DNS:	Discussion Networking Sites
DoS:	Denial of Service
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DLP	Data-Loss-Prevention
ICT:	Information Communication Technology
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IEC:	International Electrotechnical Commission
IoT:	Internet of Things
IP:	Internet Protocol
IPS	Intrusion Prevention Systems
IS:	Information Systems
ISO:	International Organization for Standardization
ISPs:	Internet Service Providers
IT:	Information Technology
ITU:	International Telecommunication Union
MitM	Man-in-the-middle attack
MSS:	Media Sharing Sites
ML	Machine Learning
NAC	Network Access Control
NIST	National Institute of Standards and Technology
PLC	Programmable Logic Controller
PMT:	Protection of Motivation Theory

PRISMA	Preferred Reporting Items for Systematic Review and Meta-Analyses
RBAC:	Role-Based Access Control
SCADA	Supervisory Control and Data Acquisition
SE	Social Engineering
SLR:	Systematic Literature Review
SM:	Social Media
SMPs:	Social Media Platforms
SNS:	Social Network Sites
SPBN:	Social Publishing and Blogging Networks
SRS:	Social Review Sites
URL	Uniform Resource Locator
XSS	Cross-Site Scripting

CHAPTER 1

INTRODUCTION

This chapter presents the study's background and problem, followed by the study's aim, the significance of the study, limitations, and an overview of the research.

1.1.Background of the Study

The technology of information plays a significant role in shaping our lifestyle and cultural structure constantly. Society is being structured around the widespread availability and reliability of Information Systems (IS). In the modern era, information technology keeps increasing ubiquity and to the extent that we give responsibility to these systems with national security, privacy, digital identities, and physical safety (Jethwani, Memon, Seo and Richer, 2017). In recent decades, digital technology diffusion has created new opportunities for organizations, individuals, and general society. Indisputable new possibilities for private and public institutions to gather, preserve, and information manage and generate new knowledge to the point that knowledge managing becomes a fundamental part of the organization (Bongiovanni, 2019). Recently, Social Media (SM) websites have been wildly popular. It is a web-based application group that constructs internet-based applications and ideologies that allows the exchange and creation of User-Generated Information (Thakur, Hayajneh and Tseng, 2019).

Equally important, organizations and individuals have become dependent on computer and internet access, most importantly, share information through virtual connections. This tends to make data security one of the most critical issues of today. Protecting individuals and institutions from being attacked by cybercrimes are now a priority for business and academia (Gupta et al., 2018). Furthermore, social media like Instagram, Facebook, YouTube, Twitter, Snapchat, etc., is based around the production and sharing of user-generated information and offered a wide range of applications and services to meet individual’s social requirements. In recent years, SM has been seen as the most common

digital platform for global attention on the internet (Hu et al., 2020; Thakur et al., 2019). These SM's platforms provide novel possibilities for engagement and socialization among users, which have changed the method users share data, such as news, personal information, opinions, and successful online business conducts (Thakur et al., 2019). Today, social broadcasting paradoxically can extend, but yet to restricted, the volume of information that people are exposed to during their use. The ever-increasing amount of information produces difficulties in our ability to truly enjoy user knowledge due to human beings' finite capacity to handle vast volumes of knowledge.

The accommodation and speed of information processing provide efficient communication in digital ecosystems (Netto and Maçada, 2019). With the exponential development of Information Communication Technology (ICT), access to information has become simpler and affordable to almost all. As a result, personal information safety has become a difficult challenge, particularly for any security event in every area of the world; new legislation or regulatory requests for access to private information emerge from time to time (Baazeem and Qaffas, 2020). It appears that social media provide consumers with, particularly paradoxical results that information security usage calculations have been worried about it. Individuals are expected to post personal stories and private details, regularly partake in public conversations and connect to client content.

According to a study done by Hu et al. (2020), citizens are anxious about cyber-security problems, which are supposed to negatively impact their trust in and actual actions in SM's use. As claimed by Baazeem and Qaffas (2020), the privacy of information is the capability to determine the private information of individuals that they have complete control over their data to share or not. It is perceived to become one of the top ethical, legal, social, and political problems of the information age. According to a study done by Zamir (2020) Internet Service Providers (ISPs) divided customers' data into sensitive information and less sensitive information. Sensitive personal information involves "children's, geographic, financial, health, social security numbers, application usage history, the content of the

communication, and web browsing history." The less sensitive personal information holds "address, user's name, subscription levels, Internet Protocol (IP) address, also anything else not exist in the empowerment category. Underneath the new law, internet service providers could sell second-category or less sensitive personal data. However, social media and its consumers have a connection that is impacted by cyber-security and its context. Since the use of social media increase, this relationship often gets more intense as cyber-criminals widen their phishing area and continue to keep their eyes on social media profiles. Because most SM users do not have sufficient knowledge and awareness of security and privacy; therefore, SM utilizers are now one of the hackers' goals (Abd Rahman, Permatasari and Hafsari, 2017).

As a consequence of the robust growth of digital providers all over the world, ICT infrastructure and devices are increasingly vulnerable to cybersecurity and privacy risks, as a growing range of applications demands a high degree of information security and the need for a secure information communication technology infrastructure (Polverini et al., 2018). Furthermore, the real possibilities of the information age have arrived with new safety requirements, manifesting in various forms a framework of constantly changing Information Technology (IT) best practices, new legislative requirements for information privacy, and the schema of developing ethics problems. These standards have a similar origin: ethical, legal, and technological to the growing number of data security violations encountered in current years (Bongiovanni, 2019).

Additionally, the global market for storage capacity and computing power is increasing at a very rapid rate. These directions in the product and utilize ICT tools could influence energy efficiency throughout the operation and manage waste ICT, material efficiency, and generally on the environmental consequences of everything in this sector. The ICT industry will progress in the coming years will be affected by concerns relating to privacy, ecological impact, and cybersecurity (Polverini et al., 2018). Cybersecurity, which includes confidentiality and information security as a subsection, is a global concern. The

modern world grows more integrated and emphasizes information technology development, economy, commerce, banking, health care, and marketing. The management system is continuously taking place in the modern world. Physical, societal, and personal dependency on cyberspace may continue to develop in the upcoming years (Bess, 2017). Over time, diverse variations of cyber-security strategies have evolved in individual countries according to local needs. These developments reflect success in understanding the value of Cyber-security not just for security experts but also for ordinary citizens. Consequently, cyber-situational understanding has hit novel heights, and extra specific safety counteractions are prearranged (Sadik et al., 2020).

As Bashir et al. (2017) stated, improving data security contests is an essential aspect of fixing labour deficits in information security. Moreover, social media users who were using social networks continuously keep rising annually; therefore, data privacy and confidentiality and cybersecurity of personal information are becoming critical issues for social media and as a right for each individual. However, many researchers surveyed to improve knowledge about these significant parts of SM. Nevertheless, we couldn't find a systematic review on cybersecurity in social media. In order to address this gap, this study displays a Systematic Literature Review (SLR) of cybersecurity in social media. The main aim of this study is to provide a systematic review regarding cybersecurity in SM from existing literature.

1.2.The Problem Statement

Social media has made it easier to share information through incredibly vast individuals' networks without wasting any economic and time required for electronic and print media. However, the growing number of SM pages with a range of targets and applications the ever-increasing number of users have made this more difficult (Almarabeh and Sulieman, 2019). In the meantime, internet access is almost everywhere globally, which leads to increasing the number of users and the size of online information shared between users. The growing growth of the internet technologies and access to online information

services and contact with people worldwide have increased the number of participants on Social Media Platforms (SMPs) like “Facebook, Linked In, Instagram, Snapchat, and so on.” Individuals use social media to express their feelings, start conversations, and make themselves known. Since often individuals will be the first to raise a question, they frequently overlook whether the proof provided is genuine or not (Rahman et al., 2020). Moreover, most SM users share personal information, posting news, photos, videos, etc. It has raised internet safety risks that affecting the network infrastructure, cybersecurity confidentiality, and computer systems. Nonetheless, specialists agree that people are the weakest link in a company’s cybersecurity management framework. More specifically, it is suspected that the most prevalent cause of information security flaws is careless and unintentional behaviour by machine users (Parsons et al., 2017; Győrffy et al., 2017).

The increasing reliance of today’s population on ICT has created a new type of weakness, enabling attackers to run behind targets. Air traffic control systems, national defense systems, telephone networks, transportation, power networks, and financial systems are examples of systems that may otherwise be invulnerable (Nam, 2019). As a result of the increasing need for IT management, threats have risen, impeding advancement and preventing complete control of information and data. Malicious systems have spread in many ways and constantly evolve in their complexity, making it much more challenging to avoid dangerous and often destructive outcomes (Almarabeh and Sulieman, 2019).

Nonetheless, as these inventions become more advanced and universal, everyone’s personal information is processed and often shared with known and unknown people, often without understanding (Yun et al., 2019). Cybersecurity is the first vital thread to be considered repeatedly. Cybercriminals found various methods through structural walls and accessing different materials involving social media, software, sports, movies, games, and music. This issue is significant since there are various cases in which someone’s identification has also been hacked. Criminals have targeted social accounts over. The risk of exposing people to diverse unsuitable contented, like pornographic objects, obscene,

harmful, also exploiting, is relatively high. Day after day, advertising campaigns, newspapers, social media, journals are covered with victims of cybersecurity threats besides cyberattacks activities. Moreover, cybercriminals and hackers established and utilized different methods to attack individuals' computer systems and private information (Szumski, 2018). There are different types of malicious software and threats such as viruses, computer worms, trojans horses, bots, social engineering, phishing, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attack, ransomware, spam, hacking, identity theft, malware, pharming, and impersonation (Almarabeh and Sulieman, 2019). As a result, annually, huge numbers of people's personal information and data have been stolen online; cybercriminals attacked millions of computers by one of the presented methods above. Correspondingly, many passwords have been stolen by hackers.

Besides, many online financial account operations have been attacked, and consumers' critical data information has been lost. Accordingly, around are many safety issues around connected devices to the "Internet of Things (IoT)" wireless gadgets, including Bluetooth and Wi-Fi. Besides, intelligent devices involving laptops, television sets, and other small appliances make the IoTs vulnerable to threats due to low cybersecurity points. Different internet protection vulnerabilities include malicious malware attack platforms, which reflect inadequate virus protection and file sharing in popular free services such as BitTorrent, Vuze, Deluge, uTorrent, BitTorrent.

Therefore, the fundamental motivation for conducting the current study is that the individual victims of cyber hackers are becoming widespread. Cybercriminals and cyber threats develop virus techniques to attack; social media users lose their privacy and personal information. As users are the weakest link in online social networks, individuals don't have sufficient awareness of cybersecurity; even some don't know about cybersecurity and cyber-criminals or how to protect themselves from these electronics wars.

1.3.The Aim of the Study

The main aim of this study is to conduct a systematic literature review to provide an understanding of cybersecurity issues in social media. To achieve this goal, the following research questions are answered

1. What are the cyber-attacks for social media?
2. What are the factors that lead to social media websites vulnerable?
3. How does vulnerability differ according to the age of social media users?
4. What are the ways of gaining cybersecurity awareness for social media users?
5. What are the cyber-attack prevention ways for social media users in the literature?

1.4.The Significance of the Study

Advancing technologies in today's developing environment mean that people can store vast amounts of information in cyberspace, allowing multiple individuals all over the world to access it more straightforward. Having information on the internet has been fast and more comfortable than it was years before; susceptibility to cyberspace intelligence entails implementing dependable data security controls to avoid malicious access and unnecessary sensitive information related to government finances and confidential information. At present, social media has become an indispensable part of every person's daily life and share personal information, financial information, news, healthcare, e-commerce, etc.

So, the study is significant in presenting some info and tips about SM security and privacy. Information security is becoming a considerable case for every individual to learn and aware of cybersecurity, cybercrime, and cyberthreats that attack social media users by utilizing social media network platforms. Similar studies on this topic have not been seen in the literature. Consequently, the finding of this study is important for social media users in general, students, employees, companies, even parents can benefit from the finding of the study. They can utilize the social platform more securely if they are aware of the many types of cyber threats and are knowledgeable of the susceptibility factors. Besides, it provides

prevention techniques from cyber threats that they can use and apply to be protected from risk and attacks.

1.5. Limitations of the Study

The limitations of the study can be highlighted as follows:

- Four databases (Science Direct, Web of Science, Scopus, and IEEE explore) are included in this study.
- The study only concerned about cybersecurity in social communication and media platforms.
- Included articles are limited to the years 2015 to 2020.
- Only review articles are included in this study.
- The evaluation of research quality is limited.
- Many reviews did not provide sufficient summaries of the included studies.

1.6. Overview of the Study

The study describes the following five chapters to give readers an understanding of the entire thesis:

CHAPTER 1: Give details about the general introduction of cybersecurity in social media and the background of the study. The study's problem definition, the significance, the study's goal, the study's limitations, and then an overview of the research.

CHAPTER 2: Presents the related research and introduces the theoretical framework whereby various cybersecurity aspects in social media also some facets of social media and its associated concerns were discussed.

CHAPTER 3: Displays a detailed description of the specific research method and the research procedure used to gather and analyze data and select relevant articles systematically using the PRISMA framework. It also describes search strategy, selection criteria, quality assessment, data extraction, descriptive analysis, and data synthesis.

CHAPTER 4: Presents the study research questions' results that provide the interpretation and description of the study. Regarding following PRISMA guidelines, findings with each relevant literature are scheduled for all records. Then, separately for each research question, the items are displayed and listed in a tabular format and then discussing the thesis.

CHAPTER 5: Presents the conclusion of the entire research study and recommendations of the thesis, suggestions, and future studies.

CHAPTER 2

THEORETICAL FRAMEWORK AND RELATED RESEARCH

This chapter presents the theoretical framework and concentrates on previous studies relevant to research about cybersecurity and social media.

2.1.Theoretical Framework

2.1.1. Cybersecurity

The internet is the fastest-growing infrastructure in daily life, and innovations transform the way people act in today's technological environment. The advancement of the latest technologies influences how human beings see and use the internet and other information technology systems. Due to new technology, fast developments in virtually every aspect of our lives, where these technologies are present, make it difficult to secure our private information in a very efficient manner. As a result, cyber-attacks are growing day by day. The exponential development in IS administration throughout the last 25 years has taken the entire world into a new form of defense and threat models (Szumski, 2018). Anyone who uses social media and new technology has at least known specific activity trends on the internet that protect data from hackers. Besides, having terms such as hacking and data security in news headlines about cyber-security is becoming a widespread discussion between technology utilizers (Szumski, 2018).

The development of the internet and SM allows people to entertain two domains: their actual life and virtual reality. Through search engines like google, Yahoo, and video distribution platforms like YouTube, all content is now accessible at an individual's fingertips. Nevertheless, cyberspace's growing field can also have detrimental consequences on internet users, such as cybercrime. Therefore, those problems should be included early enough that they may not have a significant impact, so internet users' introduction of cyber-security is very substantial (Rahman et al., 2020). Tirumala, Valluri, and Babu (2019) argued

that cybersecurity is a universal term associated with the computer's security, the internet, and information security; still, it is necessary to recognize the field, proper usage, and application. While many people are misunderstood, cybersecurity is not limited to ensuring devices on the network. Cybersecurity history goes back to the 1970s, before most citizens had a computer (Townsend 2019; and the future of tech, n.d). Figure 2.1 shows the history of cybersecurity from 1969-2020. Cybersecurity, as highlighted from various previous studies, can be defined as it is a universal term. It is the body of processes, technologies, methods designed to protect the computer network, information, software, applications, and internet (Khidzir et al., 2016; Tirumala et al., 2019; Jabee and Alam, 2016; Xiong and Lagerström, 2019; Michael et al., 2019; Scheponik et al., 2016; Das and Patel, 2017), from damage, unauthorized access, or attack, the security term means cybersecurity in the computing environment (Khidzir et al., 2016; Jabee and Alam, 2016; Rahman et al., 2020). These properties would be vulnerable to malicious and hacking attacks without sufficient security (Xiong and Lagerström, 2019). Michael et al. (2019) showed that protecting the above assets from attacks aimed at changing, accessing, or destroying delicate information, obtain by force money from utilizers, or disrupting regular business operations.

Furthermore, the International Telecommunication Union (ITU) gives the meaning of cybersecurity as the collection of different tools, related policies, safety safeguarding conception, and guide-lines. Also, risks management and assure performance to practice, use technology to preserve and protect information technology infrastructures (Sadik et al., 2020). The ICT has brought significant transformation in human beings to live, do business, and communicate (Rahman et al., 2020; Chang and Coppel, 2020). The existence of the www organizations and individuals can share any information, but it will harm people's lives if used for destructive purposes (Rahman et al., 2020). The cybersecurity aspects have become significant because of the increasing combination of technology in various fields like banking, entertainment, finance, communications, national defense, government department, and e-commerce (Baazeem and Qaffas, 2020). New technology is facing undisputed transformation, which may lead to more difficult cyber vulnerability. Nearly 40 percent of

countries world-wide anticipate cyber threats, making cybersecurity a global problem that requires essential efforts throughout the whole level (Alali et al., 2018).

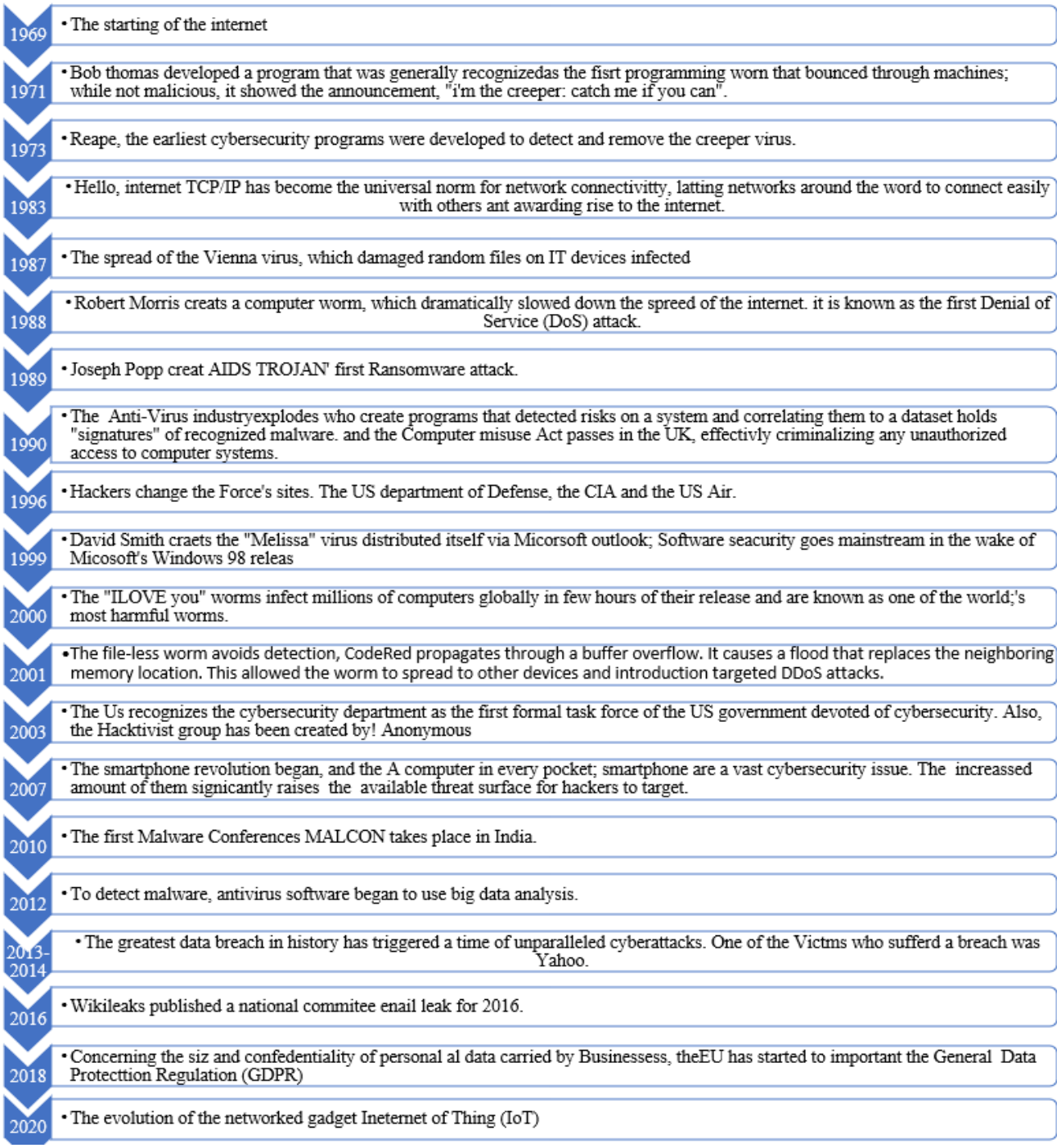


Figure 2.1: Cybersecurity Trimline (1969-2020) (Townsend, 2019)

Accordingly, Sadik et al. (2020) illustrated that cybersecurity involves developing and maintaining mechanisms related to monitoring potential cyber-attacks and minimizing costs. In effect, it is a requirement to adopt a stable computing environment to protect the functioning of new, innovative communities. There is an increasing need to enhance the cybersecurity climate, but security advancements lag due to the persistent rise in disruptive online activities. According to the Global Risks Report of the World Economic Forum (WEF), 2019, cyber-security attacks are presently surrounded by the top global risks.

Additionally, cybersecurity seeks to preserve information from criminals, which is affected private and public organizations, individuals, big and small companies, transnational organizations, and significant infrastructure schemes (Chang and Coppel, 2020; Michael et al., 2019; Sadik et al., 2020). As tales of data theft, hacking, the shutdown of the system, hate speech, and fraud create anxiety and fear about utilizing modern technology (Chang and Coppel, 2020). As maintained by the WEF, the evaluation for cyber security's business value is assumed to expand in 2024 from one hundred twenty to three hundred billion. They argue that computer security often necessitates a broad area, ranging from designing secure networks that can avoid attacks to building systems and techniques which can produce irregularities and identify risks, ensuring a system's adaptability and announcing a strategy to any dangers. (Sadik et al., 2020).

Al Amro (2020) studied infrastructure security in government and cyber in fairness. He emphasized in his study that the relationship between human rights and cybersecurity, in critical the right to freedom of expression and privacy, is continually changing. Besides increasing movement in electronic records for health, government ID's education indicates that the value and importance of information have become valuable to individuals who want to infiltrate the system for reputational profit, financial winnings, and cause weakness to show vulnerabilities that exist. The internet has not been designed with safety and not considered in mind, but much of the world's data sources are being transmitted via public networks; thus, the world's information is susceptible to attack (Michael et al., 2019).

Al Amro (2020) stated that since the infrastructure of the internet has not been taken cybersecurity into consideration, including security protection of the current internet architecture and IP required substantial modification, which including infrastructure security, incorporation of security into its design, secure operating systems, secure coding, mechanisms that protect computers, data, capacity, and access control lists. The growth in the use of technology apps has resulted in a rise in cybercrimes, thereby improving cybersecurity. Enhanced cyber-security is accomplished by information security strategies like using one-time login protection, preventing malware threats, and users' virtualization (Baazeem and Qaffas, 2020).

Besides that, users often do not strictly follow the regulations and rules or be unsuccessful in practicing the proposed protocol when utilizing ICT. Although most networks are theoretically stable, "human error" facilitates a significant cybercrime proportion (Chang and Coppel, 2020). Human factors are another essential feature of cybersecurity that can consider between challenge problems to mitigate and manage. General cyber-security risk circumstances like privacy violation, Phishing Pods, corporate espionage, the hazard of losing the legal conflict, malware, and viruses, productive loss (Khidzir et al., 2016).

As a consequence of the insufficiency of security, different cybercrime has appeared in the previous decades. Data security plays a considerable function in the modern enlargement of services and IT. Information security is also an effort by people to keep their secret and technical knowledge secure from online threats. The highest number of users are unaware of the dangers and unintentionally express their ideas, and their lack of awareness leaves them more vulnerable to cyberattacks (Das and Patel, 2017).

It is of most significance to sustainability achieve security in cyberspace, maintaining digital protection and secure information. In everyone's interest, it focuses on defending the information ecosystem from hackers and malware, thinking about the consequences of a large wave of ransomware in recent decades (Sadik et al., 2020). Baazeem and Qaffas (2020)

declared that cybersecurity must be pursued through sufficient technical and procedural security controls. However, this is not enough since hackers continue to invent various ways to commit serious crimes that supersede these security creativities' capacities. In addition to incorporating data security technology, training the community about using it effectively is essential. Cyber protection and data ethics need to be incorporated into the education framework right from the outset.

2.1.2. Cybersecurity framework

The extensive use of electronic information systems connected with the development of the companies transferred within the web-based industry has increased the need for companies to secure confidential and users' information from nations and malicious cyber actors. As a result, several companies have realized the value of adopting efficient cyber protection practices (Grispos, 2019). Increasing security has ensured that any transaction or action on the online public access platform faces many threats from spyware, malware, and hackers. Companies have enforced effective and reliable cyber defense measures to counter evolving cyber threats like espionage, warfare, and cybercrime. Risks have contributed to the evolution of the framework into a national security problem, that one has now become a vital agent that has impacted universal communication nowadays (Baazeem and Qaffas, 2020).

As Aminzade (2018) stated in his study, there are several options available to consider the evaluation of security risk, the most universally identified frameworks are both the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO). According to (ISO/IEC), cybersecurity involves implementing confidentiality, integrity, and availability of information in cyberspace (Grispos, 2019; von Solms and von Solms, 2018; Ribeiro et al., 2018). Al Shamsi (2019) given a substance that most countries in the European Union, Australia, America, and other nations have been defined cybersecurity concepts, e.g., the idea of cybersecurity in India includes the defense of both the information systems and information. Australia described cyber protection as a standard that applies to information property to guarantee its availability, confidentiality, and

integrity. However, France described cybersecurity as resistance towards any breaks of integrity, confidentiality, and data availability.

2.1.3. Types of cybersecurity

Nowadays, humans and the world are dependent on technological devices; however, neglecting the possibility of cybercrime occurring in individuals' businesses is very dangerous and harmful to the employees, business, and customers. The company is operating in danger for cyber threats without a sense of security (Mindcore, 2018); therefore, defending ourselves and our companies online is more critical than ever. Cyberattacks will take place right underneath our noses, and it is impossible to control all the private information we store on the web with more and more data online (Bootstrap Business, 2020). Thus, protection from different kinds of cyber-security threats necessarily involves knowledge of the various types of cyber-security (Asher, 2020). The following are multiple kinds of cybersecurity users should learn and aware of.

2.1.3.1.Cybersecurity of critical infrastructure

Maintaining and securing the integrity of physical systems are related to the cybersecurity of the critical infrastructure on which modern communities depend (Mindcore, 2018; Asher, 2020; San Juan, 2021). According to Mindcore (2018); and San Juan (2021), the critical infrastructure general examples include hospitals, smart grids, traffic lights, water refinement, and Shopping centres. So, with the smart grid on the internet, it is vulnerable to cyber threats. Vital infrastructure companies must take due care to consider and defend their enterprises from vulnerabilities. Security and stability are essential for the safety and well-being of society. Companies who are not accountable for critical infrastructure, but depend on them for part of their operation, should create a mitigation plan to determine the possible impact of an assault on critical infrastructure (Mindcore, 2018).

2.1.3.2. Cybersecurity of cloud

Most users' activity during online lifetime is storing within the cloud. For backup, most users utilize online services like OneDrive for Microsoft, Google Drive, and iCloud. Because of the vast volumes of data stored on these platforms, it is substantial these platforms remain secure all the time (Reid, 2021). Over the past decade, cloud-based storage data has become a widespread choice because it is improved privacy (Bootstrap Business 2020). Enhanced cybersecurity is one of the fundamental causes that the cloud took over. Cloud security offers the safety and control of data on individuals' cloud infrastructure by a software-based security platform (Mindcore, 2018).

Additionally, cloud systems are increasingly being integrated into economic models, and they must be appropriately configured to preventing any effective attacks (Asher, 2020). To ensure suitable cloud safety measures were in their place, the users should be considering the end-utilizer interface, data storage protection, recovery plans, and human error that disclose the network (Reid, 2021). Although cloud storage is more protected, users must secure it with a security application that detects activities and warns their cloud account if unusual incidents occur (Bootstrap Business, 2020).

2.1.3.3. Network cybersecurity

Network cybersecurity is one of the significant information technology infrastructure fields, so a safety evaluation of network safety is of considerable significance. And its examination should consider features and safety associated with network equipment, also identified as protection gateways. Any of these are open to businesses in any way. The test parameters are also the topology type of the network: the number and type of security gateways, physical or logical (Győrffy et al., 2017). Cybersecurity concerns external risks, network security guards against unwanted interference with malicious intent on the internal networks (Bootstrap Business 2020; Mindcore, 2018). Protection of the network guarantees stable intern networks by safeguarding and blocking access to the infrastructure. Security departments also use Machine Learning (ML) to flag suspicious traffic and alarm them to

real-time threats to handle network security surveillance. Network protection refers to all of the mechanisms responsible for keeping the network secure from unwanted entry and unauthorized intrusions. A reliable networking architecture protects the integrity of the intranet, remaining uncompromised (Asher, 2020; Reid, 2021). Also, it is comprised of hardware and software designed to safeguard the data and network by monitoring connectivity and preventing attacks from accessing or spreading across the networks (San Juan, 2021). It uses various tactics to deter malicious malware or other breaches of data (Reid, 2021). Accordingly, in their reports, both Mindcore (2018); and Bootstrap Business (2020) presented the famous typical cases of network cybersecurity as follows: additional logins, secured and new passwords, and application security.

2.1.3.4. Cybersecurity of the internet of things

IoT introduced a broad difference to non-critical and critical cyber-physical systems such as sensors, applications, printers, televisions, security cameras, and WiFi routers. It is a broad and expanding field of cybersecurity aimed at securing a wide range of customers and enterprises with IoT physical systems like programmable devices, doorbells, watches, and many linked devices (San Juan, 2021). According to Mindcore's (2018) report, during 2021, the global IoT markets will rise to about 520$ billion, the IoT's information center, consumers, analytics, networks, devices, connectors, and the legacy embedded system they're the core IoT business technologies. IoT devices are usually shipped and provide little to no protection patching in a vulnerable environment. For both apps, this creates unique safety problems for every user. The study also found one of the most critical IoT problems acceptance is security. Also, if security issues were resolved, businesses would purchase more IoT products on average. And Businesses are optimistic about the importance and development of IoT. To propose and execute more strategic resolutions, vendors must engage in learning from security problems. While that is going on, IoT devices are almost challenging to prevent, and your best choice is to find an IT provider to handle your protection.

2.1.3.5. Cybersecurity of applications

Technological application usage has helped work efficiency be improved, streamlined, and problems to be solved. It has since exposed businesses to the ability for cyberattacks to lose their knowledge. In the process of incorporating technologies in an enterprise, data privacy thus becomes a crucial feature (Baazeem and Qaffas, 2020). Using both hardware and software to assure the apps are secured from external attacks, even in development. Applications must be constantly updated to keep ahead of any new risks, vulnerabilities, and errors that could be exploited to destructively impact (Asher, 2020; San Juan, 2021). Moreover, the user interface of smartphones was fundamentally changed by web apps. Most smartphones have GPS and BlueTooth, memory, WiFi, Battery, Camera, Data Storage, and many other sensors, such as light sensors, microcontrollers, etc., for detecting and connection capabilities (Awojobi and Ding, 2020).

Besides, most software systems are not entirely independent and require a certain level of employee decision-making to do valuable processing effectively. Well-determined software interfaces for users offer logic, meaning, and feedback for human decision-makers making required personal decisions more straightforward and more successful reliably. The individuals must ensure that human decision-making tech support offers total satisfaction for what could be called first-order education about the software process for users. Similarly, it can be combined to help the user's view outside the independent application definition of second-order education (Győrffy et al., 2017).

Mobile apps often build a user account for identification or tagging on their server; by default, they can also monitor the handset's sensor and networking functions. This ensures that if a third-party developer controls the smartphone device, the application developer will gather confidential user data without the user's knowledge (Awojobi and Ding, 2020). Therefore, the protection of the information stored on the apps that individuals use to manage their business is significant. As apps are more convenient and accessible across different networks, they are mainly available for cyber-attacks (Bootstrap Business, 2020). It is safe

that you choose application protection as one of the many protection steps that must be taken to secure your devices. The safety of applications uses hardware and software techniques to respond to external threats in an application's development stage. Application across networks is much more available, and the acceptance of security mechanisms is imperative during the growth phase (Mindcore, 2018). For this reason, the reporters distributed by Mindcore (2018); and Bootstrap Business (2020) summarized that the users could keep from harm and protect their application by using cybersecurity antivirus applications, use encrypted program services, and firewalls. In other instances, to defend against a security violation, the owner of devices needs to perform the authority; it is necessary to implement password security policies such as biometric authentication and use powerfully complex passwords, age and reuse criteria (Awojobi and Ding, 2020). It leads to avoiding unwanted entry. Companies may also identify and secure critical information assets and preserve them through particular apps protection framework processes linked to these information sets (Mindcore, 2018).

2.1.3.6. Information security

The protection of motivation Theory (PMT) in 1975 has been developed by Rogers that argues that peoples' intention or motivation to secured themselves from harm based on four aspects: the perceived intensity of a harmful event, the perceived vulnerability that probability of occurring, the effectiveness of the suggested behaviour or defensive activity, and self-efficacy at performing reducing risk perceived; since several security-related behavioural criteria associated with the execution of such experiments are difficult to analyze, PMT theory has established a robust theoretical basis for information security studies (Alqarni, Algarni and Xu, 2016). In the context of information safety, it has been proposed that perceived severity and perceived susceptibility increase the range to those individuals understanding malicious information technology as harmful or risk (Wang and Rao 2017).

Additionally, the security of information highlights issues about the safety of users' data. Thus, it is characterized by the scope of damage, disclosure, alteration, and misuse of individual data. And privacy centres for personal data use are described as how much users monitor and influence their data on behaviour, attributes, and characteristics (Hu et al., 2020). As Van den Bergh (2018) addressed in her study, the danger to information security, honesty, and availability is sadly raised in our linked world. While the social network has some overly optimistic qualities, it tends to be associated with a hint that information security is unacceptable.

Nearly 35% of younger users ignore the harmful security component of information, as Győrffy et al. (2017) in their study highlights that the number of cyberattacks can be minimized by information technology used to implement safety measures. However, when the rules required to reduce defined threats are expanded continuously, you cannot obtain an acceptable degree of cyber-attack mitigation or data loss. Junior administrators, elected officials, or individuals from elsewhere make critical information insurance decisions without comprehensive and detailed expertise and experience. Also, the study found that this suggests real risks in the cybersecurity environment and high-risk factors. The proactive guide-lines on the protection of information allow people to appreciate the importance of the laws. They do not know about the need for confidentiality of knowledge and understanding social engineering how the corporation is not casualties of a potential assault on social engineering.

Awojobi and Ding (2020) illustrated those four controls could be summed up in the technology for information security and privacy: controls to access, controls to flow, controls to inference, and encryption controls, and that reported that the four authorities yet apply to advanced privacy and information security.; even though numerous new control models were invented, Role-Based Access Control (RBAC) has been extensively involved in modern computer systems. Several large data consumers, including Apple and Google, have implemented various privacy controls.

2.1.4. Requirements of cybersecurity

Cybersecurity is a field of increasing concern for all telecommunications companies. Technicians are becoming ever more dependent on the smart grid for better operations and services. This increased dependency renders it more vulnerable while at the exact moment amplifying the inherent outcomes of effective cyber-attacks. Efficiency companies of all types are responsible for ensuring that their cyberinfrastructure is sufficiently secured; however, limited utilities typically do not even support committing to cyber defense (Kaster and Sen, 2015). Continuous ICT growths lead to transforming the conventional energy infrastructure into the smart grid to an increasing extent. However, one of the main drawbacks of smart grid implementation is cybersecurity challenges, cybersecurity problems bog down network applications' advancement. Still, incremental changes will boost innovative grid activities over the next few years. Intelligent grid cybersecurity concerns require ensuring the CIA triangle of control systems and ICTs. The CIA pattern characterizes the three fundamental priorities of the cybersecurity (Confidentiality, Integrity, and Availability) triad is essential for communication infrastructures and the operation, security, and administration of capacity (Gunduz and Das, 2020; Nweke, 2017; Khidzir et al., 2018; Michael et al., 2019).

In addition, the classical CIA triad is also used as the foundation for an IT risk evaluation. The co-operation between three parameters, secrecy, honesty, and availability, is challenging to accomplish. More attention on availability is likely to negotiate integrity and confidentiality while focusing on integrity and confidentiality will eventually affect availability (Aminzade, 2018). However, the organization's cybersecurity goals are to protect the CIA of information properties and information within its independent cyberspace. Differing methods can be implemented to accomplish this goal, including implementing security strategies, security controls, guidance, and standards using hazard assessment methods, training programs, and education. These methods have persisted and developed for many decades and been identified as generational waves (Grispos, 2019).

Besides, Nweke (2017) clarified that cyber-security goals are accomplished using the (AAA) or three-A scheme. At the same time, AAA refers to (Authentication, Authorization, and Accounting). Another principle of cyber protection on distributed generation is cybersecurity objective and cybersecurity requirements as high-level cybersecurity objectives including confidentiality, integrity, and availability and specified cybersecurity requirements covered: authentication, authorization, authenticity, accountability, privacy, survivability, dependability, and safety criticality (Gunduz and Das, 2020). Furthermore, looking at the definition of cyber-security as described earlier, it is clear that the context of cyber-security necessarily requires the safety of online end-users as well as all the processes that are used to verify the integrity, confidentiality, and availability of applications and data (Al Shamsi, 2019); as well as Authorization, Authentication, and Accounting (Nweke, 2017).

2.1.4.1. Cybersecurity confidentiality

Confidentiality of information indicates that the customer may trust that their sensitive information would not be distributed with others who are not explicitly authorized to access it. This method can be partially accomplished by implementing control access mechanisms, such as allowing only specific individuals access or information access and processing. Resources hiding is another significant part. Organizations may not want people to know about the exact equipment they use, and so the very presence of such facilities must be protected confidential. The confidentiality of the data is either violated or not. (Michael et al., 2019).

Confidentiality indicates the security of sensitive data that can be easily affected and the limitations on the utilize and holding of various type of information from the unauthorized acknowledgement (Khidzir et al., 2018; Grispos, 2019; Bertino, 2016; Nweke, 2017; Scheponik et al., 2016; Ribeiro et al., 2018; Kaster and Sen, 2015; El Mrabet et al., 2018; Awojobi and Ding, 2020). In his study Nweke, 2017 stated that confidentiality is interesting viewing of information or data because if unauthorized or wrong people have seen that data or information, several difficulties could appear. Similarly, the meaning of confidentiality

according to ISO 27001 secrecy is a feature that refers to the information. Preserve, protect and ensure the interests of information include verifying that it is not made public or leaked to unauthorized individuals. In this case, entities accommodate both processes and individuals (Ribeiro et al., 2018; El Mrabet et al., 2018). Moreover, Tu et al. (2020) defined confidentiality as ensuring that the information's contents were not leaked illegally. Confidentiality is lost as improper distribution of information happens. For example, information like metering usage, control of a meter, and billing data transmitted between the customer and different agencies must be protected and confidential; otherwise, the knowledge of customers may be modified, manipulated, or being used for other else malicious goals (El Mrabet et al., 2018).

Confidentiality includes privacy and is among the most critical problem for utilizers. The information can never be manipulated by anything or anyone in the system. It is essential to ensure that all type of information is non-tampered and correct. Therefore, the information should not be modified unobserved or unauthorized (Gunduz and Das, 2020). Equally important, about the confidentiality and privacy, Baazeem and Qaffas (2020) clarified that it is crucial to understand and follow privacy from the individuals' perception and recognize the social-historical viewpoint; furthermore, they have been recognized different dimensions of privacy of information, including secondary unauthorized use, collection, errors, improper access, information processing, information collection, invasion, and information dissemination. They also declared that internet privacy perception refers to the consumers' anxiety about online shopping. Electronic banking systems hold data that the company or bank collected on users through clients' interactions online.

Hence, encryption is a tool for keeping information confidential. An encryption function mixes a plaintext with a secret key in a complicated way to produce ciphertext, with the intention that an eavesdropper witnessing the only encrypted text cannot decipher the encrypted text to generate the plain text without understanding hidden essential information (Scheponik et al., 2016). To illustrate, Sadik et al. (2020) said that the attacks' types to

confidentiality are eavesdropping, data injection, sniffing, traffic analysis, masquerading, unauthorized access, and social engineering.

2.1.4.2. Cybersecurity integrity

Among different types of cybersecurity problems, the integrity of the information attacks, whereas criminals' access to the data that is supposed to be protected and the introduction of incorrect information is of great significance to the society to predict since the input quality of the data directly affects the prediction precision (Luo, Hong and Fang, 2018). Integrity has been defined as information protection and preventing data from unauthorized alteration, modification, and destruction (Gunduz and Das, 2020; Khidzir et al., 2018; Bertino, 2016).

Integrity Safeguarding against inappropriate data destruction or modification includes ensuring authenticity and data nonrepudiation (Kaster and Sen, 2015). Grispos (2019) in his research, defined integrity as "the completeness, accuracy, and validity of data according to expectations and business values. Correspondingly, in another study, Scheponik et al. (2016) highlighted integrity and refers to the difficulty of recognizing whether information has been changed either in transit or at rest. On the other hand, the CIA framework of cybersecurity for integrity requires that the individuals should feel safe as their information transmitted, stored, and processed have not been modified from its initial form maliciously or accidentally (Nweke, 2017), also in the context of cybersecurity, it requires safeguarding information completeness and accuracy (Ribeiro et al., 2018; Gunduz and Das, 2020).

Further, integrity helps continue providing network architecture with a completely safe time surveillance system. Safety guarantees the security and accuracy of the information; truthfulness consists of keeping records private and avoids unauthorized data misuse (Tu et al., 2020). From this angle, a conventional data integrity attack is called a False Data Injection Attack (FDIA) (Tu et al., 2020; Luo et al., 2018; Sadik et al., 2020).

Likewise, Sadik et al. (2020) presented the integrity attacks type such as masquerading, load-drop attacks, spoofing, time synchronization, replay, and wormhole. Additionally, a smart system should still be available all time. It is also essential to ensure that the accessibility and use of the information system are timely and reliable. Availability and reliability impact critical infrastructure control systems directly (Gunduz and Das, 2020). Accordingly, integrity within an intelligent network requires defending against unauthorized information alteration or loss. Unauthorized data deletion, alteration, or degradation in an unrecognized way is a lack of credibility. For instance, Power Injection is a deliberate attack by an enemy who smartly changes measures from energy movement to the state evaluated, power injection, and retranslates them from them. To uphold integrity, both authenticity of information and nonrepudiation are required. Non-denial indicates that individuals, organizations, or entities are incapable of implementing a particular activity and rejecting it later; originality is the evidence that information is produced from legal sources (El Mrabet et al., 2018).

As Michael et al. (2019) lighted, integrity involves the trustworthiness and correctness of the information; the honesty of information must be more valuable as many sectors utilize decision making and data-driven. If the info holding behind the decision is damaged, the effects of that determination are destructive for businesses, governments, individuals, and communities. Prevention mechanisms are necessary to prevent unauthorized data changes or any effort to modify data unofficial, and disclosure tools to communicate when the data's integrity is no longer confident. To maintaining integrity, prevention mechanisms should be used. These honesty structures are especially relevant in managing authorized cyber-physical foundations in telecommunications, energy, water, gas, oil refining, transportation, and waste control.

2.1.4.3. Cybersecurity availability

Security of the information system from disturbance is the availability. Access attacks can cause the delay of information or block, corrupt it (Gunduz and Das, 2020). Consequently, many previous studies defined availability as the accessibility of information and ensuring reliable and timely access to authorized individuals in the smart network, and using data when it is required (Gunduz and Das, 2020; Kaster and Sen, 2015; Scheponik et al., 2016; Bertino, 2016; Grispos, 2019; Khidzir et al., 2018; Michael et al., 2019; El Mrabet et al., 2018; Tu et al., 2020). Availability is the most significant protection standard in intelligent frameworks because losing availability income disable access to the innovative grid information (El Mrabet et al., 2018).

Accordingly, with all cybersecurity standards, availability warranty in place for co-operation with software, hardware, processes, individuals, and many utilizers allowed to do their work must be capable of doing. Therefore, it enables authorized customers to quickly access the required services and the resources they need while ensuring that systems have complete understanding and capacity balancing in the case of an accident or catastrophe of cybersecurity (Nweke, 2017). Khidzir et al. (2018) explained that the cybersecurity uncertainty in modern social media is aroused by the highest moderate positive relationship between honesty and information availability. The degree to which content is accessible in social media is moderated between integrity and accessibility. Info integrity should not significantly affect the information available that can cause a danger of modern social media for cybersecurity. The poorest moderate partnership in current social media was between information secrecy and cyber-security risk availability (Khidzir et al., 2018).

Still, attacks such as (DoS) may block or delay legitimate users' access. Such attacks are currently rising alarmingly at the current time. Cybercriminals profit from an individual's financial, personal, or confidential information through cyber-theft or cyber espionage. Cybercriminals attempt to take control of such networks through botnet malware. In particular, it may be determined that the availability, confidentiality, and integrity of the

information and internet-based info system are usually staying endangered through effective cyber-attacks (Thakur et al., 2019). Also, Attacks on availability are (DoS) denial-of-service (Tu et al., 2020; Sadik et al., 2020) buffer overflow, low-rate DoS, spoofing, time synchronization, smurf, wormhole, masquerading, and teardrop (Sadik et al., 2020).

2.1.4.4. Authorization

The authorization ensures that a person has the proper level of arrival based on their certifications. This is linked to the principle of most insufficient privilege, which asserts devices, users, processes, and programs must be allowed sufficient permission required to do their jobs and not more. Any license that goes behind the regular work function unlocks the door to occasional or malicious breaches of availability, confidentiality, and integrity (Nweke, 2017). Moreover, the authorization ensures that the authentication and other cyber-security specifications distinguish between legal and unauthorized actors. If breached, approval could give rise to security problems. Access management provides that services are reached in an intelligent grid correctly defined by the corresponding workers and parties. Strict access management procedures should be executed to prevent unauthorized access to sensitive data and critical infrastructure. Methods for access control like access control Role-based, mandatory, and discretionary; maybe increase system decrease possible protection threats and reliability (Gunduz and Das 2020).

2.1.4.5. Authentication

The main processes for authenticating a user's identity or device to secure the intelligent framework infrastructure from unauthorized access are authentication and identification (Gunduz and Das, 2020). Authentication, which indicates that you are who you pretend to be. It is called identity when you pretend to be someone, verifying it when you confirm it. Authentication includes evidence in one of three possible forms: something you know, you have, and you are, and these forms are password, key, and fingerprint. Multifactor authentication is considered the synthesis of all of these groups. Confirmation with multifactor makes it impossible for anyone else to authenticate (Nweke, 2017). Authenticity

ensures the data came from a reliable source (El Mrabet et al., 2018). Besides, it helps anyone to confirm if an object's identity is correct. Items can be smart devices, Users, or other network-connected components. A typical authentication approach is to use a password. Established protocols for authentication can be modified for an intelligent grid design. However, the authentication architecture process would be vulnerable to severe errors if energy networks do not pay adequate attention (Gunduz and Das, 2020). Authentication and encryption are obligatory encryption mechanisms to secure the data's security and integrity in an intelligent grid. It is also a necessary mechanism for the detection of threats to data privacy. Both safety standards include asset authentication to determine whether to communicate with data. Authentication and integrity may ensure security for intelligent network apps toward widespread cyber threats like a man-in-the-middle attack, message modification, and impersonation (Gunduz and Das, 2020).

2.1.4.6. Accounting

Accounting that records what users do when they log into a device. It is essential to track users and their behaviour. From the investigative viewpoint, it may be beneficial for an investigator to trace activities that lead to cybersecurity accidents (Nweke, 2017). The contract or accounting is defined concerning this protection condition. It helps the identification by proven proof of affected parties. The properties acquiring the data cannot dispute it later, which is known as nonrepudiation. Accountability requires nonrepudiation. In mobile grid networks, violations of responsibility usually have legal or business implications. The most popular means of maintaining accountability is auditing logs. However, audit records are prone to attacks of availability and honesty. In terms of confidentiality, honesty, and safety, more stable smart grid implementations are required. When a security risk exists, accountability activities will decide who is in charge of it. The network traffic shifts will be seen as facts in the future (Gunduz and Das, 2020).

2.1.5. Social media

For the time being, technologies have changed how groups, individuals, and companies recognize themselves and describe their personality and identity; hence, in the context of investigation on identity theory, IT is becoming more critical (Netto and Maçada, 2019). Social media provides users with the ability to construct and share content, views, information, and interest in a multi-context to many; SM and Web 2.0 are frequently utilized interchangeably. They may be distinguished slightly. The idea of Web 2.0 has been at the forefront of social media and applies Web 2.0. In other words, we use the definition of Web 2.0 to incorporate social media. At the core of social communication is the concept of Web 2.0, which is the application of the idea of Web 2.0. In other words, based on the concept of Web 2.0 is achieved and the means of SM (Khan, 2017).

The exponential growth and everyday development of IT and digital social networks have brought innovative improvements to diverse industries, sectors, and aspects of society world-wide. Science 2.0 and web 2.0 become vital network infrastructure, information platforms, and a vast volume of intelligence for all participating individuals (machine, man, community, and brain, and even brain-like a computer) in the world village for sharing, exchanging, information, wisdom, knowledge, and contribute a large quantity of data. The SM ecosystem focused on content media, organization, stakeholders, diversity, intelligence, and comprehensiveness. Therefore, it helps develop modern virtual social networks and forms organizations (Zhang and Gupta, 2018).

A universal description of "Social Media" is the collection of web-based broadcasting technologies that allow content to be widely adopted, providing individuals with the capacity to emerge from contentment users to publishers. These technologies enable people to communicate to generate value through online collaborations and conversations with the potential to achieve huge scalability in real-time (Khidzir et al., 2016; Khidzir et al., 2018). Another social media definition by Khidzir et al. (2016) is electronic communication form(s) used by which users build online societies to sharing information, personal messages, ideas,

and other contents. Besides exchanging information about their habits, location, status, feelings, emotions, etc., they don't know that their knowledge on social media networks could offer cyber-security threats that may be difficult to mitigate and manage. The SM term involves a grouping of online networking resources for communication goals. However, these resources are not restricted to blogs, micro-blogs, Twitter, chat rooms, forums, e-mail, conversation boards, and SM co-operations like Facebook and social distribution assistance as YouTube. Since these tools are developed for social communication, the purpose is to be used by people for participation, communication, share content, and collaboration (Van den Bergh, 2018).

Correspondingly, in his study Khan (2017) defined social media as the internet-based concept/technologies/tools which enables the exchange and creation of contents that have been generated by the user while allowing users to organize (one of these at least) conversation, identity, relationship, groups, connectivity, share contents, and reputation. Nevertheless, SM instruments are different from conventional media like television, radio, and books due to their content created by the user as they encountered professionally produced range.

Likewise, they change the kind of platforms they offered. The easy access and use of SM websites give the groups considerable well-being, mainly because they are close to real life and information utilization. As the universe is interconnected increasingly, SM has been embedded into the culture and daily life (Van den Bergh, 2018). There has been a widespread increase in recent years in the number of social media users. From 2010 to 2019, the Statista, Data Reportal, & eMarketer company saw consistent subscribers' improvements in most countries. Figure 2.2 shows the significant growth in the number of users during that period.

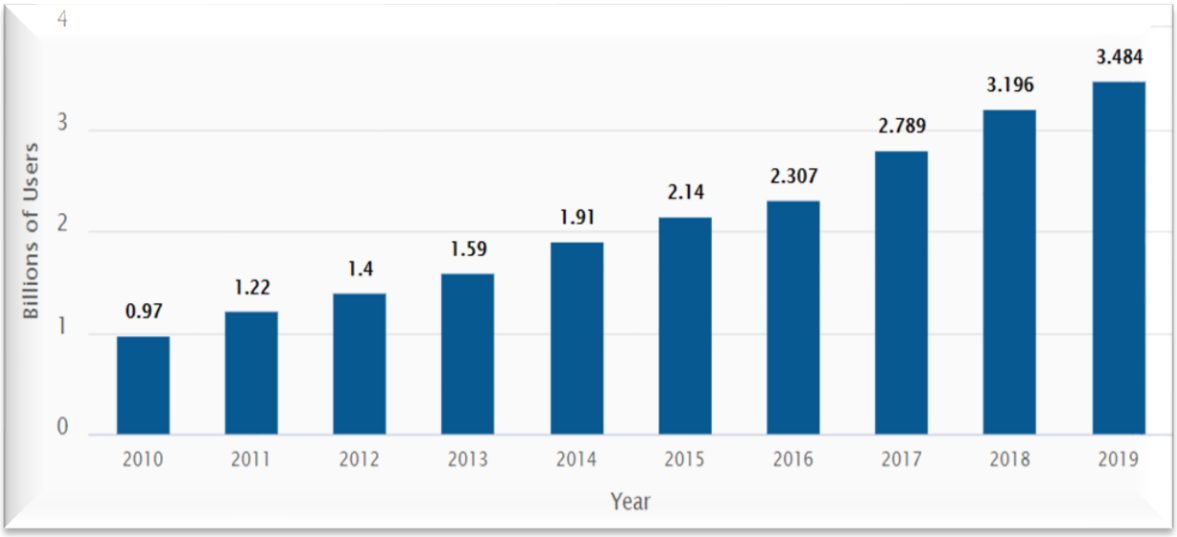


Figure 2.2: Social media users from 2010-2019 (Lambert, 2020)

In his report, Lambert (2020) illustrated that over several geographies, the use of social media is very comprehensive over the globe, that the most active SM sites generate content on a vast range in real-time. Figure 2.3 shows the social media spread rate geographically.

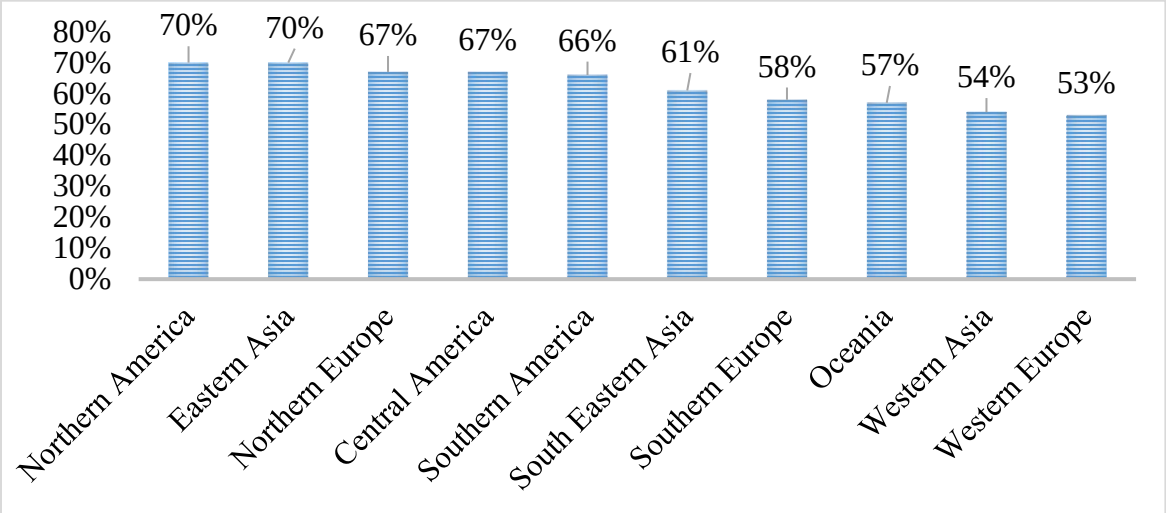


Figure 2.3: The social media spread rate geographically (Lambert,2020)

Further, Clement (2020) addressed that as of October 2020, nearly 4.66 billion people, representing 59% of the world's population, were active internet users. Mobile has become the world's largest internet platform, with 91 percent of all internet subscribers accounting for mobile internet; Figure 2.4 shows the active internet user

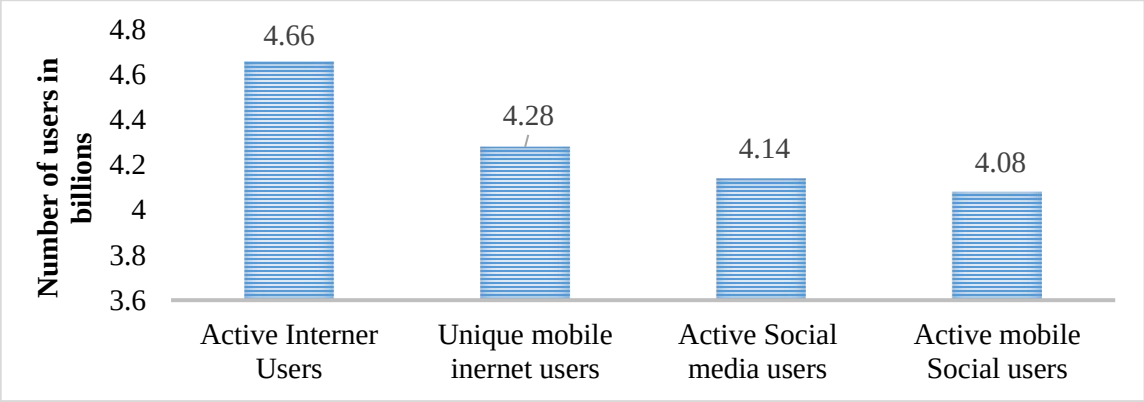


Figure 2.4: The active internet user (Clement, 2020)

In the early 2000s, the SM era arrived, allowing everyone to publish everything using social tools online. Today, we are in the age of collaboration, when people using ICT to develop and share products and services through peer-to-peer trading (Yun et al., 2019). SM sites' history is very short-tempered SixDegrees.com is considered the first forum for social media (Zernetska, 2016). Figure 2.5 demonstrated the social media chronicle timeline.

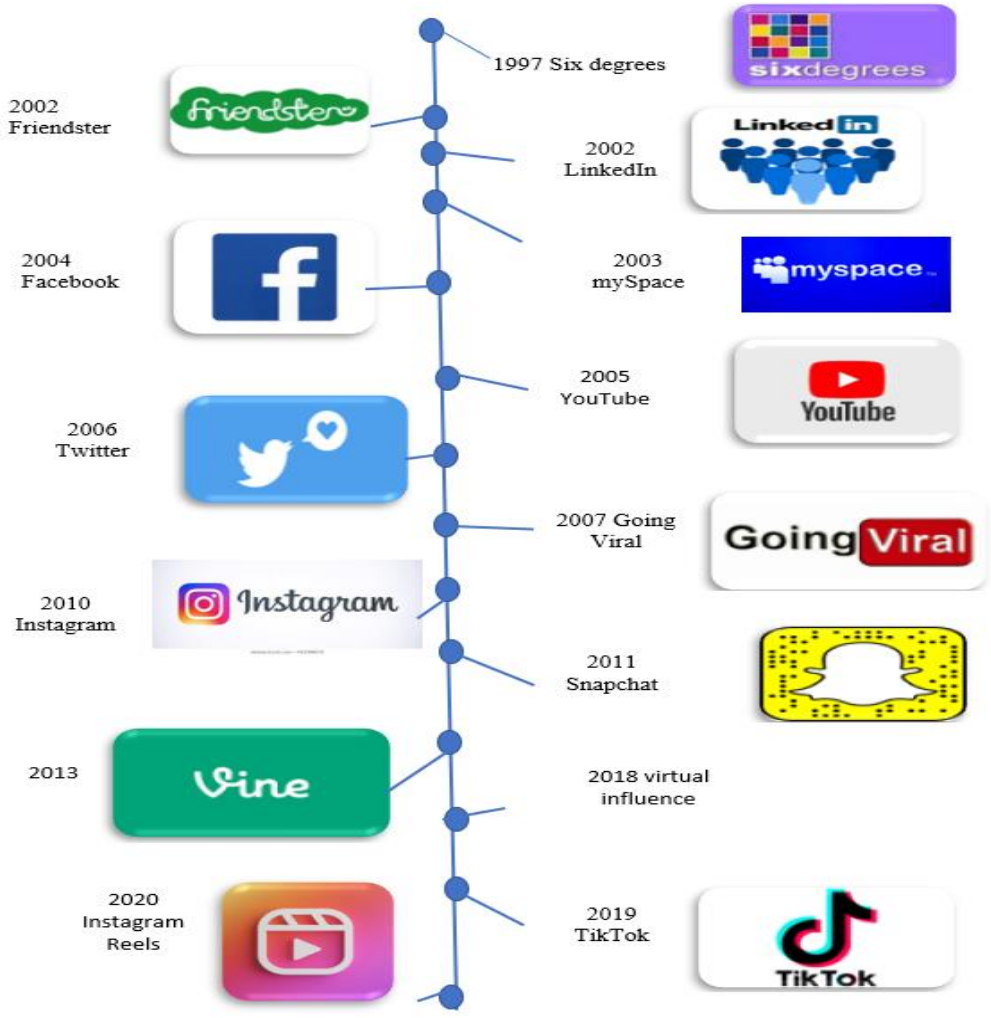


Figure 2.5: Social media chronicle timeline (Vamp, 2020)

In current years, the frequency of social media use has dramatically increased world-wide (Almarabeh and Sulieman, 2019). For example, Clement (2020) addressed that Facebook is the largest social network globally, with more than 2,7 billion active utilizers monthly in the second quarter of 2020. Accordingly, in the same group as laptops, smartphones, and online services, social media have been listed as consumption tools. Despite this, while using social communication, individuals engage in more complex networks than fixed IT tools such as text editors or spreadsheets (Netto and Maçada, 2019). Equally important, Khan (2017) identifies that through its essential characteristics, SM is distinguished from the traditional medium, and this is the only way to understand this according to core features as following: many-to-many communication, participatory, user-owned, conversational, allows openness, relationship-oriented, easy to use and free.

SM may be helpful to different parties through private user information. Users, displays, and renew it voluntarily, in online advertising, data mining, or even psychological assessment of candidates for jobs (Baazeem and Qaffas, 2020). Also, it is used to collecting information on different subjects within social communication and interaction between peers. Various SM resources are available, such as blogs, social network pages, wiki, and forums, where people pursue an interest in information interaction and exchange. A vast quantity of information is thereby generated and made available to the world in the form of unstructured text files (Lima and Keegan, 2020).

Social media has radically changed how firms gather information and interact with their environments. IS research has extensively examined how social communication can enhance traditional business processes like customer service activities and predict or enhance firm value (Wade et al., 2020). Additionally, it has changed dramatically how businesses obtain communication and information with their context. IS investigation has researched thoroughly how SM can strengthen conventional business structures, such as service activity for customers, and anticipate or improve corporate value. But because the internet was initially planned for science instead of industrial use, safety was not taken into account in its

design (Chang and Coppel, 2020). Consequently, the growing popularity led to social networking sites' emergence of a new set of problems and issues facing the twenty-first century (Bhatnagar and Pry, 2020). In understanding the context that cybersecurity issues apply to personal data disclosure, prior IS research examines the role of inconsistency in preserving the critical section of active users for SM (Baethge, Klier and Klier, 2016). However, SM use's value comes at the expense of cybersecurity, which raises the unimaginable risk of losing sensitive information (information safety) and personal information disclosure (Hu et al., 2020). Therefore, SM helps the social engineer use individuals' psychological manipulation to perform information confidentiality operations for data collection targets, system access, or fraud (Khidzir et al., 2018).

Unfortunately, people are looking toward an urgent shortage of a severe lack of cybersecurity professionals as a country; organizations and governments world-wide are express anxiety around the crisis in cybersecurity skills (Jethwani et al., 2017). It is essential to concentrate on the relationship between the user's characteristics, current environment, and the effective message technique when studying human behaviour against online threats. According to categorization, the type, channel, and operators are three principal entities encapsulating social engineering assaults; either a person or malicious program can be the attack operator. The operator type will also specify social engineering attacks (Albladi and Weir, 2018).

Social networks such as Twitter, Facebook, etc. perform an essential role in connecting consumer engagement in recent years. People's willingness to exchange knowledge with millions of audience members is at the core of the unique problem facing corporations in social media. In addition to encouraging others to share content sensitive to business, there is also the power in media platforms to distribute misleading and harmful information. One of the emerging threats is the quick dissemination of false information through SM (Thakur et al., 2019). Accordingly, SM can be used differently to distribute illegal actions. The sharing of hacker services and malicious software is one everyday

activity. These products usually use tools to exploit a system's vulnerability that allows hackers to broke into networks and exfiltrate private data with distributed espionage and DoS attacks (Lima and Keegan, 2020). Unfortunately, most social engineers' key sources of info may have become digital SM to gather required information and data to plan cyberattacks. The increased probability of cyber-security threats happening may have significant implications for the cyber community and organizations, like privacy violations, the danger of losing lawful attacking, Phishing Ponds, productive loss, malware and viruses, and corporate Espionage (Khidzir et al., 2018). Besides, Albladi and Weir (2018) identified attacks type and classified to technical-based that involves malware, came, phishing, or human-based like identity theft, convert social engineering, and impersonation. Thus, cybersecurity concerns have been recognized widely (Baethge, Klier and Klier, 2016); and become severe problems in digital SM because of the growing number of users of the means of social communication globally (Khidzir et al., 2018). That is also the key explanation that people give up on social media (Baethge et al., 2016). Notwithstanding the cyber-security worries, the SM users' population continues climbing (Hu et al., 2020).

2.1.6. Social media types

There are many different types of social media available, whether users explore it for new market potentials or look for new channels to connect with customers. Some of them are quite necessary for any company, while others are beneficial for a junior subset of specialized business (Morrison, 2020); the popular SM types are as follows:

2.1.6.1. Social network sites

The Social Network Site (SNS) is among the most common forms of social media. These networks enable the user to communicate and link with family, friends, brands, and other people online. Most societies are familiar with these types of SNS, and the examples are Facebook, Twitter, and LinkedIn (Storm, 2020; Foreman, 2017; Morrison, 2020). Indeed, SNS is beneficial for the company and can help individuals or stakeholders build awareness of brands, lead new generation, build relationships with clients, offer support and service to

clients, develop partnerships, etc. (Storm, 2020; Foreman, 2017). Further, Morrison (2020) illustrated more advantages for SNS in his report, including access to the target audience through advertising, networking, contacting fans, identifying clients or future collaborators via hashtags and forums, and creating links, also research by the use of social listening devices to track communications throughout specific terms. These will help users to understand the audience better. Many peoples called SNS "relationship networks or platforms of relationship" due to their ability to communicate and build relations; users can share photos, information, videos, and more within these SNS (Storm, 2020; Foreman, 2017).

Facebook and Twitter offer outstanding opportunities to join other audiences and share photos, status updates, links to content, polls, and video. LinkedIn is an excessive place for professionals' connections, enabling the user to build professional relations, find new jobs, select new candidates, and share information (Storm, 2020). Nowadays, and especially after the beginning of the cellphone internet, social platforms attractive hubs that convert almost all aspects of everyday life into a shared experience and from reading the news to posting holiday images (Foreman, 2017).

2.1.6.2. Social review sites

Social Review Sites (SRS) are a category of content that combines benefits to many online services and websites, imagining the shopping process on amazon or the search experience on Google Maps for a local company. User review channels push things a step forward by establishing networks throughout the review as a central value they offer (Morrison, 2020). Examples of SRS are TripAdvisor, Yelp, Zomato, and Glassdoor. Both Yelp and TripAdvisor show comments from members of the community for all types of sites and experiences. This removes many of the speculations which go into booking a hotel or restaurant. Users can search the reviews, and they will recognize a location and know about it somewhere (Foreman, 2017). This SM platform type enables people to review, find, and share information related to products, services, brands, travel goals, and restaurants (Storm, 2020; Foreman, 2017). This SM platform type enables people to review, find, and share

information related to products, services, brands, travel goals, and restaurants (Storm, 2020; Foreman, 2017). Besides, SRS's other advantages are understanding the users' perspective, solving the problems, interacting with the reviewers, and resolving any possible difficulties before converting to a large deal (Morrison, 2020).

2.1.6.3. Media sharing sites

Many people are educated visually. Media sharing sites'(MSS) participation is an excellent location for users' businesses to attract your audience and post visible content. Like primary network relationships MSS are valuable for lead generation, brand awareness, engagement audience, and the majority of individuals' social trading goals (Foreman, 2017; Storm, 2020). Examples of MSS are Instagram, YouTube, Imgur, Pinterest, Snapchat, and Vimeo. These platforms give brands and users who utilize these platforms a place to share and find visible content such as infographics, images, share photos, live videos, videos, and pictures that catch individuals' hearts and fantasies (Morrison, 2020; Foreman, 2017).

While most posts on SNS contain texts, sharing posts on MSS like Snapchat and Instagram beginning with video or an image, employees may determine to add content such as mention another user, captions, or filters that change users look similar to a rabbit. Likewise, on other sites like Vimeo and YouTube, videos are the primary communication mode (Foreman, 2017). Morrison (2020) reflects in his study that people curate, create, and exchange photos that inspire and talk to each other. The company could have an image worth a thousand words. He also addressed that MSS can encourage and promote content created by users: photo sharing sites are a gift for photogenic corporations. Users can manage campaigns to inspire users to take a pic, post a particular hashtag with your product, and generate inspiration by curating, creating, and sharing private photos. They can also engage and inspire users, bonding across a participated interest.

2.1.6.4. Social publishing and blogging networks

Social Publishing and Blogging Networks (SPBN) give brands and user tools to distribute content online in arrangements for another audience that encourage and support them in discovering it, commenting, and sharing. This type of SM platform is an excellent method to build interaction and definition of people to your business. SPBN is a unique kind of SM due to the need to create constant dissemination content; however, they improve brand awareness, visibility, and leads generation, which needs extra work than other SMPs (Storm, 2020; Foreman, 2017). Examples for SPBN are Medium, Tumblr, WordPress. These networks differ from many more conventional blogging sites such as Blogger and WordPress to microblogging co-operations such as Tumblr and interactive common publishing networking platforms like Medium (Foreman, 2017).

Sometimes, the picture will not be involved or complex sufficient for a message that you have to share, but not everyone wants to run online in a blog from a self-hosted web site. Blogging sites for sharing, such as Tumblr and Medium, give human beings space to communicate their viewpoints and connect them with other readers; the social blogs platforms offer an audience and enable lots of room for self-expression customization (Morrison, 2020). As Foreman (2017) reported that SPBN could be useful for business as marketing content could be a highly efficient method to contract with an audience, generate leads, create your brands, sales. Another advantage of SPBN is developing your voice and content inclusion; if you have a blog, you can use society blogging sites to share, re-post, and old content to a new audience (Morrison, 2020).

2.1.6.5. Discussion networking sites

Another particular type of SM platform is Discussion Networking Sites (DNS). These sites focus on information, opinions, discussions, and share news; people recognize and join threads content to see anything people comment on or say (Storm, 2020; Foreman, 2017). Furthermore, these networks may have excellent market research tools. Individuals should take correct, while you must be mindful to keep the advertisements and posts apart, you could

also advertise on them (Foreman, 2017). Examples of discussion platforms are Reddit, Quora, and Digg. DNS such as Quora and Reddit are especially have been designed to sparkle a conversation. Everyone is free to make a question or statement, and that exciting person has common interest sharing and curiosities (Morrison, 2020). Storm (2020) highlights in her report that people can use Quora in their business to make the question and be involved with other people and ask online. Reddit is also a popular DNS to manipulate users to post topics that differ from economics to electioneering to entertaining videos. Except for the sites that have been explained above, there are other various types of SM platforms; in his study Foreman (2017) identified the follows:

Social sites for shopping: Etsy, Polyvore, and Fancy are used to discover trends and follow-up brands, share beautiful discoveries, and make purchases.

Networks that Interest-based: examples Houzz, Goodreads, and Last. fm individual uses it to communicate with others through a hobby or shared interest.

Economy sharing networks: like Taskrabbit, Airbnb, and Uber; the aim of using these platforms is to find, advertise, buy, share, sell services and products among peers.

Social anonymous networks: After School, Ask.fm, and Whisper are examples of these types; the primary purpose of using these sites by some individuals is to vent, gossip, snoop, and bully sometimes.

2.1.7. Social media and cybersecurity

Social media has converted a powerful mechanism for information sharing, solving safety issues, understand current computer attacks. It is reachable for everyone who has an interest in it. Forums and specialized blogs are the entrance place for those who want to acquire knowledge of hacking techniques. Specialist and forums websites are the entry point for those seeking to learn hacking techniques. Otherwise, some SM platforms are convenient tools for individuals who wish to earn money by trading harmful products, like personal information, exploits, and stolen numbers of credit cards. The resources are sold on deep internet sites, where people are primarily concerned with confidentiality and privacy (Lima and Keegan, 2020).

Additionally, the success and popularity of SM have also attracted cyber-criminals, who see SM as a rich environment for their illicit activities. For example, SMPs may be the primary outlets for cyberbullying practices. Social engineers can use SMNs to carry out overt attacks, such as SN phishing and reversal social engineering, and indirect threats. Victims' SN profiles are hijacked to gather the information that enables future attacks in other situations (Albladi and Weir, 2018). Today, cybersecurity media is anxious about users being subjected to attacks on SM websites. Humans' particular harmful intention to mislead other humans is a cyber threat among the most challenging to deal with (Van der Walt, Eloff and Grobler, 2018).

SM's appearance necessarily involves developing an IT system that facilitates consumers communicating as almost equal contributors. This framework creates virtual online communication and social requirements similar to physical online and structure conditions. Therefore, as might be expected, it interacts not only with the technical specifications "hardware requirement and software requirement" of the programs but also with the social demands "human requirement and communication requirement" of the populations (Ahmad et al., 2017). Online social media is gaining all over the world prominence among internet utilizer. Unfortunately, the new SM does not necessarily offer a good result and the desired advantage. There are many threats involved, particularly cybersecurity threats, that may have a significant effect on the cyber environment and the organization (Khidzir et al., 2016).

SM has changed the individuals' lifestyle, and people share almost any events in their daily routine; it has replaced the telephone and e-mail address. However, despite anything on the web, it is necessary to know about threats and risks. PCs, mobile phones, and various technologies are priceless devices that allow people of all ages to communicate and work with everyone else in the world. They will also bring an unfamiliar view into others' lives, whether they live near or outside the world. Sadly, these networks also provide security to people's PC, privacy, and safety (Kalakuntla, Vanamala and Kolipyaka, 2019).

More significantly, these cyberthreats are compounded by a large number of vulnerabilities present in social media websites, such as the amount of accessible and diverse types of SMPs, the inadequate architecture and construction of SMPs, the large volume of unorganized fulfilled, and the possibilities that SMPs offer to individuals interacting maliciously (Van der Walt et al., 2018). Still, SM is primarily targeted at promoting social communication. Many SM sites are often used to search for information, participate in the social association, search for identity, shape, and retain a community. It also offers a means for users to introduce themselves to others through the development of a user profile and the sharing of e-mail, etc. with other users, and the connection to other platform participants to maximize the value of apps that are solely founded on contents that generated by users (Penni, 2017).

Additionally, SM lets social engineers exploit people's media techniques to classify knowledge collection, misuse, or machine access activities. It is now a pool of information for social phishing to harvest and capture valuable knowledge for cyberattack purposes (Khidzir et al., 2016). Hence these aspects also lead to SMPs moving highly unprotected to cyberattacks from unauthorized attackers. Moreover, as a consequence of these cyber risks and SM vulnerabilities, people can see a dangerous rise in the widespread presence of identity theft, cyberbullying, dissemination of pornography, fraud, identity impersonation, and the related (Van der Walt et al., 2018).

Equally important, interaction among SM users is crucial in determining specific internet movements if they are professionals, commercial, social communication, or other ways. Moreover, several institutions, companies, and peoples have familiar with using different SMPs such as Twitter, Facebook, and LinkedIn to communicate with customers and colleagues (Almarabeh and Sulieman, 2019). SM site plays a huge role in cybersecurity and will also add a lot to personal cyberthreats. SM sites that adopt an employee increase dramatically, and so does the risk of misfortune. Since SM or SNS are used by many of them every day, cybercriminals have become an essential system to hack related personal

information and obtain useful information. Although social media sites may be used in cybercrimes, it is easy for service providers not to stop using SNS because they play an essential role in its propaganda (Sunil et al., 2020). In contrast, SMPs' significant problem is that anyone, like criminals, can discover knowledge through them. It is not possible to verify the actual identity of an individual on SNS. It's rapid to create fake profiles to communicate with businesses, organizations, or some group. It uses a false encrypted profile with such a fake e-mail account that it cannot be tracked back. Commonly, when obtaining information, the person appears as a former employee of the organization or sends a message from a friend to all relevant friends of the target customer. Later, with the support of shared friends lists, he will represent himself as a true friend of the community and quickly add another individual or group to the list of friends (Kunwar and Sharma, 2016).

Baazeem and Qaffas (2020) declared that cybercriminals use social engineering methods to access information using social media and distributing phishing apps and malware. Almarabeh and Sulieman (2019), in their studies, focus attention on that as a consequence of this exponential rise in the use of SM websites, risks including computer viruses, malicious software, and spyware have risen, targeting information security and confidentiality. Also, there two kinds of SM and internet threats, classified as modern and classic threats. Figure 2.6 shows the modern threats and types of data expected to be attacked.

Surveillance	Social, e-commerce, Environment, and political governance
User Profile	Actives and behavioral characteristic
Inference Attacks	Prediction Sensitive, political, religious, and educational information
Cyberstalking	Harassment and intimidation
Clickjacking	Press Link or like button, moving cursors, using camera and microphone
Location Privacy	Geotagging
Identity profile cloning	Creating a fake profile
Information Leakage	Health, infrastructure, operational, and intellectual property information
Fake profile Attacks	User information
De-Anonymization	Health service, e-commerce trade, and social media.

Figure 2.6: Modern threats and types of data expected to be attacked (Almarabeh and Sulieman, 2019)

In comparison, the civilian mistrust of data privacy for both government and SM companies regarding information security. Latest privacy and security attacks have also raised fears (Zamir, 2020). As a result, providing an excellent communication platform in SM during countless applications, including informal channels, online forums, blogs, video streaming, etc., unluckily, SM can allow vulnerabilities and threats that could lead to cyber-security hazards for organizations, and cyber community. Therefore, it is essential to manage data security and integrity in SM (Khidzir et al., 2018). In other instances, cybersecurity reflects on the social meaning and strategy of cyber technologies and social security. Public cybersecurity analysis is not based on protecting individual confidentiality but on how communities are exploited and formed (Carley et al., 2018).

Notwithstanding having certain essential principles, SM interaction does not translate without friction into cyber abilities. Every environment meets different problems and demands a variety of instruments and facilities. Even state actors or non-state SM courage is not a good predictor of their technological competence or cyber capacity. Indeed, in many instances, the use of social media and its bi-directional nature will potentially make

the target extra vulnerable (Herrick, 2016). Instead, they require options informing them of danger to fix it before any real damage is done. However, companies should recognize this and support the usefulness of assessing the details, especially in social conversations and providing optimum protection services if individuals want to direct clear of risk. One has to deal with SM sites using particular policies and the appropriate modern technologies (Sunil et al., 2020). Therefore, organizations need to ensure they are just as quick to recognize risks, increasingly react, and steer clear of any kind of rupture (Kalakuntla et al., 2019).

2.1.8. Cybersecurity risk managing techniques in social media

There is various use of social media from maintaining close ties to creating new friendships, organizing events, to exchanging ideas via rich media content such as images, videos, and network interactions, all of these can be completed in unique hyper-connected communication. Whereas the world is closer, the resulting costs are also higher (Zamir, 2020). Consequently, the human factor study reports indicated a significant rise over the year in the number of social engineering attacks that target human vulnerabilities. This increases the need to find a solution that allows consumers to accomplish appropriate protective actions in their social media networks (Albladi and Weir, 2020). To mitigate the cybersecurity risk and attacks, individuals should follow the following techniques in social media through their use.

2.1.8.1. Browser updates

It is best to ignore social media log-in invites from unknown party connections to avoid ransomware attacks and personal data loss by clicking on links. Bookmarks and accessing SM pages by browser access are wiser. Viruses sometimes influence browsers, and the failure of stored personal data becomes apparent. So, keeping private information on social media account browsers is not safe. It’s indeed extremely dangerous when accessing the accounts and profiles on public networked computers. For different factors, public WiFi links to unsafe networks are hazardous for the use of social media. Hackers can quickly enter these untrusted networks and control all online activities (Zamir, 2020).

2.1.8.2. Passwords

People play an essential role in their digital defense. The missing link in many personal information abuse cases can be connected back to a very poor password, an old mobile application with no safety patches, or using foreign WiFi networks. Cybersecurity professionals typically suggest multiple steps to help users limit their vulnerability to the theft of information. Including a separate, complicated password for the specific account, not password sharing, utilizing some form of mobile security feature, and continuously upgrading the smartphone applications and the OS to secure that they have the newest safety updates (Olmstead and Smith, 2017).

Also, robust passwords are very useful for protecting SM accounts. Security specialists are advised to use the latest and most strong passwords frequently. Using a unique password for all SM platforms is certainly not a good practice never. Content passwords, such as beloved animals and sites posted on social media, are easy to break. String random characters enable passwords stronger in the anxiety of forgetting and losing passwords or fear—however, too advanced password administration applications are increase (Zamir, 2020; Olmstead and Smith 2017). Equivalently, Shillair and Dutton (2016) addressed that a possible security vulnerability is initially determined by user identity authentication. Password and username are also used to confirm the user identity. Passwords with specific sizes or special symbols are also needed. Users are recommended to use secure passwords, multiple passwords on various devices, update their passwords regularly and use two-factor tests where accessible. These four components of verification the identity are the measures that a user will seek to reinforce if they have a safe mindset.

Additionally, Awojobi and Ding (2020) clarified that smartphone passwords are not necessary but suggested. Some smartphone users choose that their phone does not have a password because of the difficulties of opening the device. It must be remembered that passwords in the security community are not well valued because some discuss those policies have to be followed to ensure protected passwords. Methods such as requirements the age of

the password, where cannot use the password only for a specific time, after that the user should change the password; use a complicated password; also, the requirements for reusing passwords are supported reinforce security aspects of individuals smartphone. For years, information technology users were told that it is difficult to remember that people should not write down their passwords but must renew their passwords quite regularly (Szumski, 2018).

2.1.8.3. Security update

Updates of security are essential for SM account security. The correct version of apps is more secure to utilize. Differently, vulnerabilities and errors are faced down to be exploited by hackers. Unknown web requests should be handled with caution without proper detail. SM could be a play area for tricksters to attract users with false content and information. People become simple social engineering targets at the cost of sensitive private data, financial capital, etc. (Zamir, 2020). Also, the critical cybersecurity exercise is ensuring that downloading software updates and activated. There are new risks constantly, which only technological updates can fix. Every component controlled by the software needs frequent updates, which covered applications, operating systems, programs, browsers, and smartphones. Windows also contain regular updates to preserve a user's OS (Shillair and Dutton, 2016).

The company's protection security enterprises are increased. Facebook addresses spear-phishing threats by affording special announcements, expanding disclosure systems, and promote anti-phishing measures between users. Most SM organizations standard dual-factor. Also, for the password, usually, users get a code and link sent to their phone and e-mail to verify an account. A lot of people use third-party apps connected with SM accounts to play games, outputs, etc. It is essential to check third-party applications regularly (Zamir, 2020).

2.1.8.4. Regulations and laws of social media sites

Almarabeh and Sulieman (2019) determined different risks to SM sites throughout the globe and the significant drop in user information secrecy. For the anti-threats that users face on SM sites, the following measures are necessary.

- Determine the required privacy level of the site is because of the status of the degree of user communication and use on SM
- Taking benefit of all updates on the website, which is developed continuously to raise them
- Before accepting or dealing with other users, choose them carefully
- Users must stop the characteristics used in the website periodically and re-run one after the other.
- Read all the new features carefully when updating software and SM sites.

Furthermore, Newberry (2020), in her study, distributed some security tips for SM users as follows, creating an SM policy.

- Training employees on the security of the means of social communication issues.
- Determine accessibility to increasing SM information security.
- It is establishing a system of support for social participation.
- In charge put someone.
- Establish an early alert system with tools to surveillance social media protection.
- Check out regularly for new SM security problems.

2.1.9. Social media security tools and privacy

Improvements in ICT smartphones, the mobile industry, big data processing, IoT, and artificial intelligence improve the quality of our day-to-day experience. As these systems are advanced and detailed, our private information, often with little knowledge, is captured and commonly exchanged with unknown or known organizations. Privacy issues have recently escalated dramatically due to the advent of a hyper-connected network, emerging technology and widespread events involving personal privacy breaks (Yun et al., 2019). Two different

factors support people's actions to preserve their privacy on the internet, a common concern and technical privacy protection. Public problem is the logical procedure that people use to protect their privacy on the internet. In reverse, technical security uses hardware and software as tools to defend their privacy on the internet (Baazeem and Qaffas, 2020).

SM sites also present various unfamiliar privacy dangers to platform users, especially risk-related user profiles (Isaak and Hanna, 2018). The privacy issue is compounded, especially when the SM platform owner is not aware of users' sensitive information gathered within their platform. People must have the right to delete users' phone apps from their smartphones and erase their presence on thoroughly SM platforms. Privacy and security must be protected through the five stages of the information life cycle. The five phases of the information lifecycle are generation, sharing, usage, storage, and destruction of information. The SM platform holder must create explicit confidentiality and security guidelines and policies for platform developers and users (Awojobi and Ding, 2020). Accordingly, with the massive and explosive increase in the number of social users, current SM services, tools, and platforms are trying to maintain the number of everyday users and content service providers, activity, and vitality by providing customized services, suggested friends, or content, side by side.

In contrast, they are improving the quality of the user experience. Users are becoming more addicted to sharing their single thoughts, feelings, and experiences with a wide range of colleagues and friends using videos, photos, images, etc. Unfortunately, this type of SM ecosystem, which is taken from people and used in the concerns of the people, suffering interception of data, identity theft, spying on privacy, and information copyright violation by disorganized social, organizational forms and unfriendly engagement organizations (Zhang and Gupta, 2018). Consequently, privacy on the internet is one of the significant difficulties for internet users (Baazeem and Qaffas, 2020). And most SM users are unaware of the privacy setting and its importance of their SM; young adults and teenagers are most likely to be indifferent about setting up privacy on social media (Abd Rahman et al., 2017). Therefore,

security and privacy issues have dire consequences for users and online social network help providers. For utilizers, the potential impacts mean unsuitable private information distribution, such as exploitation and leakage of personal details utilizing practical mining, for example, linking information. For online social network services, security and privacy threats interrupt the service's proper functioning and harm service providers' reputations (Kayes and Iamnitchi, 2017).

According to Baazeem and Qaffas (2020), users share their own and other individual data, which leads to privacy violations and trust problems. Service providers' role is to ensure that sound cyber-security policies decrease negative user skills, enhance effectiveness, and gain user trust. Furthermore, Isaak and Hanna (2018) stated any legislation on data protection and privacy should incorporate the following principles, the basic principles of privacy and information security include transparency, public, user disclosure, surveillance, announcement.

Besides, Yun et al. (2019) showed the different context that influences data privacy they distinguished four important contextual forces to investigate as follows: the type of data gathered from people, usage by multiple industries or organizations of information (e.g., finance, healthcare, and marketing), context political, and technological apps. The SM account security level is associated with various data protection tools built on the server by social media developers and other external safety tools that a user should regularly use (Shevchuk and Pastukh, 2019). Moreover, Shevchuk and Pastukh (2019) illustrated two kinds of safety tools: SM developers' protection tools; remote network providers' security tools. The integration of these two tools helps users fully customize account security:

- Authentication with two-factor
- Special account
- Login notice
- Safety check
- Reliable contacts

- Code for identification
- Checker for the password's strength to create a robust password user can use the web service Uniform Resource Locator (URL) https://strongpasswordgenerator.com
- Checker for breaches of a password; users can access the web-service via the URL https://haveibeenpwned.com/Passwords.
- Checker for e-mail breaches; users can access the web-service via the URL https://haveibeenpwned.com/.
- The user must change the password regularly.
- Checkup for site access or external application.

Regardless of how much you are involved in your social media, users can not track them 24 hours a day, but systems can (Newberry, 2020) presented some favorite protection tools for social media as follows:

Management permissions: Through SM administration platforms such as the Hootsuite, the team memberships never require understanding information for login for any SM account.

Social surveillance flows: Monitoring of social allows you to stay on top of threats.

ZeroFOX: When combining ZeroFOX with the Hootsuite information board, it will inform the user to:

- Offensive or threatening, dangerous material targeting users' brands.
- Spreading malicious links on users' social accounts
- Tricks targeting peoples' customers and business
- Fake accounts that represent the users' brand
- Also, it helps to protect against phishing and hacking attacks

SafeGuard for Social: Social protection screens all outgoing and incoming social messages against the SM policies before sharing. This will help defend users' organizations and employees from SM risks.

BrandFort: Is an artificial intelligence application based on content control and can help users protect their SM account from junk mail.

2.2. Related Research

The interest in cybersecurity has been increased in social media, and many researchers have been studied and published various articles while focusing on specific subsections within cybersecurity. For example, Bhatnagar and Pry (2020) conducted a survey and distributed it to 107 students about students' perception of cybersecurity and personal privacy in social media utilization. He found that most SM participants have a misshaping view of the individual risk of working with SM; the study investigates this creates a compulsory reason for getting a more extensive knowledge of students' perspectives, consciousness, and attention of cybersecurity and personal confidentiality while using SMPs.

Jabee and Alam (2016) paper focused on the problems and difficulties individuals faced when using SMPs. The aim was to evaluate and identify vulnerabilities in privacy settings and assess the associated risks with identity and confidentiality breaches. The study concluded and found that SM users must be aware of their privacy outcomes; the Facebook platform should also move forward with their protection setting's sack to save Facebook users from different cyberattacks and privacy breaches.

A questionnaire survey has been performed by Baazeem and Qaffas (2020) and distributed to 509 members on user religiosity and cybersecurity in the social media context then how the human religious belief impacts user confidentiality which in reality, has an impact on cyber-security in an overall look at the privacy of the online knowledge community and its relationship to the five structures, behaviour, technical, social network, companies, and religion that influence the cyber-security. The result demonstrates that religious belief indirectly affects SM's use through privacy concerns; the further religious an individual is, the fewer details she/he may reveal through SM that will impact cyber-security. Consequently, Decision-makers and SM platforms should consider faith as one of the critical reasons affecting SM's use by consumers and completely share their private information. Modifying the terms of use and usage to resolve the customer's faith's privacy issues will be a possible solution to today's problem.

Mathur (2019) established a study trying to develop social media shopping efficiency as a Protection from expected cyber-security threats. The research shows that improving SM shopping capacity enables a retailer to indicate its capacity to address purchasers' concerns, convey their credibility, and effectively respond. Besides, marketing on social media abilities allows companies to decrease the disadvantageous influence of cyber-security risk in declining firm value and reputation. Moreover, an SLR on threat modelling done by Xiong and Lagerström (2019) researchers reviewed with 176 publications, and 54 articles were chosen for more advanced analysis, and describe factors from the findings that the most significant quantity threat modelling work continues to be performed manually, with little guarantee of validity.

Cybersecurity concerns for Co-Created value have been demonstrated by Hu et al. (2020) that suggests a model that examines the perception/belief variables and the collaborative mechanism that pushes people to reconcile and exchange their information security issues for co-created trust through social media. The study's concluded and recommended dimensions information security and privacy on perceived cyber-security, sharing information, social network and fun on observed co-create values are significant. And the importance and weight of privacy are higher than that of information security in determining the nature and characteristics of users' cybersecurity concerns. The study also found that individuals' cybersecurity issues have a substantial and negative influence on behaviours, while co-created weight views have a considerable and optimistic impact on behaviours.

Van der Schyff and Flowerday (2019) presented a study on social media surveillance the study introduced a model that is improved to determine personality and awareness on users' decision to utilize third-party Facebook applications. The study result shows that individuals' personality would likely impact their intention of using the Facebook application and that awareness of social media surveillance would affect a customers' decision to use the Facebook application.

Besides, Sunil et al. (2020) disseminate a study that designed a prototype model for forecasting user vulnerability depending on various user characteristics viewpoints. The suggested framework involves relationships between different social network-based variables, such as network engagement levels, the motive to use the internet, and the ability to deal with attacks on the web. The record shows the different kinds of cyber-security and the social media role. The Sustainable ecosystem of cybersecurity presented by Sadik et al. (2020) concentrates on cybersecurity for smart networks and recent technologies, including the Internet of Things (IoT), while using blockchain.

When thinking about patients and health, the most critical concerns were patients' information privacy and security. Therefore, Al-Muhtadi et al. (2019) disseminated a study with mobile healthcare applications and cybersecurity in a multi-cloud ecosystem. To discuss the diverse nature and visible threats, a health care system that, combined with SM and infrastructure, offers a feasible alternative for maintaining privacy and data protection. The design was based on a multi-cloud ecosystem that guarantees data availability and supports to be concerned with trading with the unpredictable nature of the patient's urgent medical needs is necessary.

A systematic literature review has been implemented by Offner et al. (2020), which presents essential information about cybersecurity in the Australian healthcare organization. The study compares the cybersecurity aspects of foreign and Australian health services regarding universal electronic medical records. It discusses emerging developments in health cyber-security breaches that could threaten critical care if patients' protection and privacy are violated.

Moreover, many previous studies published and contributed to various fields on cybersecurity and analysis data in different techniques (e.g., The importance of cyber-security in school (Rahman et al., 2020), social engineering attacks in social networks (Albladi and Weir, 2018), cybersecurity risk factors in digital social media (Khidzir et al., 2016), cyber-security data rights and Privacy (Michael et al., 2019), Cyber Attack Detection

using social media (Khandpur et al., 2017), cybersecurity challenges and the way forward in social media (Thakur et al., 2019).

From the review of related research, it appears that several studies that have been conducted were focused on the privacy and protection of individual's data in social communication sites; also, some researchers were paying attention to awareness and knowledge about cybersecurity as it is the leakest point in media platforms. Additionally, some other studies investigated the perception and individuals' viewpoint about information security and how data are surveillance on social sites. Accordingly, vulnerabilities and cybersecurity risks have been discussed while users using social platforms as they are vulnerable to lose their personal information. Moreover, some of the articles were interested and focused on the security and protection of patient’s information in the healthcare sector. As this study couldn't find any systematic review about cybersecurity in social media, the main goal of this study would be to provide an understanding of cybersecurity in social media.

CHAPTER 3

METHODOLOGY

This chapter presents the research method, describe search strategy, selection criteria, quality assessment, data extraction, descriptive analysis, and data synthesis.

3.1. Research Method

The research method of this study is the systematic literature review. In today's knowledge culture, most scholarly papers are accessible in journals online and database libraries. Systematic literature reviews aim to assess, synthesize, and select high-quality original research related to a particular topic to offer further accurate and updated frequent results (Huang, Chen, and Liu, 2020). A systematic review is a detailed data review and synthesis procedure focusing on a subject or similar core issue and drawing together what is learned from the academic literature by transparent and accountable processes. Furthermore, it entails analyzing and assessing all existing data relating to a specific research subject, topic field, or phenomena of interest by employing a reliable, systematic, and highly secure technique (García Holgado et al., 2020).

The following process was carried out for the current systematic literature reviews; preparing the study involves developing research questions and protocol review—carrying out the analysis, which consists of the research review, quality and selecting of the studies, extracting data, and synthesizing data. This review was undertaken in coordination with the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA). The PRISMA guideline is intended to enhance the documentation of comprehensive reports focused on related research; PRISMA seems to be the most frequently utilized systematic review evaluation guideline, assisting authors in improving review and meta-analysis documentation (Wang et al., 2019).

3.2. Search Strategy

The systematic review research, conducted in December 2020, devised a search strategy to identify appropriate literature for this SLR search. To carry this SLR, the study searched for published scientific articles. The search strategy was tailored and implemented through the four databases in the research field: Web of Science, IEEE Xplore Digital Library, Scopus, and Science Direct. The study used the metadata fields, title, abstract, and full text. The search string term is (("Cybersecurity" OR "Cyber Security" OR "network security" OR "cyber safety") AND ("Social Media" OR "Social Website" OR "Social Network" OR “Social Networking Site” OR "internet community")). The study focuses on primary articles and studies published from 1 January 2015 until 31 December 2020, and the articles written in English.

3.3. Selection Criteria

The study searched for the related articles in the selected databases. The selection criteria were carried out in two phases; in the first phase, the papers were filtered according to the period of publication, language, document type, and the article should be open access. In this stage, without applying any filtration criteria, the search gets 4549 papers from Science Direct, 779 from IEEE, 424 published scientific papers from Web of Science, and 230 from Scopus overall 5979. Articles, conference papers, workshops, book chapters, seminars, and newspapers were included in the initial literature search. Following that, applying the first selection criteria as it was study duration (2015-2020), the overall numbers of documents reduced to 4089. Afterward, from the second inclusion criteria, just articles included, the number of papers limited to 2388.

The study included only articles published in English. Through this criterion, six records were excluded, as it was not in the English language; 3 from the Web of Science and the rest from Scopus; the number of documents declined to 2798. Also, through applying the last selection criterion in the first phase of the study search, where reports were to be accessed open articles, the total number of articles became 394. For the second phase of selection

criteria, the study flowed by the PRISMA statements within the selection criteria. Any related full-text literature review on cybersecurity within social media for instructional practice was interested in the inclusion criteria. The reviewer determines whether or not to include any of the publications in the systematic literature review by applying inclusion and exclusion criteria; first reviewing the title and abstract, 246 articles were excluded at this stage. Particularly, 133 studies were evaluated for full-text eligibility; 58 papers excluded for the following reasons Conference paper and workshop (n=19), irrelevant to social media (n=7), cloud computing (n=3), big data, and data science (n=3), industrial 4.0 (n=7), irrelevant cybersecurity (n=11), social networking for automation and vehicle (n=3), IoT (n=3), blockchain (n=2), and studies include in Qualitative (n=75).

Despite this, certain full-text papers were relevant to the study based on the search topic. Still, during data extraction, 25 articles were excluded because two articles were published in 2014. Another one was 2021, one book chapter, and 21 articles were excluded as they were not answering the research question. As a result, 50 articles met the inclusion criterion. A PRISMA flow diagram was used to outline the preceding systematic literature review process Figure 3.1

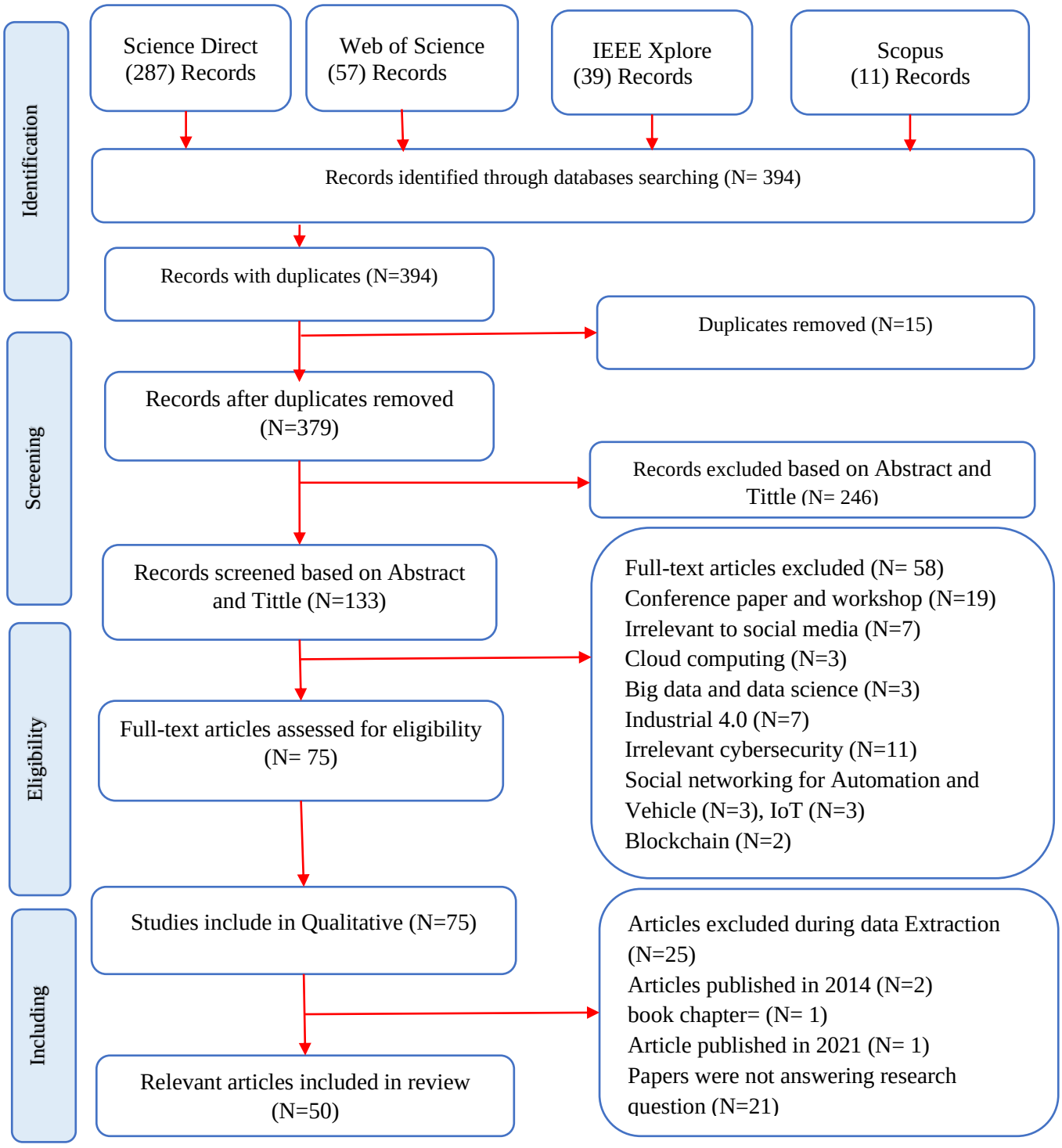


Figure 3.1: PRISMA flow diagram for Systematic Literature Review

For the SLR method, it is essential to select records from databases; the study used different criteria for evaluating and choosing papers. The core items of the study's inclusion and exclusion criteria are listed in Table 3.1, as the selected articles should meet the documented standards to include in the survey.

Table 3.1: The study's inclusion and exclusion criterion

Criteria for Inclusion	Criteria for Exclusion
• Articles distributed from 2015 to 2020 • Articles mostly related to social media and cybersecurity • English-language distributed articles • Articles in full text are freely available to download. • Articles must be open access. • Only articles from the high impact factor carried in scientific journals were included.	• All papers before 2015 excluded • Articles irrelevant to the research question and duplicated articles • Non-English articles • The articles' full text is not available • Abstracts and titles that differed from the study's goal • Except for articles, any other type of document has been excluded

3.4. Quality Assessment

The quality assessment was done by reviewing each paper to ensure that such criteria were met so that the research could be regarded as acceptable scientific validity. The quality evaluation assists in the review of research to validate the degree of conformity with predefined criteria. If the paper meets all of the inclusion requirements, it was included in this study; otherwise, it was rejected. Given the topic's importance, study wanted to incorporate as many experiments as possible that met the eligibility criteria and presented original data. Additionally, the study accurately described and evaluated the quality of each article. The thesis relied solely on original review publications. The papers' abstracts were thoroughly reviewed for interpretation and filtration to verify the reliability and validity of scholarly literature used in the assessment process. At a later point, each scientific paper has been carefully analyzed. If the accepted articles answered the research question, the selected papers' information was carefully read and extracted for each question.

3.5. Data Extraction

The final step of the study's PRISMA framework is the data extraction of 50 studies included extracting data and finding the answer for each research question. After identifying all of the articles used in the study, each article's related data was systematically collected and calculated based on the research questions. From each article, the study selected data regarding the study's objective, publication date, critical finding, the methodology that have been conducted. In this stage, the study excluded several articles as they did not answer any research question. During extracting information or the answer for each question, an excel sheet has been prepared. The finding collected information from qualifying articles has moved to a prepared excel sheet to analyze the data and illustrate it with graphs and charts for each research question separately. The worksheet was prepared and the extracted data for the question transferred. The data were extracted concerning the research question was the type of cyberattack, factors of vulnerability, way to gain awareness about cybersecurity, and the prevention ways.

3.6. Data Synthesis

Initially, a descriptive analysis of the data from all reviewed studies was reported. The study collected data from 50 systematic review articles tabulating and summarizing the data based on various criteria, such as publishing year, percentage of each database, number of articles according to databases, search study design, author and year, study aim, and critical finding for each survey. In the subsequent phases, each of the criteria is thoroughly examined.

3.6.1. Distribution of articles according to years

This study included articles that have been conducted from 2015 to 2020. Figure 3.2 illustrates the number of articles disseminated during the same period. Moreover, the study found a rise in publications related to the subject throughout that period. Particularly in the Science Direct and Web of Science databases, the study saw an increase in the number of articles published in 2019 and 2020. However, as shown in the column chart, Scopus has not

published any documents related to the subject during the given timeline in the study, compared to the earlier two databases.

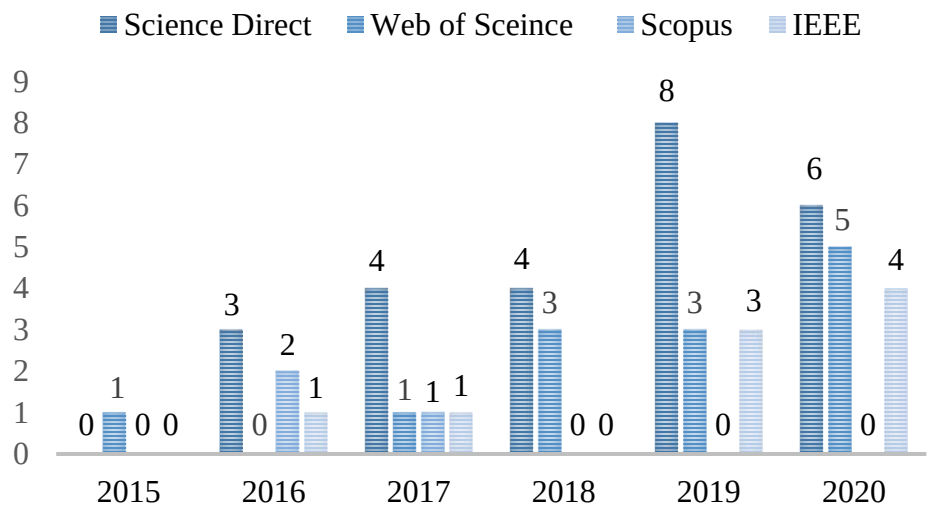


Figure 3.1: Distribution of articles per years

3.6.2. Distribution of articles according to databases

Figure 3.3 presents the majority of papers that related to the subject of the study were presented in science direct (n= 25), web of science (n=13), IEEE explore (n=9), and the final one, Scopus, only offered three articles.

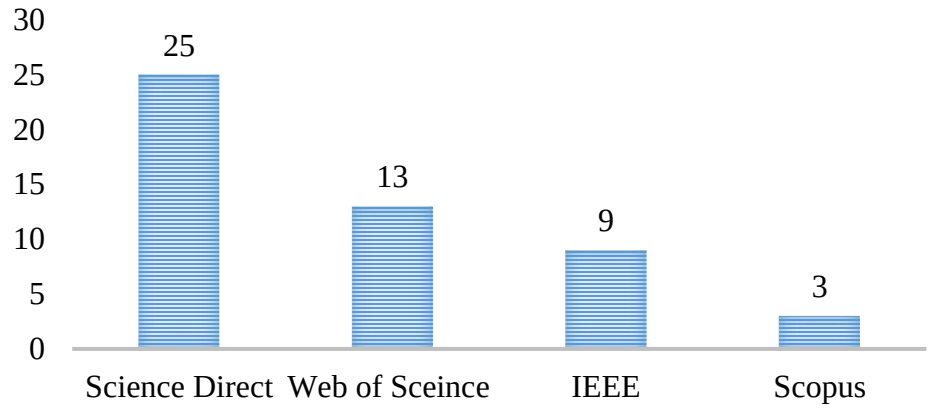


Figure 3.2: Number of articles according to databases

3.6.3. Distribution of articles according to methodology

Figure 3.4 illustrates the study design methodology for the taken articles. Where the study's structure starts to group different methods, and the records were classified as follows: 62% of analyzed studies were experimental research, then 24% of articles investigated were qualitative research, including systematic summary, case study, interview, and review articles; following that 8% were quantitative research which is involving survey, an online questionnaire, and the empirical study. Furthermore, the final one by 6% was mixed-method research.

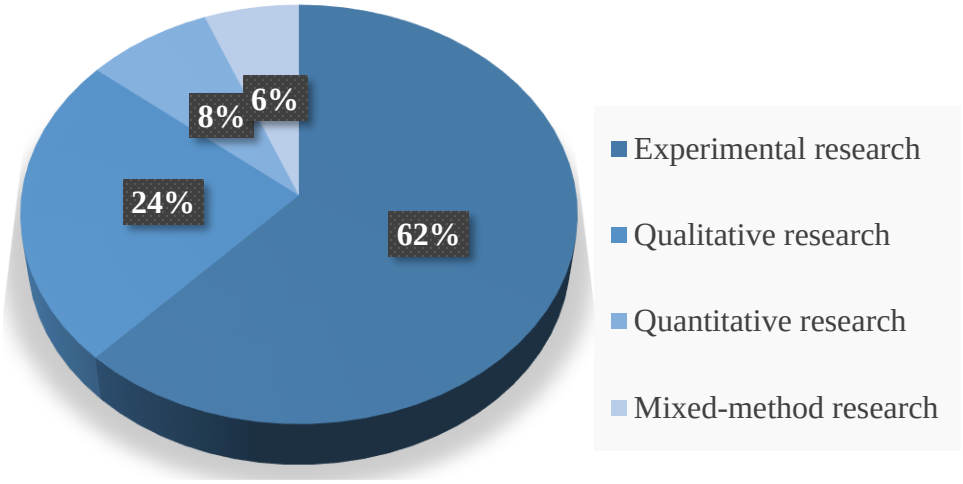


Figure 3.3: Distribution of articles according to methodology

3.6.4. Distribution of articles according to the percentage of databases

Figure 3.5 shows the percent of databases containing the number of papers used in the analysis and data synthesis for the current study. Consequently, the databases that fulfil the research questions' answers were Science Direct as the percentage was (50%). Following that, (26%) records from Web of Science satisfy the answers to research questions. The databases IEEE and Scopus complete the answers to the study objective by 18% and 6%.

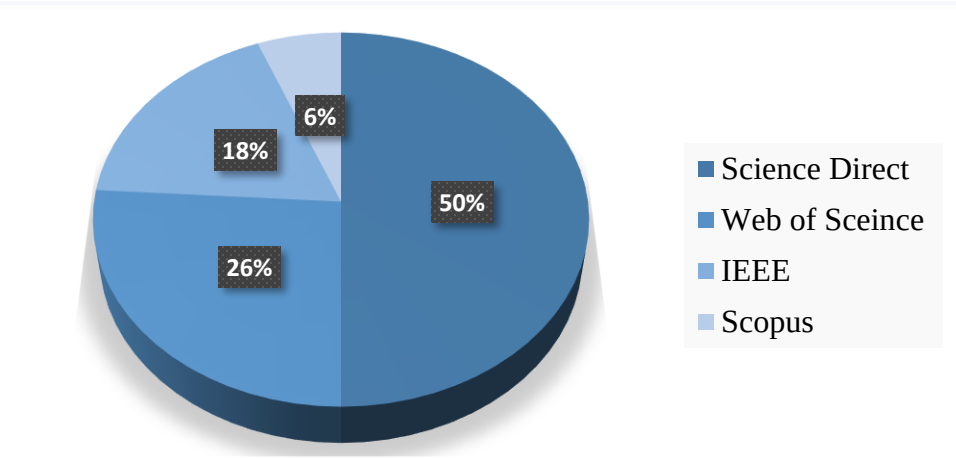


Figure 3.4: Distribution of articles according to the percentage of databases

3.6.5. Analysis of reviewed articles

The analysis comprised 50 research after scanning the complete text of articles. As a result, Science Direct (n=25), Web of Science (n=13), nine studies in IEEE, and only three publications met the study questions' findings in Scopus. According to the thesis research questions, the articles were fully evaluated, classified, and ordered based on a restricted number of documents. Table 3.2 highlights the articles chosen for this study by displaying the reference, purpose of the study, findings, study design methods.

Table 3.1: A summary of Selected articles

Author and Year	Aim of Study	Method	Results
Alzaylaee et al. (2020)	Recommended DL-Droid, a "deep learning" framework for detecting Android apps' malicious using dynamic simulation and stateful information production.	Experimental	According to the report, DL-Droid will achieve up to 97.8 percent detection accuracy (with just dynamic features) and 99.6 percent detection rate (with dynamic and static features), outperforming conventional ML methods. Besides this, the findings illustrate the relevance of improved insert generating for dynamic analysis, as DL-Droid by state-based input production out presents current state-of-the-art methods.
Li et al. (2020)	The study aimed to identify self-reported encounters of corruption involving the health care sector.	Experimental	The research discovered a limited number of utilizers regularly documenting corruption experiences, listed users in countries considered by their people to have high levels of fraud, and found that the bulk of messages contained accounts of users' personal experiences and corruption documentation.
Bruning et al. (2020)	The study aims to describe people's power flaws using the principles of social involvement and network engagement.	Review	The study found that 1) people consider their vulnerability to social impact as a function of their SM participation if this impact poses a danger, and how they would reduce harmful impact vulnerabilities by structured preparation. 2)Although specific individuals constructively handle effect vulnerabilities, organizations and communities should encourage more efficient adaptive reuse of effect vulnerabilities in their constituents and workers. 3)Run public knowledge campaigns; provide training on constructive self-management of impact vulnerabilities.
Palaniappan et al. (2020)	The study presented a mechanism that uses the regression analysis classified algorithm	Experimental	The study found that by using the mechanism that uses the regression analysis classified algorithm to classify malicious domains and

	to classify malicious domains and favourable.		favourable; it looks forward to improving on this classification algorithm and transform it into a multi-classifier to organize the kind of maliciousness for either a given web address, like phishing, spam, defacement, or ransomware.
Cohen et al. (2020)	The study's purpose was to present a MalJPEG as the first ML-based solution explicitly designed to identify unknown malicious JPEG images efficiently.	Experimental	The findings reveal that MalJPEG has the best identification capability when combined with the LightGBM classifier, with a region underneath the curve method of 0.997, a positive predictive value of 0.951, as well as a feeble false-positive rate of 0.004.
Dennehy et al. (2020)	The purpose of the study was to show creativity to the scant observational literature on cyberbullying.	Qualitative	Findings show that the damaging effect of cyberbullying on young people's mental wellbeing emerges as a harmful and long-lasting internal debate fueled by the invisible, ubiquitous, and irreversible existence of cyber experiences. Death was viewed as a viable exit path for youthful offenders who had been defeated and entrapped by online victimization as well as their self-destructive thoughts by stakeholders.
Jenkins et al. (2020)	The study created and present a new deep learning algorithm to creating a simulated spoofing dataset	Experimental	Deep learning-based approaches improved classification precision for spoofing attacks significantly over baseline. They also discovered parallels in the pre-processing stage of biometric characteristics before the application of the methods. The proposed algorithm demonstrated significant advancements in retouching detection.
Tai et al. (2020)	This study aims to bridge the difference among pre- & post-Internet written types and include an in-depth observation of	Experimental	The findings indicate that vocabulary can be used to discern human variations in style and personality. And the integration of input vectors

	written styles strategies in OSN texts through three multidiscipline factors: demographic, behaviour and personality, and cybersecurity.		generated the highest accuracy in various ML and statistical methods for authorship identification, including for simple comments like chat posts.
Kim (2020)	The study aimed to investigate malware delivery networks using social network analysis established on theories of the graph.	Experimental	The research discovered that associated with international metrics are useful in locating center nodes involved in malware delivery. This core intelligence is far and away from the most useful in comprehending malicious web infrastructure characteristics.
Alsariera et al. (2020)	The research suggested four meta-learner frameworks for detecting phishing websites created using an extra-tree dependent classifier.	Experimental	The suggested AI-based meta-learners were configured on phishing site datasets, and their performance was evaluated. The simulations reached a detection performance of at least 97 percent and a false-positive average of not higher than 0.028. Furthermore, the proposed methods outperform current ML-based methods in detecting phishing attacks.
Shin et al. (2020)	Via develops an innovative embedding algorithm; designers suggest a new text classifier for categorizing cybersecurity intelligence positive & negative tweets.	Experimental	The result showed that the proposed method to enhance precision, 0.934 of F1-score and 0.935 of region underneath the curves, increases the baseline models by 1.76∼6.74 percent of F1-score and 1.64∼6.698 percent of the area under the curve.
El Kamel et al. (2020)	The study aimed to create an effective cyberattack ID system and avoidance by using a honeypot to collect ML algorithms.	Experimental	The basic approach built on honeypots and the mixture of ML algorithms creates an extensive simulation and predictive method for suspicious profile identification and classification. As a result, it describes an advanced and effective cyber defense architecture for dealing with future and zero-day attacks.

Aljably et al. (2020)	The study introduced a model to secure patient confidentiality in Online SN and discourage insiders unauthorized from reaching and interfering among the user's info.	Experimental	The proposed model has been successfully tested on actual datasets, including over 95% reliability that used a Bayesian algorithm and 95.53 percent accuracy on the curve method using Deep Learning (DL) models and long selective memory recurrent neural network classifiers. The experimental findings indicate that this significantly achieves other identification methods like assistance vector device, isolated forest, Kolmogorov Smirnov, and component analysis.
Fang et al. (2020)	Offers a multitasking method for combining two activities that identify cyber-attacks through "Named Entity Recognition" (NER) and Twitter for tweets	Experimental	The findings reveal that the multithread model will outperform dual sub-tasks performed separately. This significantly reduces the difficulty of using DL models. Also, the proposed pattern outperforms many baselines in detecting cyber hazard incidents from tweets.
Pangrazio and Cardozo-Gaibisso (2020)	The study presented the comparative research and assert that it is essential for schools to go ahead with the cybersecurity dialogue to support learners in considering and thinking more carefully regarding the SM they utilize.	Comparative	The result shows that many of the challenges that pre-teens are dealing with necessitate more complex and sustainable instructional services that promote vital social media literacies. With the advent of mass consumer artificial intelligence and platforms, schools must train students to use and secure their personal information.
Tschakert and Ngamsuriyaroj (2019)	In a 2 x 2 mixed factorial outline, investigating partner phishing vulnerability to see whether educator classroom instruction, in addition to a different method screen-, game-, and text-based training kit, offers a substantial differential in	Experimental	The findings show that integrating classroom instruction increases phishing resistance only slightly. Moreover, they found that participants have a substantial preference for one training method, i.e., classroom education, only when one method's decisions are needed.

	vulnerability mitigation as opposed to no classroom education.		
Patil et al. (2019)	The research disseminated a proposed collaboration style known as E-Had, which detects DDoS offensives earlier.	Experimental	The findings explicitly show that the proposed identification system detects DDoS offensives' different situations early and distinguishes them from flashing audiences.
Bhathal and Singh (2019)	The aim of this article was, various forms of weaknesses are explored, as well as potential ways to minimize or remove specific vulnerabilities.	Experimental	The outcomes demonstrate the impact of threats on achievement. As per the findings, the need to secure data utilizing a defense-in-depth approach to safety.
Connolly and Wall (2019)	Aims at investigating how organizations and researchers have reacted to the change throughout the ransomware environment from locker and scareware threats to the mostly exclusive utilize of crypto-ransomware	Qualitative	The study's findings indicate that reactions to crypto-ransomware are complicated by the intricate interaction between the technological and human dimensions of an assault.
Tsikerdekis et al. (2019)	The article shows a constructive method for identifying malicious identities at the level of potential entrance into sub-society.	Experimental	The categorization identifies between characteristics and their sophistication, and this is extended so that it can be applied to other social platforms. The syntax could also be used as a preventive tool to determine access granted to consumers in sub-society.
Venter et al. (2019)	The study objective was to investigated mobile cybersecurity awareness among South African college students.	Qualitative	The study result verified the value of cybersecurity training in this regard: a gratifying but challenging discovery the previous because it indicates that the university has been doing an excellent job of raising the interest in cybersecurity education.

Kamal et al. (2019)	The paper introduces a new paradigm that utilizes Twitter information to track Emotion identification and crowd-source signaling.	Experimental	The findings show that in a good climate, individuals develop good feelings in specific Tweets, although, in poor weather, they express negative feelings, as shown in the associated word cloud. The present structure offers a tool for understanding the sentiments expressed in microblogging. It can provide clear and straightforward visibility into public attitudes in various contexts and for multiple purposes.
Javed et al. (2019)	Created ML algorithm utilizing machine behavior data and tweet metadata to go beyond comment detection of these URLs being malicious then predict when a URL would be malicious.	Experimental	The emphasis has been on track, and excellent results have been obtained by observing the Web pages' dynamic or static movement.
Okutan (2019)	The study focused on a technique for Investigating Cybercrime	Review	The study investigated and discussed different types of cyber-crime and presented measures for protection against various attacks.
Wang et al. (2019)	The study aims to Use K-L deviation to describe spam dissemination and a multiscale cross-validation test to identify potential drifts.	Experimental	Extensive studies demonstrate when drift occurs, K-L divergence has strongly stable shift patterns among features. Furthermore, the multiscale drift detection test helps enhance last classification results in precision, memory, and f-measure.
Masood et al. (2019)	The study presented a taxonomy and used techniques to identify and detect Twitter spam and classified them into various forms.	Experimental	This approach's results are helpful for the development of spam detection strategies. It also reveals that the characteristics used in this work pose various problems; for example, some are easily deceived while some are difficult to remove.

Priestman et al. (2019)	Estimates on an independent evaluation aimed at hospital employees and summarizes peer-reviewed research on healthcare and phishing.	Experimental	The experimental study found that 468 worker email accounts were known from publicly available data and targeted via phishing using various payloads such as malicious links and attachments; however, no passwords were retrieved, or malicious materials were downloaded. Even so, numerous hospital staff was found on SM accounts, including those duped into allowing fake friend requests.
Soomro and Hussain (2019)	Explain cybercrime prevention guidelines and approaches	Review	The study shows different types of cyber-crimes and presented techniques and recommendations to prevent each given kind of threat.
Ahmad et al. (2019)	Examine parental awareness and willingness to determine if they are mindful of the effects of internet risks on their children.	Quantitative	According to the results, parental understanding of cyberattacks is at a medium level and needs to be increased to foster cyber protection. Early exposure to the parental knowledge of cyberattacks will help in raising parental awareness of cybersecurity.
Behal et al. (2018)	The article suggests D-FAC, an anomaly-based shared protection mechanism that effectively detects various types of DDoS offensives and efficiently mitigates their effects.	Experimental	D-FAC outperforms current instability and divergence-based DDoS security systems on detection metrics such as detection accuracy, classification average, precision, F-measure, and FPR.
Craig (2018)	The study shapes future order design, online behaviors, and cyber policy, also human aspects would be advanced as an essential part of cybersecurity design.	Review	When cyberspace evolves and changes, so does its susceptibility to an ever-changing and ongoing cyber threat. The importance of cybersecurity research cannot be overstated since it will include the answers that will make the modern world a colourful and secure environment to be.

Tuptuk and Hailes (2018)	Investigate the difficulties by these attempting to protect smart factories networks face.	Literature review	1) The study discussed the protection of current manufacturing and industrial infrastructure, vulnerabilities, possible future cyber-attacks, the shortcomings of interventions, levels of understanding, and strategic planning for future security threats. 2) To provide effective safety mechanisms, the management and commercial sectors must collaborate and concentrate on scalable, stable, secure, low-cost security solutions that can meet today's and tomorrow's production systems' implementation and runtime needs.
Van der Walt et al. (2018)	The study estimates ML algorithm utilizing characteristics contained on SMPs like the "profile picture" to identifying the bot accounts.	Experimental	The findings of studies into identifying non-human likewise recognized as bots accounts are also used to build on the initial results. And the effects of ML are extended to a developed framework for intelligent identification and analysis of identity fraud on SMPs.
Alguliyev et al. (2018)	The importance of social media and safety in e-government is investigated.	Experimental	The fuzzy approach determines the parameters for categorizing potential risks. The statistical experiment suggests that members of social networks will be subjected to a series of disruptive attacks. The challenges are analyzed and ranked using the recommended approach based on factors such as surveillance of sensitive information, credibility loss in government-citizen ties, and organization of social-political disputes.
Williams et al. (2018)	Investigate the vulnerability of workers to directed phishing emails, also recognized as spear phishing	Mixed-method	According to the findings, the inclusion of authority signals raised the risk that a person will click on a suspect connection in an email.
Martin et al. (2018)	Investigating cyberbullying between middle schoolers	Survey	According to the findings, 17% began using social media at the age of nine or younger, 40% welcomed connection request from individuals did

			not meet, and 40% indicated that their family did not control their SM use, highlighting the importance of cyber-security education. According to the report, students who used SM more increased than ten times a day, especially girls using it more than boys significantly.
Moreno-Fernández et al. (2017)	Since it is always tricky for phishers to use precisely the same fonts as in the initial web page, the research focuses on typography and the impact of simple learning on human results.	Experimental	The findings indicated that while undergraduate classmates were already trained with simpler iterations of the diversity challenge, they were more sensitive to discrepancies than when educated with the more complex target diversity from the outset "easy-to hard effect."
Edwards et al. (2017)	It aims to show possible threats to the target and show that crucial knowledge relevant to Social Engineering (SE) threats on organizations can be actively harvested on a wide scale during an automated manner and automatically analyzing online SE attacks surface.	Experimental	Studies demonstrate that it is possible to instantly classify an organization's employees among individuals in its online footprint. They show that it is possible to immediately and accurately address employee identity through various online platforms for large-scale mining of information relevant to conducting SE attacks.
Ki-Aries and Faily (2017)	The paper describes a method for defining security-related human factors by integrating personas into the design and application of information protection awareness.	case-study	A person-centered approach to cybersecurity awareness can respond to the resources and time taken for its execution within the enterprise while also making a meaningful contribution to minimizing or minimizing Cybersecurity threats via security knowledge.
Hughes et al. 2017	Investigate how well the balance of and benefits can change at the worldwide,	observation	The think about found that, whereas yearly costs relevant to cyberattacks and cybersecurity investing do not come to override the yearly

	country-level, and country-grouping until 2030		incremental financial advantages of ICT utilize in high-income nations, over time, the compounding universe of the profits versus the more added substance nature of the charges implies that the total benefits will surpass the total costs by $10 trillion over indeed medium-term figure skylines. Both annual and average analyses for low- and middle-income countries indicate that gains will appear to offset expenses. Globally, the combined net benefits could top 100 trillion dollars by 2030.
Zhou et al. (2017)	paper presented ProGuard, a novel method for proactively discovering malicious profiles before online marketing activities.	Experimental	Experiment findings show that the device will achieve a high detection accuracy of 96.67 percent while having a relatively low false-positive rate of 0.3 percent.
Buglass et al. (2017)	The study's objective was to conduct an online survey to investigate the online vulnerability and behaviours of UK social media users.	Survey	There was an essential direct impact among online vulnerabilities and self-esteem, suggesting that increased sensitivity to online exposures was correlated with lower self-esteem.
Li et al. (2017)	Explore how ML detection techniques could be used to differentiate between legitimate and fake posts for a consumer on an SM site using the platform's available information	Experimental	Empirical results showed that when determining whether a person established a text, a quality score of 79.6 percent was obtained.
Arora (2016)	The paper provides a brief description of cybercrime groups.	Review	The study shows that the offences are classified as crimes against people, infrastructure, governments, and institutions. Different Internet crime schemes have been tested, and offenders' behaviour in committing cybercrimes has been examined.

Ilie-Zudor et al. (2016)	The paper included a systematic review of seemingly contradictory priorities for process openness against protection threat reduction in production networks, thus discussing widespread security risks, limitations, and countermeasures.	systematic summary	The study found: 1) It is realistic to expect those strategies and technology in developing networks and engaging firms will continue to be influenced by technological and economical, and existing values, with certain shortcomings remaining. As a result, identifying and preventing unexpected threats and creating robust strategies at different organizational levels remain essential. 2) Modeling knowledge exchange and assault phenomenon is the focus of many studies. These inquiries are likely to gain significance because they lead to a clear understanding of the fundamental issues, both in the sense of the identified production level process and in an interconnected view of broader organizations. They allow the creation of research and decision support tools. 3) With knowledge exchange and businesses regularly crossing both organizational and technical borders, a comprehensive approach to dynamically controlling the end of the protection cycle while having the essential capacity to adjust business and development processes to continually changing trust boundaries within and across organizations is needed.
Zhang et al. (2016)	Create and compare rule-based and learning-based approaches for inferring triggering relationships from data transmitted. also present a user-intention-based protection policy for detecting covert malware	Experimental study	The findings reveal that the dependency study effectively detects different malware behaviors on hosts, such as spyware, exfiltrating data malware, and DNS bots. The learning-based approach outperforms the rule-based method in classification accuracy and scalability for massive datasets.

	behaviors using a triggering connection graph.		
Chen et al. (2016)	Address the "Spam Drift" issue in predictive features focused on Twitter spam identification by using a proposed method called "Learning from unlabelled" (Lfun).	Experimental study	Experiment findings show that by using learning from unlabelled strategy, both detection performance and F-measure increase significantly.
Silic and Back (2016)	carried out a field investigation in a "Fortune 500" business investment services to learn how an attacker can use SE tactics to participate in an SNS private community and then collect data through company workers.	Mixed-method	The study found that 1) Workers are quickly tricked and vulnerable to victimization throughout social media platforms where relational elements serve as social stimuli for attackers. 2) Institutions do not have the systems in place to monitor online social media security risks. 3) Companies must reinforce their SNS-related information management practices, specifically by tighter employee identity and identity verification. 4) SMPs have been critical protection vulnerabilities from which cyber threats can be effectively carried out using social engineering techniques.
Buglass et al. (2016)	The paper explores how utilizing the SNS raises the risk of psychological, reputational, and physical weakness online.	Mixed-method	The finding showed a favorable relationship between the Facebook size of the network and online vulnerabilities, which was influenced by network structural characteristics and social variety. Web classification, as well as the range of individual connections, in particular, is indicative of vulnerabilities.

Abulaish and Bhat (2015)	Presented a significant category and specification of different structure-based features and evaluated the achievement of boosting and bagging community teaching techniques for spammer identification in SM.	Experimental study	The results show that the packing group learning method utilizing the decision tree (J48) core classifier functions better than its single model and more valuable than the other group learning strategies for detecting spammers applying community and topological-based SM features.

CHAPTER 4

RESULTS AND DISCUSSION

This chapter introduces the research findings and provides an explanation and discussion of the study's findings.

4.1. Results

After applying selection criteria, 50 reviewed articles were included in this study. Likewise, in the synthesis of the data section, the selected articles were analyzed using various techniques. In this section, the study will address the answer to the study research questions based on the analysis of articles.

4.1.1. The cyber-attacks for social media

Social media sites are indeed ubiquitous, and their user's number is increasing quickly. SM platforms like Facebook, Twitter, and Flickr, enable billions of utilizers to exchange personal information and multimedia content with family, friends, and other internet users (Soomro and Hussain, 2019; Alguliyev et al. 2018). There are several vulnerability risks in the SM that endanger users' distributed data. Unauthorized utilization of personal data for marketing purposes, collection of possible friends, or collection of the material may be of interest among the most visible relatively innocuous choices in the SM sense (Alguliyev et al., 2018).

Malicious users and multiple companies misuse customer data to increase their income. There are several security attacks in the SM that abuse users' distributed information. Unauthorized usage of private information for marketing purposes, collection of possible friends, or collection of material that may be of concern is one of the most visible, relatively innocuous choices in the SM environment (Alguliyev et al., 2018). Cyberattack is a general concept that encompasses a wide range of illegal communications practices conducted through using a computer. A cyberattack is described as committing a criminal act by utilizing cyberspace as a medium of communication. Cyber threats have increased due to increasing globalization, the low price of smartphones, and the quick accessibility of the

internet (Arora, 2016). Nowadays, cyber-attacks have posed a significant threat to information security. The attack intends to infiltrate the entire internet infrastructure to collect sensitive information or to manipulate web resources. There are two kinds of such attacks: aggressive and passive. Active threats are quickly identified, while passive threats are disguised and difficult to detect (Soomro and Hussain, 2019). Consequently, users post a vast amount of unique information on SMPs, making them a priority for various internet attacks. Posted online multimedia material may also contain information transferred by a virus, which starts circulating on the SM site and even beyond its borders almost directly after posting (Alguliyev et al., 2018).

Cyberattacks often include malicious practices and malicious attacks that can capture sensitive data, hacking or surveillance that causes significant harm to the victims, spam, ransomware, identity theft, and social bots (Alguliyev et al., 2018; Cohen et al., 2020). In current years the cyber-attacks targeting businesses, individuals, and organizations are constantly under assault from criminals trying to hack their operating networks by manipulating the behaviour of human users' (Cohen et al., 2020; Williams et al., 2018). According to Hughes et al. (2017) the cyberattacks environment is divided into actors, targets, motivations, and actions.

There is no standard agreed-upon actor and threat categorization in the field of cybersecurity: Hacktivists—groups or individuals whose ideological motivation for carrying out cyberattacks. Cybercriminal's individuals or organizations that conduct attacks for financial benefit. Cyberespionage refers to threats with the ultimate goal of stealing intellectual resources from businesses or governments. Cyberwarfare—destructive attacks were undertaken by state or non-state entities with political or military motivations. Similarly, Soomro and Hussain (2019) clarify that as maintained by the National White Collar Crime Centre's white paper "Criminal Use of Social Media," there are six types of cyberattacks utilizing SM such as phishing and social engineering, SM Burglary, malware, cyberstalking, Identity theft, and cyber-casing. Moreover, Alguliyev et al. (2018) illustrated that the threats are categorized into groups (media content attacks, conventional attacks

targeting personal data, social-oriented attacks, and child protection attacks) each of these categories including some types of threats as follows:

Media content attacks covered: multimedia content exposure, discloser of sensitive information, content manipulation, metadata discloser, links discloser and redirection, unauthorized access to messages, video conferences, fake targeting, sharing, and unauthorized use of information and discloser.

Conventional attacks target personal data: including phishing, malware, fake profiles, spam and links, violation of user anonymity, and profile cloning disclosure of relations.

Social-oriented attacks covered: corporates espionage, cyberstalking, impact of social opinion, reputation loss, encouraging social confrontation on racial, ethnic, and religious grounds, destructive protection, forming fake image and reputation, and creating target groups.

Child protection attacks: including cyber grooming, cyberbullying, cyber blackmail, cybercide, malicious content addiction, incite to bad habits, internet addiction, and trust abuse.

Cyberattacks can be started on networks by using links and various techniques to obtain targets; the following are the most common type of cyberattacks:

DoS and DDoS Attack: A denial of service (DoS) attack happens when registered users cannot access services. DoS attacks are carried out by loading the victim with transactions or causing data to crash. The DoS assault deprives legal service users or resource individuals anticipate in each case. DoS attacks can be carried out in two ways: services that flood or crash (Bhathal and Singh, 2019). This attack attempts to prevent legal users from accessing properties including a network, a server computer, or any computing resources like memory, a process, or a file system (Tuptuk and Hailes 2018). While to attack a target, (DDoS) Distributed Denial of Service attacks use many infected computers affected by malware. An attacker assumes control of a large number (possibly thousands) of machines and utilizes them to invoke the functionality of a target machine, such as a website, forcing it to crash due to an excess of request (Okutan, 2019; Behal et al., 2018; Tuptuk and Hailes 2018; Patil et al., 2019).

Phishing: In today's world, phishing is regarded as a rapidly rising problem in cybersecurity, and hence defensive measures for identifying phishing attacks are being created. Phishing is done via websites and e-mail that include malicious material to harvest information from an unaware or inattentive internet user (Alsariera et al., 2020). Phishing is a criminal method that enables both technical deception and social engineering to steal users' personal identification information and try to take possibly valuable information; like passwords, usernames, or medical info, for malicious purposes, through reaching people by e-mail or messaging in which the offensive party supports participants to click on the links to the websites utilizing code for malicious, downloading, or installing malware (Alsariera et al., 2020; Priestman et al., 2019; Silic and Back, 2016; Moreno-Fernández et al., 2017; Alguliyev et al., 2018).

Tschakert and Ngamsuriyaroj (2019) clarified that phishing is a type of social engineering that has been observed since the middle 1990s and continues to be a problem until today. Even though phishers may use a variety of tactics to achieve their objectives, in a standard case, they act as a trustworthy individual, for example, trustworthy businesses, friends, or even government authorities, and use e-mails as bait to direct Web users to fake websites (Soomro and Hussain, 2019; Moreno-Fernández et al., 2017). Targets were typically found by phishers using publicly accessible sources such as Google searches, Facebook, and LinkedIn (Priestman et al., 2019). Furthermore, the primary targets for phishing attacks were internet payments, online games, internet banking, internet stocks, Web 2.0 innovation utilized pages, and so on (Alsariera et al., 2020; Alguliyev et al., 2018).

Malware: Social media is an excellent medium for the dissemination of viruses and malware. Adware, malware, and virus creators conceal their malicious programs throughout links, messages, and attachments, which seem everyday tasks on any SNS. When users answer them, malware infiltrates their device outside their knowing (Soomro and Hussain, 2019). The malware was described as software that implements a malicious activity on a target computer or network, such as corrupting data or gaining control of a serve (Alzaylaee et al., 2020; Okutan, 2019; Tuptuk and Hailes 2018; Zhang et al., 2016). The most effective method

of launching attacks on production infrastructure is installing malware with insiders deliberate or unintentional assistance. Malware has the potential to adversely affect the availability, honesty, and secrecy of production processes. While the attacks on smart factories have risen, so has the amount of sophisticated malware containing advanced evasion ability that targets industrial processes (Tuptuk and Hailes, 2018). The malware spread networks were made up of malicious websites that use redirection URLs, landing pages, and URLs based on their functions (Kim, 2020).

Furthermore, malware is frequently installed on the infected systems via external devices such as compromised USB drives, watering-hole attacks, and spear-phishing attacks (Tuppuk and Hailes, 2018). Consequently, most malware spreads by exploiting the vulnerabilities in commonly used networked applications, such as a heap overload vulnerability in a browser or its extensions. Once infected, through zero-day activities, network demands from sophisticated malware cannot display specific communication habits. Pattern-based screening is inefficient due to the absence of signatures (Zhang et al., 2016).

Malicious and spam: The more successful online social networks developed, the more engaging they become, like a forum for malicious hackers to execute their threats. The rapidly rising vulnerability of malicious websites is one of the top attacks (Javed et al., 2019; Abulaish and Bhat, 2015). Malicious criminals pose a constant threat to social media sites' stability and regular activity (Tsikerdekis et al., 2019). This malicious website used to create malicious URLs are indeed a famous and essential threat to cyberspace security. They may be used to trick users into being victims as they access the drive-by downloads, phishing, spam, and other material, which can breach the user's privacy, cause financial harm, or results in the installation of malware on the user's computer (Palaniappan et al., 2020). Attackers will also raise their friend count by fake friending profiles. Hackers can also diversify recharging channels, maximize recharging volume, and spend from financial bank accounts (Zhou et al.,2017). While SM spam can cause catastrophic damage to network environments, network security companies and SM sites have committed to detecting spam to ensure user security (Wang et al.,2019). Spammers accomplish their destructive goals

through commercials and various other methods, such as supporting multiple mailing lists and then arbitrarily dispatching spam messages to broadcast their desires (Masood et al., 2019; Abulaish and Bhat, 2015).

Trojans: Identified just after the Trojan Horse of Greek mythology, a Trojan is a form of malware that accesses a target device pretending to be someone else, such as a standard software piece, but then releases malicious code within the host system (Okutan, 2019).

Spoofing: spoofing crimes occur when an attacker's device impersonates a machine object. Due to a lack of sufficient authentication control systems, individuals may masquerade as each other to achieve unauthorized entry (Jenkins et al., 2020; Tuptuk and Hailes, 2018).

Worms: worms represent malicious software that can reproduce themselves on machines or through computer networks even without the user's knowledge; any subsequent copies of these kinds of malicious software can also replicate themselves (Okutan, 2019).

Social Engineering: The most popular strategy used by criminals relying on the human aspect is social engineering. It is defined as the technique of misleading or manipulating people to assist attackers in achieving their objectives, which primarily includes obtaining personal information from SM users to gaining knowledge from them or persuading them to take any action that will profit the offender in any way (Silic and Back, 2016; Edwards et al. 2017; Soomro and Hussain, 2019; Abulaish and Bhat, 2015; Okutan, 2019). People who use SN services get texts from friends asking for emergency financial support. The thief received these notes took their friends' addresses and passwords, not through their associates. Cybercriminals employ various techniques, including social media tricks and strategies, to obtain possible target material (Soomro and Hussain, 2019). Consequenlty, Edwards et al. (2017) clarified that social engineering uses the following vectors as attacks utilized in actual world interaction e-mail, telephone, and physical.

Sniffer: Sniffing is the process of inspecting, recording, decoding, and analyzing the information contained within a network package flowing on a TCP/IP web. The only reason for this is to steal data generally in the shape of passwords, user ids, credit card numbers, network records, and so on (Okutan, 2019).

Identity Theft*:* Academics describe identity theft as an effort to obtain an individual's details to commit a criminal act. Identity theft is defined as the malicious use of a victim's private information without lawful authority and criminal intent (Soomro and Hussain, 2019; Ahmad et al., 2019; Okutan, 2019; Martin et al., 2018). Identity theft happens when a person uses other people's information that has been accidentally leaked or hacked to steal money, gain access to private information, engage in tax, health care fraud, like a person's identity, birthdate, home address, phone number, or any other personal information. They will even open an internet/phone account under your name, organize an illegal operation in your name, and apply for government services in your name. They can accomplish this by breaking into users' passwords, obtaining personal information from SM, or submitting phishing mails (Ahmad et al., 2019; Okutan, 2019; Martin et al., 2018). In addition to using fake identities, certain SM users have been seen using fictitious images known as avatars to describe themselves in the online world. Twitter, Facebook, and other online social networks have established many identity fraud declarations on their SMPs (Tai et al., 2020).

Cyberbullying: Cyberbullying and online violence are described as using social media to convey misleading, humiliating, or aggressive information about others. Cyberbullying occurs when someone intentionally upsets or attacks another person frequently using the internet or smartphone devices (Ahmad et al., 2019; Martin et al.,2018; Okutan, 2019). When children anonymously threaten or embarrass others, spread lies, share hurtful details or photos online, or say derogatory things publicly shame others in society, this is a sign of cyberbullying. As cyberbullying happens, there is an evident abuse of internet or smartphone devices, necessitating parents' and schools' involvement (Martin et al., 2018).

Cross-Site Scripting (XSS): XSS is a widespread threat in which malicious code is injected into a vulnerable network application. It is a disinformation attack in which the attacker injects fake data into the network by transmitting malicious codes over a domain bus (Tuptuk and Hailes 2018; Bhathal and Singh, 2019; Javed et al., 2019).

Cyber-Stalking: Cyber-stalking is described as stalking within cyberspace using SM or other online communications that may cause the victim to feel irritated, abused, or

emotionally anxious. Mobile apps have played a crucial role in advancing this movement for no legal reason (Soomro and Hussain, 2019; Ahmad et al., 2019).

Man-in-the-middle attack (MitM): An attacker establishes a position between the sender and recipient of electronic messages and intercepts them, perhaps changing them in transit. The sender and recipient believe they communicate directly with one another (Okutan, 2019; Tuptuk and Hailes, 2018).

Cyber-Casing: This is described as a method that uses different information available in online databases to generate a real-world position. Geographic tagging is a principal function that SM networks have provided in recent times. Because of the widespread use of smartphone apps (Soomro and Hussain, 2019).

4.1.2. Factors that lead to social media websites vulnerable

The digital revolution evolving in several facets of our lives and being carried out in cyberspace's technology arena exemplifies technology's potential to influence our lives fundamentally. Cyberspace is critical to social and economic well-being because it offers unmatched access and global scope. The reliance on cyberspace is growing. Simultaneously, cyberspace's vulnerability to malicious events increases, and cyberattacks become more adaptive, potent, enduring, and challenging to track and fight (Craig, 2018). Vulnerability is a weakness or defect in system safety protocols, architecture, execution, or internal controls is referred to as a vulnerability. The susceptibility may be mistakenly or deliberately abused, resulting in protection breaches (Bhathal and Singh, 2019).

While it is true that revealing and exchanging private information is required to be accessible on SNSs, criminal acts may be greatly encouraged as a result of information disclosures. Users seem to be unaware of these challenges, and they seem to be unconcerned about the potential consequences and dangers of data distribution. Besides the growth of SNSs, along with a lack of active and well-established safeguards, researchers are seeing a rise in the number of protection accidents involving the misuse of the human element on SNSs (Silic and Back, 2016). Buglass et al. (2016) have argued that the millions of global consumers who frequently communicate with these networks can offer various social and

psychological advantages. Simultaneously, there are possible threats and vulnerabilities in using SNS to engage and collaborate with social relationships. Susceptibility online can suffer psychological, reputational, or physical harm resulting from threats faced in online activities. Threats to personal protection, internet chatter and misinformation, online abuse cases such as cyberstalking, and links to offensive and unwelcome material are also examples of online dangers (Buglass et al., 2017; Buglass et al., 2016). Therefore, SM's popularity poses significant riskiness to their utilizers (Alguliyev et al., 2018).

The weakness factors mean that simply being a member of an OSN does not make a person vulnerable to online exposure; instead, vulnerability is based on how they communicate with the web. Self-disclosure and the proliferation of vast unmanageable internet networks have been identified as contributing factors to online insecurity. It has been proposed that such online self-promotional behaviours are motivated by a user's effort to regulate psychological needs deficiencies related to social influence, social interaction, and belonging resulting from potential social ostracism (Buglass et al., 2017). People are an essential component of successful cybersecurity. Humans are often the cause of cybersecurity vulnerabilities, whether by malicious acts or harmful cybersecurity procedures, regardless of cybersecurity steps. Understanding personality attributes such as cognitive function, enthusiasm, actions, and control is critical for sustaining and strengthening cybersecurity (Craig, 2018).

Similarly, Ilie-Zudor et al. (2016) argued that human behaviour is often the weakest link in withholding sensitive knowledge; it may also be an obstacle to revealing details communicated the behaviour of human communication decisions and in establishing sharing strategies. Furthermore, the causes of vulnerability that people should accept based on their knowledge as different from network engagement vulnerabilities threats faced by a lack of authenticity and integrity of social interaction in a social power sense will most likely reflect a generalized susceptibility to deception. Integration represented an individual's awareness of if the impact effort can be rejected or accepted based on its correlation to their goals (Bruning et al., 2020). Many studies emphasize that awareness and education are the

significant factors of vulnerability and cybersecurity issues which seems to be the users' lack of awareness of protection and security metrics. Users may lack sufficient knowledge of technological tools (Venter et al., 2019; Moreno-Fernández et al., 2017; Williams et al., 2018). Van der Walt et al. (2018) explained that the harmful nature of humans deceiving other humans is one of the most challenging cyber threats to deal with. More particularly, the sheer number of vulnerabilities found in SMPs, the pool of data and diverse types of SMPs, its inadequate architecture besides construction. The vast amounts of unorganized material and the resources that SM platforms offer to humans behaving maliciously all aggravate these cyber risks. All of these aspects combine to make SM websites highly vulnerable to cyber-attacks perpetrated by unauthorized attackers. Weak protection procedures and standards also incorporate vulnerabilities into production processes. Still now, widely established and generally apparent fundamental principles like eliminating irrelevant links and modifying default link configurations and passwords are much less prevalent in the industry than one would logically expect considering the background of attacks. In contrast, mass-production networks are usually built without regard for protection or the explicit assumption that the system is independent and vulnerable to outside threats.

When developing these systems, security requirements engineering practices focusing on mitigating software vulnerabilities, such as the specification of security standards and the implementation of safety properties such as testing, code review, and security patches, have not been widely considered (Tuptuk and Hailes 2018). Additionally, when cyberspace expands and progresses, it becomes more vulnerable, caused by various reasons. The growing number of networks, computers, and users creates permanent security expansion vulnerability. Increasing interrelation and interdependence dramatically raises danger since a breakdown in one device component may have cascading and far-reaching consequences. Growing complexities and outsourcing make complete device visibility and security hard to succeed. Old systems, inadequate computer hygiene, limited control of the electronic infrastructure supply chain, and a scarcity of qualified cybersecurity experts are critical risk factors (Craig, 2018).

Misidentified profiles exist when an SM account owner generates a profile that does not conform to a typical profile's general standards or requirements. Inevitable cyberattacks can target related profiles in specific. Detail each of these vulnerabilities, and show how additional information, such as telephone numbers, can be best obtained when several subject profiles can be connected. Also, the lack of a profile on a specific SM may be a weakness in and of itself (Edwards et al., 2017; Buglass et al., 2016).

Bhathal and Singh (2019) illustrated in their study that vulnerabilities can be grouped into three types: software/technology vulnerability, web interface /configuration vulnerability, and security policy/network vulnerability—also classified as infrastructure reliability, data protection, and information management. They are subdivided into three aspects: design dimension, data life cycle dimension, and data supply chain. Infrastructure includes software and hardware vulnerabilities in the design dimension. Data protection encompasses both data stored and data in transit, as well as the data's life cycle.

Bruning et al. (2020) reported that companies, employees, and other society members need strategies to manage their influence vulnerability since it can have negative implications. The following are some tips for reducing weakness: first, people must become aware of their effect weakness. Second, people consciously consider and maintain their responsibilities. Third, citizens participate in strategic preparation by developing and refining a systemic approach for self-management of effect vulnerabilities.

4.1.3. The vulnerability according to the age of social media users

Social media affects people's cultural, technological, and social lives; it has become an integral part of human life. SM platforms are a portal that allows users to engage in and exchange multimedia material, such as text, audio, video, photographs, graphs, and animations, through the means of a website or an application. There are significant data cloud-based contents presented in terms of length, range, speed, authenticity, flexibility, consistency, exploration, and moralism (Soomro and Hussain, 2019). Therefore, concerns have been raised about the increasing incidence of cyberattacks, which have a wide range of

characteristics. Cybercrime is a general concept that encompasses a wide range of illegal activities carried out with a device's aid. It is describing as committing a criminal act by using the digital world as a communication tool. It has increased as a result of rapid globalization, low-cost smartphones, and fast internet connectivity; cybercrime, such as cyberbullying and cyberdefamation, is a widespread and quickly growing issue (Arora, 2016). These days, the cyber-security media is worried about individuals being subjected to various violence types on SMPs. The harmful nature of humans misleading other individuals is among the most challenging to manage cyber-attacks (Van der Walt et al., 2018). Nevertheless, the government is developing laws and measures to overcome various kinds of attacks. The majority of countries lack the lawful infrastructure to deal with cyberattacks (Arora, 2016).

Online abuse is now well recognized as a common health issue (Dennehy et al., 2020). Many studies emphasize that adult and young people have been among the most vulnerable segments of society impacted by electronic communication's harmful impacts (Dennehy et al., 2020; Martin et al., 2018; Arora, 2016). And this happens because sharing and grouping different risky activities, like sharing the e-mail address and school name, interacting with strangers, initiating online bullying and sex, and determining Internet blocks and filters, can put vulnerable young people at risk (Martin et al., 2018). Likewise, adults don't even have direct familiarity with cyber technologies in their teens (Dennehy et al., 2020).

Additionally, another age group who have a severe attitude to the internet are children with social media access, so without surveillance them by parents, or if parents neglect to track their children's online activity at home, the child would be vulnerable to cyber risks such as addiction, pornography, pedophilia, internet theft, personal information disclosure, and social issues such as cyberbullying (Ahmad et al., 2019). Other studies indicate that children are the victim of electronic criminals for example: Pangrazio and Cardozo-Gaibisso (2020) state that several vulnerable social communities are children aged from 5 to 8 years old. Children are one of society's weakest elements of social technology risks (Arora, 2016).

Furthermore, women are likewise expected to be targets of a variety of cybercrimes. In their research, Venter et al. (2019) discovered that women had more deficient security awareness than men. When it comes to cybersecurity, women had a weaker feeling of self-efficacy. Silic and Back (2016) explained that females were more likely to be victims (54.9 percent), and the younger generation aged from 20 to 30 constitutes the most vulnerable categorization. According to Soomro and Hussain (2019) in the United States, one female out of every 12 and one male out of every 45 will be hunted at some point in their lives. And this reflected on the fact which females between the ages of 18 - 29 are the most common victims of online, but women aren't always their goal. Van der Walt et al. (2018) conducted a study, and they discovered that in South Africa, an alarming rise in cyber-attacks against women had been identified. Venter et al. (2019) reported that women have slightly lower rates of protection self-efficacy than men.

4.1.4. Ways of gaining cybersecurity awareness for social media users

The use of ICT is now strongly intertwined with to use of the internet. As a result, anyone who uses the internet, regardless of age, should be aware of how to protect their computers, and being prepared for the consequences is forearmed. Protection and safety are semantically differentiated terms that necessarily require distinct sets of skills and ability groups. App users of all ages should be aware that their devices are susceptible to attack and should also be mindful of increasing system protection. Since education is at the core of security knowledge and capability, cybersecurity awareness must reach all society segments and people of all ages (Venter et al., 2019).

Cybersecurity awareness consists of two components: first, people must be aware of the need to take the necessary precautions, and then instructors must impart the essential skills to take the wanted precautions (Venter et al., 2019). Ki-Aries and Faily (2017) explained that an engaged safety culture is built on four pillars: responsibility, confidence, collaboration, and cooperation. It is essential to use an approach that motivates and encourages workers to participate in protection to achieve understanding and constructive behaviour. The output of awareness must be adjusted to the organizational sense of workers,

meeting individual security requirements on a continuing process to strengthen awareness and integrate security activities into a security-minded society's daily routine. Essential life skills in data protection can be learned in primary school and provided to all students, meaning that knowledge is increased in all genders equally. The awareness of cybersecurity and flexibility is critical to be left to chance by any administration (Venter et al., 2019). Several earlier studies discuss and present different ways of raising cybersecurity awareness and protect themselves from cyberattacks. Simulated phishing experiments are one method by which organizations aim to raise awareness of spear-phishing e-mails within their employees. This entails sending out simulated, targeted phishing e-mails to various workers and tracking the resulting click-rate, specifically, the number of workers who click on phishing e-mails inside e-mails (Williams et al., 2018).

Besides that, Silic and Back (2016) indicate that training and education on safety awareness may be very useful in defending and protecting against phishing attacks. Similarly, Moreno-Fernández et al. (2017) emphasized that training utilizers to identify malicious websites and protect themselves is a critical component of cybersecurity today. Likewise, Tschakert and Ngamsuriyaroj (2019) clarify that using security awareness and education training to make users less vulnerable to malicious websites shows that education is an effective method. Another approach to gain awareness about cybersecurity in computer science; as Venter et al. (2019) discovered in their study, individuals or students taking computer science-related degrees are different from other people. Therefore, it is evident that computing science training raises awareness of computer privacy and protection concerns and the steps that should be taken; this shows that a computer science curriculum has a strong positive effect.

Ahmad et al. (2019) stated that the effectively managed schools in Singapore introduce "Cyber Wellness Education" it is led by a comprehensive structure known as the cyber wellness framework. It is designed and incorporated based on the needs of student profiles and school environments. The overall objective of "Cyber Wellness Education" is to provide students with lifetime social-emotional competencies and values to be healthy,

tolerant, and responsible consumers of media, connectivity, and technology. The program's introduction is extended at home by including parents as partners in the program. Also, the "National Cyber Security Centre" offers general principles for how companies should defend themselves against cyberattacks, including guidance on protecting internet connectivity, computers, managed access, software patching, and data access (Priestman et al., 2019). Tuptuk and Hailes (2018) addressed that some guidelines and standards provide guidance on personnel knowledge and preparation while emphasizing that protection is human concern as it is a technological one. However, most of this guidance is focused on research conducted on business networks, and through detailed knowledge and training programs, people appear to fall victim to social engineering techniques. And they are often scammed by phishing scams; the following are several guidelines to lead the way to the security

- The "National Institute of Standards and Technology" (NIST) specific publication "NIST SP 800-82", Guidance to "Industrial Control Systems (ICS)", leads the manufacturing control area about how to manage the safety of "Supervisory Control and Data Acquisition (SCADA)" systems, "Distributed Control Systems (DCS)", and other control systems.
- The "Department of Homeland Security (DHS)" offers many publications aimed at improving the safety of industrial systems controls, involving the catalogue of control systems protection: suggestions for standard designers as well as the cybersecurity control system: security in-depth techniques documents.
- The UK's "Centre for the Protection of National Infrastructure (CPNI)" offers a series of best practices recommendations on cyber security evaluations of industrial systems controls and protecting the transition to IP-based SCADA/Programmable Logic Controller (PLC) Networks.

Tschakert and Ngamsuriyaroj (2019) in their experimental study, presented various materials for training cybersecurity awareness as follows: training based on the video, training based on the game, training based on the text, and classroom lead by the educator.

Additionally, Ki-Aries and Faily (2017) presented the following approaches to cybersecurity awareness

- Emerging technologies, strategies, and processes should be regarded and integrated into program updates to ensure their effectiveness and relevance. Optionally, the awareness training cycle defines baseline metrics, determines the appropriate population, target attitudes, elevated threats, and strategies to promote risk-mitigating behavioral improvement.
- Awareness can likewise be viewed as a targeted marketing initiative that introduces cyber-security as a commodity to workers
- Awareness materials and messaging may be sent through various channels and related themes to financial needs and accessible resources; it might include usability, scalability, interaction, and transparency, with the primary goal of continual improvement.
- Interactive communication methods might include puzzles, quizzes, short video recordings, etc., consisting of awards or acknowledgment for suitable activities.
- Face-to-face educational exercises, messages by e-mail, speaker presentations, booklets, guidelines, signs, and awareness practices seminars are other approaches.
- Online resources could also increase awareness of user communications; this could by various web-based resources and keep in existence with suitable update material.

4.1.5. Ways to prevent cyberattacks for social media users

Nowadays, people start to live in the internet community, transforming how people think of their security and privacy. This day's major problem is due to a growth in the scale, pace, range, and authenticity of data in SM platforms, which raises many questions, including security and privacy; on the other side, it can also be used to mitigate and detect crime if treated intelligently and wisely (Soomro and Hussain, 2019). General approaches to risk prevention and reduction should incorporate both technological and interpersonal strategies. Users should be strongly advised to challenge the validity of any e-mail that differs from their regular work; they must closely consider the sender and context. If in question, they

shouldn't open it and request guidance from the corporate security team. Employees should be made aware of the potential threats of harmful e-mail accessories. They should never 'confirm' any information via an e-mail, tap on web links, or unnamed open attachments (Priestman et al., 2019). Users also should be mindful of alternative approaches for confirming the legitimacy of any account connected to, such as different approaches of two-factor verification and using user-selected photos in login pages for legal sites. Corporate IT teams can uninstall features that are not needed in a worker's regular job, like office macros and Windows PowerShell, and implement appropriate firewalls with disabled lists of suspected malicious software pages, as well as spam e-mail detectors that use machine learning methods (Priestman et al., 2019).

Edwards et al. (2017) argued that updated security policy and procedures are critical to promoting a security workplace culture; strategies and best practice guidelines are valuable strategies for accomplishing this goal. Social media access policies may specify what details regarding their workers' jobs they are permitted to share on social media and what security and privacy settings will affect. Security policies across phone calls will hopefully prevent employees from neglect to disclose behaviours. Moreover, attacks can be reduced by implementing an awareness exercise program, and regular security awareness training should be provided to strengthen them (Ahmad et al., 2019; Edwards et al., 2017).

Also, employees' training and awareness is a critical prevention tool against continuing spam detection cybersecurity attacks, and it necessarily requires ongoing implementation and assessment (Priestman et al., 2019). Risk about the malicious software hazard can be minimized by providing individuals with a better knowledge of their future activities' repercussions and how these effects could be minimized at each point (Williams et al., 2018). Priestman et al. (2019) emphasized that highlighting the importance of solid firewalls, cybersecurity systems, IT regulations, and workforce education since some scam e-mails provide links to malicious sites and data, firewalls can be used as one barrier to prevent access to these pages and resources. Similarly, conventional security methods like firewalls, Intrusion Detection Systems (IDS), as well as Intrusion Prevention Systems (IPS)

could defend strategies towards simplistic threats which use the same tools and methods over and over again (El Kamel et al., 2020; Okutan, 2019). Tuptuk and Hailes (2018) suggested defining and enforcing security policy: security planning entails considering the existence of risks, detecting vulnerabilities, evaluating the benefit lost if such vulnerabilities are abused, and appropriately engaging in security. The security management process is usually defined by a policy that reflects both this significant strategic mechanism and the controls that may be placed to prevent the impact of security violations due to specific flaws and the reactions to individual breaches, both in real-time and after the incident. Prevention, authentication, identification, and answer models, making networks rely on restricted security protocols such as shared short default keys, rarely encrypted files, firewalls among various communications infrastructure elements, and the use of isolated area architectures. However, if attackers gain access to sensitive networks or records, there is nothing to prevent them from changing material properties.

Okutan (2019) demonstrated that when it comes to cyberattacks, there are various techniques for detecting and preventing them on SM, which are as follows:

Antivirus: Malicious software detection based on signatures and attitude.
Cryptographic systems: Cryptographic of both collected data and inflowing information on a network.
Network Access Control (NAC): Systems use authentication protocols to access a network or network devices.
Air-gap*:* A mechanism for transferring data securely among two different networks.
Data-Loss-Prevention (DLP): data loss prevention guarantees that sensitive data is kept within specific boundaries. Leakage information from the network or hardware is prevented.
Honeypot: To observe and target the kinds of attacks and develop the required defense mechanisms throughout the framework, especially for devices with vulnerabilities
Electromagnetic security: In the event of attacks to run data, eavesdropping devices are put in network ways, and electromagnetic leak are recorded. Physical access to network pathways is limited in defenses, and touching attacks can be reduced using tap investigative

techniques. To avoid electromagnetic leakage signal mixing or electromagnetic amplifiers may be used.

Digital-Signature: allows the digital signature verification and proof of the sender's identification and material.

Shorthand: Information is not coded but hidden in other information.

System for Filtering Content: Filtering by the web address, file type, specific words, images, applications.

Scanner for Vulnerability: NetProbe, Nmap, Nessus programs must be utilized. Furthermore, Tuptuk and Hailes (2018) recommended defending approaches from attacks: guidelines and standards, regulations, encryption techniques, systems for detecting intrusions into manufacturing or processing systems, human factors and safety skills education, and event prevention and preparation. Additionally, Soomro and Hussain (2019) presented specific suggestions and preventing tips like not sharing location, home address, personal details should not be shared with "friends of friends", limit contact and application permission.

4.2. Discussion

The study provides a systematic data analysis regarding cybersecurity issues in SM from existing literature, as cybersecurity is a very wide field of ICT. The number of social media users is rapidly increased in the communication era, and anyone can use them without regarding users' age. The study indicates that the availability of massive data and easy access to personal information on SMP leads to easy hunting for cybercriminals as they are using SM for their purpose. The study outcomes found several cyberattacks on SM. From the existing literature that the study got, the finding discovered that phishing is the common type of cyberattacks followed by malware, social engineering, then malicious, and spam. While trojans, worms, sniffers, and cyber-casing are minor attacks on media platforms.

Regarding the second research question, based on the data synthesis of the selected articles, it is found that various factors lead social media websites and its users vulnerable to cyber-attacks. From the result, the study realizes that education and awareness are influence individuals, where the lack of users' awareness and training becomes the weakest point for social communication users. Also, many previous studies indicated that both education and awareness are vulnerability factors (Bruning et al., 2020; Williams et al., 2018; Moreno-Fernández et al., 2017; Venter et al., 2019).

Accordingly, the growth of social media sites is demonstrated within the user population growing. Therefore, individuals who use digital technology might be men, women, children, adolescents, etc. Thus, the cybersecurity for communication between people is worried about individuals being subjected to various violence types on SMPs and harmful programs. Consequently, many individuals, despite age and gender, become targets and victims of multiple forms of cyberattacks. Adults do not have sufficient capacity and awareness to express their feelings and do not directly familiar with cyber technologies in their teens. Consequently, they became vulnerable and quickly hunting for cyber attacks. Many surveys have shown that adults and children are among the vulnerable segments of society regarding the harmful effects of electronic media (Martin et al., 2018; Arora, 2016).

Because young people in special own unique features surf the internet because of their character to discover innovative things, they also have a high level of belief and energy that any online data is regarded as trustworthy and genuine. And this happens because sharing and grouping different kinds of activities, like sharing the email address and school name, interacting with strangers, initiating online bullying and sex, determining internet blocks, and filters, can put vulnerable young people at risk (Martin et al., 2018). Moreover, based on the existing literature and the data that have been analyzed shows that women have likewise become victims of different types of cyber threats, as they are more exposed to electronic threats, particularly in exploiting their personal information, due to their deficient security awareness, the weaker feeling of self-efficacy. The study result from the earlier studies indicated that they are the most vulnerable group (Van der Walt et al., 2018; Soomro and Hussain, 2019; Venter et al., 2019; Silic and Back, 2016).

In the current age, where technology covers all areas of life, and people increasingly use social interaction networks for various purposes in their daily lives. They shared their thoughts, opinions, and private information; without knowing the consequences and value of their distributed data on their social platforms. Subsequently, all individuals need to gain sufficient knowledge about cybersecurity in any way. The study's outcomes illustrated some recommended methods to gain awareness about cyber safety. Based on finding security awareness and education training are effective, and using awareness/education training makes SM users less vulnerable to malicious websites. Additionally, as users become aware of cybersecurity, they can use social platforms confidently without fear of cyber threats and anxiety. This finding supports the studies (Tschakert and Ngamsuriyaroj, 2019; Abe and Soltys, 2019; Moreno-Fernández et al., 2017; Silic and Back, 2016).

Nowadays, it is easy to note the high rate of hacking to obtain personal information details. The amount of unauthorized disclosure also has increased dramatically. Online obtaining facts is now much accessible and straightforward than it was decades ago. Social communication users should implement cybersecurity protection and policies in order to prevent access to vulnerable information and data stored in cyberspace from unauthorized

and malicious access. Moreover, increasing the size, speed, range, and accuracy of data in SM platforms poses several concerns, including security and privacy. Hence, media users should realize and know the prevention methods to keep their private data safe. In effect, approaches to prevent cyberattacks, in general, should include both technical and interpersonal tactics.

Regarding research question five, depending on an analysis of relevant articles, the results observed that security awareness and training are indeed very useful in increasing awareness about the safest internet practices and preventing cyberattacks (Ahmad et al., 2019; Edwards et al., 2017; Priestman et al., 2019; Williams et al., 2018). Besides, turning on firewalls is a suitable technique for preventing cyberattacks (El Kamel et al., 2020; Priestman et al., 2019; Tuptuk and Hailes, 2018; Okutan, 2019). From the search results, can note that awareness/ education and firewalls are two effective ways to prevent cyberattacks for social media utilizers.

This study is not free from limitations and defects. Although the systematic literature review aims to use many diverse references relevant to the study, reviewing all publications is time-consuming and challenging. In spite of this, there are several publications in conferences, books, book chapters, workshop sessions, and magazines that may be useful to increase and enrich these findings.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

This chapter presents the overall thesis conclusion as well as recommendations and suggestions for future studies.

5.1. Conclusion

The twenty-first century is indeed the era of globalization. At the beginning of this century, with significant development and growth of social media apps and the internet, the interaction of either side users on SM increases with various online applications. With this development has come several cyberattacks aimed at breaching users' information security and confidentiality. Nowadays, electronic devices, such as smartphones or laptops, tablets, etc., are no longer unique in today's society. Almost every human being on the earth owns an electronic device.

Consequently, with easy access to the internet, it had become potential to connect individuals worldwide through using these electronic devices. Now people can interact, disseminate different data, sharing ideas, and address jobs in real-time. The rise of social media networks, on the other hand, poses significant threats to their users. Because of the rapid increase in the volume of personal information exchanged by social media users, they have become an attractive target of cyber attackers. At the current time, numerous threats on social media are being carried out against the networking infrastructure, and they are seen as a significant threat to consumers. The study aimed to conduct a systematic review and analysis of the literature to provide and understand about cybersecurity issues in social media.

Anyone who uses social media or new technology has at least knowledge of specific trends on the internet and ways to protect and protect personal information from hackers. In our time, the terms piracy and information security have become common, and most social media users have heard about it. Therefore, cyber-security has become a widespread discussion between technology utilizers. While cybersecurity is a broad concept that refers to computer technology, the internet, and information security, it is essential to understand

the field, proper use, and implementation. While many people believe cybersecurity is limited to ensuring network equipment, this is not the case. The history of cyber safety dates back to the 1970s. Additionally, the cyber safety aspects have become significant because of the increasing combination of technology in various fields like banking, entertainment, finance, communications, national defense, government department, and e-commerce. Also, it is affected private and public organizations, individuals, big and small companies, organizations, and significant infrastructure schemes. The study observed several options available to consider the evaluation of the cybersecurity risk; the famous universally identified frameworks were the ISO and IEC, as both of them believed that cybersecurity involves implementing confidentiality, integrity, and availability of information in cyberspace.

Another requirement of cyber safety covered authentication, authorization, authenticity, accountability, privacy, survivability, dependability. The study also concluded that protection forms different types of cyber-attacks and electronic criminals. It is essential for individuals who use the internet to know various kinds of cybersecurity. As a result of familiarity with different types of cybersecurity helps and facilitates the users' social media and internet, how to protect themselves from threats and safe their personal information uploaded, distributed over the net. Types of cybersecurity included: critical infrastructure, cloud, network, internet of things, application, and information security.

Furthermore, the rapid growth and daily advancement of information technology and modern social networks have resulted in revolutionary changes to a wide range of industries, businesses, and facets of society around the world. Social media is an electronic communication form in where individuals build online communities in order to exchange information, private messages, thoughts, as well as other contents. Except for sharing details about their activities, place, status, thoughts, emotions, and so on, they are unaware that their personal information on SM can expose them to cyber-security risks, which can be difficult to mitigate and manage. There are several types of social media available, whether users are looking for new business opportunities or new channels to engage with utilizers. Others are

essential for any industry, whereas others are useful to a younger subset of specialist sectors. The types of social media involve (social network sites like Facebook, Twitter, and LinkedIn, Social Review Sites such as TripAdvisor, Yelp, Zomato, and Glassdoor. Media Sharing Sites examples are Instagram, YouTube, Imgur, Pinterest, Snapchat, and Vimeo. Social Publishing and Blogging Networks like Medium, Tumblr, WordPress. Discussion Networking Sites examples of discussion platforms are Reddit, Quora, and Digg. And so on.

Social media has converted a powerful mechanism for information sharing, solving safety issues, understand current computer attacks. Using these different types of social media platforms, massive amounts of data were available on the internet. Whether these available data and information related to regular people or organization, company, public sector, private sector, etc. It is reachable for everyone who has an interest in it. Forums and specialized blogs are the entrance of cyberattacks. Social media and websites are the entry point for those seeking to learn hacking techniques. More significantly, these cyberthreats are compounded by many vulnerabilities present in SM websites, such as the amount of accessible and diverse types of SMPs, the inadequate architecture and construction of SMPs, the large volume of unorganized fulfilled, and the possibilities that SMPs offer cybercriminals.

Moreover, SM enables social engineers to use people's information to categorize intelligence gathering, misuse, or computer access behaviors. It is also a resource for phishing to mine and collect helpful information for cyberattack purposes. As a consequence of the exponential rise in the use of SM websites, risks including computer viruses, malicious software, and spyware have risen, targeting information security and confidentiality as there are two kinds of SM and internet threats, modern and classic threats. Therefore, for managing the cybersecurity risk and attack on SM, the individuals should follow the following techniques in social media through their use like updates the browser, managing passwords, updating security, SM policy and safety technologies, regulations and laws, and following SM security tools and privacy.

Several cyberattacks on SM were discussed as a result of the study's findings. Based on the current literature, the study exposed that phishing is the most prevalent form of cyberattack, followed by malware, social engineering, then malicious, and spam. Furthermore, the research found that a variety of reasons make social media users vulnerable to cyber-attacks. As a result, we may conclude that education and awareness have an effect on individuals, where the lack of users' awareness and training becomes the weakest point for SM users. It is critical to exercise caution when handling sensitive data, even though it is essential to protect information from cyber threats and recognize the gaps from which criminals gain access to sensitive information.

Cybersecurity awareness and education are crucial for all SM users without regarding the age and gender of the user because the study found that cybercriminals attack users without respect to age or ethnicity. Women, adults, and children are the most targeted group by cyber-attacks due to their lack of cybersecurity and methods to protect themselves. Over and above those approaches to increasing cybersecurity understanding that has been recommended based on the analyzed data again security awareness and education training was a preferable and helpful method. Besides raising awareness and understanding of cybersecurity, the individuals who use SM to prevent their social platforms from cyber-attacks should turn on the firewall, install antiviruses, follow the guidelines, etc.

5.2. Recommendations

The study presented some aspects and characteristics of cybersecurity and social media. The results of the study will help regular people, students, adults, parents, companies, organizations, and other bodies to recognize the cyberattacks, enhancing the factors of vulnerabilities, methods to gain awareness, and prevention techniques, etc. to enhance the safety of using social media and their platforms. Despite that, awareness is still the weakest point for all users of social communication. As can be noted from the results of various points the earlier studies indicated that awareness and education impact websites with different vulnerable factors. Also, the finding of the study clearly illustrated that both of them are crucial for all individuals of any age group. Therefore, the study recommends that:

- It is proposed that the researchers can create a concrete curriculum for raising awareness and education about all the risks and influences of cybersecurity in the early stages of education, particularly secondary and high school.
- Future studies can concern other fields such as cybersecurity in cloud, education, social health care, social automation etc.
- Future studies can improve the finding of the study by including various document types such as conference papers, book chapters...etc.

REFERENCES

Abd Rahman, N. A., Permatasari, F., & Hafsari, Y. (2017). A review on social media issues and security awareness among the users. *Journal of Applied Technology and Innovation*, *1*(1), 28-36.

Abulaish, M., & Bhat, S. Y. (2015). Classifier ensembles using structural features for spammer detection in online social networks. Foundations of Computing and Decision Sciences, 40(2), 3.89-105. https://doi.org/10.1515/fcds-2015-0006

Ahmad, A., Whitworth, B., Zeshan, F., Bertino, E., & Friedman, R. (2017). Extending social networks with delegation. *Computers & Security*, *70*, 546-564. https://doi.org/10.1016/j.cose.2017.07.010

Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. Jurnal Komunikasi: Malaysian Journal of Communication, 35(2). https://doi.org/10.17576/JKMJC-2019-3502-29

Al Amro, S. (2020). How safe is governmental infrastructure: A Cyber Extortion and Increasing Ransomware Attacks Perspective. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(6).

Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. *International Journal of Information Technology and Language Studies*, *3*(2). 8-29

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cybersecurity using fuzzy logic inference system. *Computers & Security*, *74*, 323-339. https://doi.org/10.1016/j.cose.2017.09.011

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence the judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1-19. https://doi.org/10.1186/s42400-020-00047-5

Alguliyev, R., Aliguliyev, R., & Yusifov, F. (2018). Role of Social Networks in E-government: Risks and Security Threats. Online Journal of Communication and Media Technologies, 8(4), 363-376. https://doi.org/10.12973/ojcmt/3957

Aljably, R., Tian, Y., & Al-Rodhaan, M. (2020). Preserving privacy in multimedia social networks using machine learning anomaly detection. Security and Communication Networks, 2020. https://doi.org/10.1155/2020/5874935

Almarabeh, H., & Sulieman, A. (2019). The impact of cyber threats on social networking sites. *International Journal of Advanced Research in Computer Science*, *10*(2), 1-9 http://dx.doi.org/10.26483/ijarcs.v10i2.6384

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health informatics journal*, *25*(2), 315-329. https://doi.org/10.1177/1460458217706184

Alqarni, Z., Algarni, A., & Xu, Y. (2016). Toward predicting susceptibility to phishing victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC)* (pp. 419-426). https://doi.org/10.1109/SCC.2016.61

Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. IEEE Access, 8, 142532-142542. DOI: 10.1109/ACCESS.2020.3013699

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning-based android malware detection using real devices. Computers & Security, 89, 101663. https://doi.org/10.1016/j.cose.2019.101663

Aminzade, M. (2018). Confidentiality, integrity, and availability–finding a balanced IT framework. Network Security, 2018(5), 9-11. https://doi.org/10.1016/s1353-4858(18)30043-6

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science, 8, 540-542. https://doi.org/10.1016/j.pisc.2016.06.014

Asher, T. (2020). What Are the Types of Cybersecurity? Retrieved April 29, 2021, from https://www.ashersecurity.com/what-are-the-types-of-cybersecurity/

Awojobi, B., & Ding, J. (2020). Data Security and Privacy. In: Cybersecurity for Information Professionals: Concepts and Applications. *Taylor & Francis Group CRC Press.* 291-304. https://doi.org/10.1201/9781003042235-13

Baazeem, R., & Qaffas, A. (2020). The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. In *Emerging Cyber Threats and Cognitive Vulnerabilities* Academic Press. 93-116 https://doi.org/10.1016/B978-0-12-816203-3.00005-8

Baethge, C., Klier, J., & Klier, M. (2016). Social commerce—state-of-the-art and future research directions. *Electronic Markets, 26*(3), 269-290. https://doi.org/10.1007/s12525-016-0225-2

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making, and interests predict the effectiveness of competitions as a recruitment tool. *Computers & Security, 65,* 153-165. https://doi.org/10.1016/j.cose.2016.10.007

Behal, S., Kumar, K., & Sachdeva, M. (2018). D-FAC: A novel ϕ-Divergence based distributed DDoS defense system. Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2018.03.005

Bertino, E. (2016). Data security and privacy: Concepts, approaches, and research directions. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). 1*, 400-407. https://doi.org/10.1109/COMPSAC.2016.89

Bess, J. C. (2017). Privacy Public Opinion: Conflicted in the Current Cybersecurity Environment.

Bhathal, G. S., & Singh, A. (2019). Big Data: Hadoop framework vulnerabilities, security issues, and attacks. Array, 1(2), 100002. https://doi.org/10.1016/j.array.2019.100002

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal*, *18*(1), 48-58.

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security, 86,* 350-357. https://doi.org/10.1016/j.cose.2019.07.003

Bootstrap Business (2020). What Are the Different Types of Cyber Security? Retrieved February 5, 2021, from https://www.myfrugalbusiness.com/2020/12/different-types-of-cyber-security.html

Bruning, P. F., Alge, B. J., & Lin, H. C. (2020). Social networks and social media: Understanding and managing influence vulnerability in a connected society. Business Horizons, 63(6), 749-761. https://doi.org/10.1016/j.bushor.2020.07.007

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. (2016). When 'friends' collide: Social heterogeneity and user vulnerability on social network sites. Computers in Human Behavior, 54, 62-72. https://doi.org/10.1016/j.chb.2015.07.039

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. (2017). Motivators of online vulnerability: The impact of social network site use and FOMO. Computers in Human Behavior, 66, 248-255. https://doi.org/10.1016/j.chb.2016.09.055

Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018). Social cyber-security. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation* (pp. 389-394). Springer, Cham. https://doi.org/10.1007/978-3-319-93372-6_42

Chang, L. Y., & Coppel, N. (2020). Building cybersecurity awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Chen, C., Wang, Y., Zhang, J., Xiang, Y., Zhou, W., & Min, G. (2016). Statistical features-based real-time detection of drifted twitter spam. IEEE Transactions on Information Forensics and Security, 12(4), 914-925. DOI: 10.1109/TIFS.2016.2621888

Clement, J. (2020). Number of monthly active Facebook users worldwide as of 3rd quarter 2020. Retrieved February 9, 2021, from • Facebook MAU worldwide 2020 | Statista

Cohen, A., Nissim, N., & Elovici, Y. (2020). Maljpeg: Machine learning-based solution for the detection of malicious jpeg images. IEEE Access, 8, 19997-20011. DOI: 10.1109/ACCESS.2020.2969022

Future of tech. (n.d.). The History of Cybersecurity. Retrieved January 16, 2021, from https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Craig, J. (2018). Cybersecurity research—essential to a successful digital future. Engineering, 4(1), 9-10. https://doi.org/10.1016/j.eng.2018.02.006

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges, and Solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *5*(4),833-838). https://doi.org/10.22214/ijraset.2017.4153

Dennehy, R., Meaney, S., Cronin, M., & Arensman, E. (2020). The psychosocial impacts of cyber victimization and barriers to seeking social support: Young people's perspectives. Children and youth services review, 111, 104872. https://doi.org/10.1016/j.childyouth.2020.104872

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analyzing online social engineering attack surfaces. computers & security, 69, 18-34. https://doi.org/10.1016/j.cose.2016.12.013

El Kamel, N., Eddabbah, M., Lmoumen, Y., & Touahni, R. (2020). A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning. Security and Communication Networks, 2020. 1-9 https://doi.org/10.1155/2020/8865474

El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482. https://doi.org/10.1016/j.compeleceng.2018.01.015

Fang, Y., Gao, J., Liu, Z., & Huang, C. (2020). Detecting cyber threat events from Twitter using IDCNN and BILSTM. Applied Sciences, 10(17), 5922. https://doi.org/10.3390/app10175922

Foreman, C. (2017). 10 Types of Social Media and How Each Can Benefit Your Business. Retrieved February 12, 2021, from https://blog.hootsuite.com/types-of-social-media/

García Holgado, A., Marcos Pablos, S., & García Peñalvo, F. J. (2020). Guidelines for performing systematic research projects reviews. International Journal of Interactive Multimedia and Artificial Intelligence, 6(2), 9. https://doi.org/10.9781/ijimai.2020.05.005

Grispos G. (2019) Cybersecurity: Practice. In: Encyclopedia of Security and Emergency Management. Springer, 1-6 https://doi.org/10.1007/978-3-319-69891-5_81-1

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues, and future directions. *Telecommunication Systems*, *67*(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z

Győrffy, K., Leitold, F., & Arrott, A. (2017). Individual awareness of cyber-security vulnerability-Citizen and public servant. *Central and Eastern European eDem and eGov Days*, *325*, 411-422. https://doi.org/10.24989/ocg.v325.34

Herrick, D. (2016). The social side of 'cyber power'? Social media and cyber operations. In *2016 8th International Conference on Cyber Conflict (CyCon)* (pp. 99-111). https://doi.org/10.1109/CYCON.2016.7529429

Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2020). Trade-off cybersecurity concerns for co-created value. *Journal of Computer Information Systems*, *60*(5), 468-483. https://doi.org/10.1080/08874417.2018.1538708

Huang, Z., Chen, H., & Liu, Z. (2020). The 100 top-cited systematic reviews/meta-analyses in central venous catheter research: A PRISMA-compliant systematic literature review and bibliometric analysis. Intensive and Critical Care Nursing, 57, 102803. https://doi.org/10.1016/j.iccn.2020.102803

Hughes, B. B., Bohl, D., Irfan, M., Margolese-Malin, E., & Solórzano, J. R. (2017). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. Technological Forecasting and Social Change, 115, 117-130. https://doi.org/10.1016/j.techfore.2016.09.027

Ilie-Zudor, E., Kemény, Z., & Preuveneers, D. (2016). Efficiency and security of process transparency in production networks—a view of expectations, obstacles, and potentials. Procedia CIRP, 52, 84-89. https://doi.org/10.1016/j.procir.2016.07.018

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56-59. https://doi.org/10.1109/MC.2018.3191268

Jabee, R., & Alam, M. A. (2016). Issues and challenges of cybersecurity for social networking sites (Facebook). *International Journal of Computer Applications*, *144*(3), 36-40.

Javed, A., Burnap, P., & Rana, O. (2019). Prediction of drive-by download attacks on Twitter. Information Processing & Management, 56(3), 1133-1145. https://doi.org/10.1016/j.ipm.2018.02.003

Jenkins, J., Roy, K., & Shelton, J. (2020). Using deep learning techniques and genetic-based feature extraction for presentation attack mitigation. Array, 7, 100029. https://doi.org/10.1016/j.array.2020.100029

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research*, *55*(1), 3-25. https://doi.org/10.1177/0735633116651971

Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber Security. *HOLISTIC A–Journal of Business and Public Administration*, *10*(2), 115-128. https://doi.org/10.2478/hjbpa-2019-0020

Kamal, R., Shah, M. A., Maple, C., Masood, M., Wahid, A., & Mehmood, A. (2019). Emotion classification and crowdsource sensing; a lexicon-based approach. IEEE Access, 7, 27124-27134. DOI: 10.1109/ACCESS.2019.2892624

Kaster, P., & Sen, P. K. (2015). Cybersecurity and rural electric power systems. In *2015 IEEE rural electric power conference* (pp. 49-54). https://doi.org/10.1109/REPC.2015.23

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, *3*, 1-21. https://doi.org/10.1016/j.osnem.2017.09.001

Khan G.F. (2017) Introduction to Social Media. In: Social Media for Government. Springer, Singapore. 1-6. https://doi.org/10.1007/978-981-10-2942-4_1

Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C. T., & Ramakrishnan, N. (2017). Crowdsourcing cybersecurity: Cyberattack detection using social media. In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management* 1049-1057 https://doi.org/10.1145/3132847.3132866

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity, and Availability in Digital Social Media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)*. 229-237. https://doi.org/10.1007/978-981-13-0074-5_21

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory Vol*, *4*(1).18-24 https://doi.org/10.18178/lnit.4.1.18-24

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. computers & security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

Kim, S. (2020). Anatomy on Malware Distribution Networks. IEEE Access, 8, 73919-73930. DOI: 10.1109/ACCESS.2020.2985990

Kunwar, R. S., & Sharma, P. (2016). Social media: A new vector for cyberattack. In *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring)*. 1-5. DOI: 10.1109/ICACCA.2016.7578896.

Lambert, S. (2020). Number of Social Media Users in 2020/2021: Demographics & Predictions. Retrieved February 9, 2021, from https://financesonline.com/number-of-social-media-users/#link1

Li, J. S., Chen, L. C., Monaco, J. V., Singh, P., & Tappert, C. C. (2017). A comparison of classifiers and features for authorship authentication of social networking messages. Concurrency and Computation: Practice and Experience, 29(14), e3918. https://doi.org/10.1002/cpe.3918

Li, J., Chen, W. H., Xu, Q., Shah, N., Kohler, J. C., & Mackey, T. K. (2020). Detection of self-reported experiences with corruption on Twitter using unsupervised machine learning. Social Sciences & Humanities Open, 2(1), 100060. https://doi.org/10.1016/j.ssaho.2020.100060

Lima, A. Q., & Keegan, B. (2020). Challenges of using machine learning algorithms for cybersecurity: a study of threat-classification models applied to social media communication data. In *Cyber Influence and Cognitive Threats*. Academic Press. 33-52 https://doi.org/10.1016/B978-0-12-819204-7.00003-8

Luo, J., Hong, T., & Fang, S. C. (2018). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting*, *34*(1), 89-104. https://doi.org/10.1016/j.ijforecast.2017.08.004

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle school students' social media use. Journal of Educational Technology & Society, 21(1), 213-224.

Masood, F., Almogren, A., Abbas, A., Khattak, H. A., Din, I. U., Guizani, M., & Zuair, M. (2019). Spammer detection and fake user identification on social networks. IEEE Access, 7, 68140-68152. DOI: 10.1109/ACCESS.2019.2918196.

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE. DOI: 10.1109/ISTAS48451.2019.8937956

Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior, 69, 421-436. https://doi.org/10.1016/j.chb.2016.12.044.

Morrison, A. (2020). What are the 6 types of social media and their advantages? Retrieved November 2, 2021, from https://www.scommerce.com/what-are-the-6-types-of-social-media-and-their-advantages/

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Netto, Y. C., & Maçada, A. C. G. (2019). The influence of social media filter bubbles and echo chambers on it identity construction. *CEP*, *90010*, 460. https://aisel.aisnet.org/ecis2019_rip

Newberry, C. (2020, May 20). Social Media Security Tips and Tools to Mitigate Risks. Retrieved February 15, 2021, from https://blog.hootsuite.com/social-media-security-for-business/

Nweke, L. O. (2017). Using the CIA and AAA Models to explain Cybersecurity Activities. *PM World Journal*, *6*. 1-3

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organizations: a systematic review of recent trends, threats, and mitigation. *Intelligence and National Security*, *35*(4), 556-585. https://doi.org/10.1080/02684527.2020.1752459

Okutan, A. (2019). A framework for cybercrime investigation. Procedia Computer Science, 158, 287-294. https://doi.org/10.1016/j.procs.2019.09.054.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, *26*, 311-327.

Palaniappan, G., Sangeetha, S., Rajendran, B., Goyal, S., & Bindhumadhava, B. S. (2020). Malicious Domain Detection Using Machine Learning On Domain Name Features, Host-Based Features, and Web-Based Features. Procedia Computer Science, 171, 654-661. https://doi.org/10.1016/j.procs.2020.04.071.

Pangrazio, L., & Cardozo-Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. Digital Education Review, (37), 49-63. https://doi.org/10.1344/der.2020.37.49-63

Patil, N. V., Krishna, C. R., Kumar, K., & Behal, S. (2019). E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks. Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.06.016.

Penni, J. (2017). The future of online social networks (OSN): A measurement analysis using social media tools and application. Telematics and Informatics, 34(5), 498-517. http://dx.doi.org/10.1016/j.tele.2016.10.009

Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy, and security by design: the first experience on enterprise servers and data storage products triggered by a policy process. *Computers & Security*, *76*, 295-310. https://doi.org/10.1016/j.cose.2017.12.001

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organizations: Threats, mitigation and approaches. BMJ health & care informatics, 26(1). e100031. DOI: 10.1136/bmjhci-2019-100031

Rahman, A., Malaysia, N. A., Sairi, M. T. U. K., Zizi, I. K., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *Int. J. Inf. Educ. Technol*, *10*, 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Reid, K. (2021). What Are the Different Types of Cyber Security? Retrieved April 29, 2021, from https://triadanet.com/blog/different-types-of-cyber-security/

Ribeiro, L. C., Damaceno, L. P., Tarelho, L. V., Mazalhães, D. V., Rovera, G. D., Machado, R. C., & Garica, G. A. (2018, April). Implementation of Cybersecurity Procedures in Remote Calibration for PNT Services. In *2018 Workshop on Metrology for Industry 4.0 and IoT* (pp. 209-212). DOI: 10.1109/METROI4.2018.8428305

Mindcore, M. (2018, September 5). 5 types of cybersecurity. Retrieved February 5, 2021, from https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. (2020). Toward a Sustainable Cybersecurity Ecosystem. *Computers*, *9*(3), 74. https://doi.org/10.3390/computers9030074

San Juan, N. (2021, April 20). What is cybersecurity. Retrieved April 29, 2021, from https://vpnpro.com/web/what-is-cyber-security/

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016). How students reason about Cybersecurity concepts. In *2016 IEEE Frontiers in Education Conference (FIE)* 1-5. DOI: 10.1109/FIE.2016.7757363

Shevchuk, R., & Pastukh, Y. (2019). Improve the Security of Social Media Accounts. In *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 439-442). DOI: 10.1109/ACITT.2019.8779963

Shillair, R., & Dutton, W. H. (2016). Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. *Available at SSRN 2756736*. 1-39 http://dx.doi.org/10.2139/ssrn.2756736

Shin, H. S., Kwon, H. Y., & Ryu, S. J. (2020). A new text classification model based on contrastive word embedding for detecting cybersecurity intelligence in Twitter. Electronics, 9(9), 1527. https://doi.org/10.3390/electronics9091527.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. Computers in Human Behavior, 60, 35-43. https://doi.org/10.1016/j.chb.2016.02.050.

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. Applied Computer Systems, 24(1), 9-17 https://doi.org/10.2478/acss-2019-0002.

Storm, M. (2020). 5 Types of Social Media and Examples of Each. Retrieved February 12, 2021, from https://www.webfx.com/blog/social-media/types-of-social-media/

Sunil, G., Aluvala, S., Reddy, S. T., Ramesh, D., & Varun, R. (2020). Various Forms of Cybercrime And Role Of Social Media In Cyber Security. *Terminology*, *29*(02), 2709-2715.

Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science*, *126*, 1271-1280. https://doi.org/10.1016/j.procs.2018.08.070

Tai, K. Y., Dhaliwal, J., & Shariff, S. M. (2020). Online Social Networks and Writing Styles–A Review of the Multidisciplinary Literature. IEEE Access, 8, 67024-67046. DOI: 10.1109/ACCESS.2020.2985916.

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cybersecurity in social media: challenges and the way forward. *IT Professional*, *21*(2), 41-49. DOI: 10.1109/MITP.2018.2881373

The history of cybersecurity. (n.d.). Retrieved January 16, 2021, from https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/

Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019). A survey on cybersecurity awareness concerns, practices, and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE. DOI: 10.1109/ICCCI.2019.8821951

Townsend, C. (2019). A Brief and Incomplete History of Cybersecurity. Retrieved January 16, 2021, from https://www.uscybersecurity.net/history/

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. Heliyon, 5(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010.

Tsikerdekis, M., Morse, T., Dean, C., & Ruffin, J. (2019). A taxonomy of features for preventing identity deception in online communities and their estimated efficacy. Journal of Information Security and Applications, 47, 363-370. https://doi.org/10.1016/j.jisa.2019.06.002.

Tu, H., Xia, Y., Chi, K. T., & Chen, X. (2020). A hybrid cyber-attack model for cyber-physical power systems. IEEE Access, 8, 114876-114883. DOI: 10.1109/ACCESS.2020.3003323

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. Journal of manufacturing systems, 47, 93-106. https://doi.org/10.1016/j.jmsy.2018.04.007.

van den Bergh, M. (2018). Protecting Personal Information on Social Media Sites from Cybercrime Activities: A Student Perspective,*1(2)* 20-25.

van der Schyff, K., & Flowerday, S. (2019). Social media surveillance: A personality-driven behaviour model. *South African Journal of Information Management*, *21*(1), 1-9. http://dx.doi.org/10.4102/sajim.v21i1.1034

Van der Walt, E., Eloff, J. H., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. Computers & Security, 78, 76-89. https://doi.org/10.1016/j.cose.2018.05.015.

Vamp, V. (2020, February). [INFOGRAPHIC] The evolution of social media: A timeline. Retrieved January 18, 2021, from https://vamp-brands.com/blog/2020/02/28/evolution-of-social-media/

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cybersecurity education is as essential as "the three R's". Heliyon, 5(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security*. 26 (1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Wade, J. T., Roth, P. L., Thatcher, J. B., & Dinger, M. (2020). Social Media and Selection: Political Issue Similarity, Liking, and The Moderating Effect of Social Media Platform. *MIS Quarterly*, *44*(3). https://doi.org/10.25300/MISQ/2020/14119

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396. https://doi.org/10.1287/isre.2016.0680

Wang, X., Chen, Y., Liu, Y., Yao, L., Estill, J., Bian, Z., ... & Yang, K. (2019). Reporting items for systematic reviews and meta-analyses of acupuncture: the PRISMA for acupuncture checklist. BMC complementary and alternative medicine, 19(1), 1-10. https://doi.org/10.1186/s12906-019-2624-3

Wang, X., Kang, Q., An, J., & Zhou, M. (2019). Drifted Twitter spam classification using multiscale detection test on KL divergence. IEEE Access, 7, 108384-108394. DOI: 10.1109/ACCESS.2019.2932018.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004.

Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. *Computers & Security*, *84*, 53-69. https://doi.org/10.1016/j.cose.2019.03.010

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570-601. https://doi.org/10.1016/j.im.2018.10.001

Zamir, H. (2020). Cybersecurity and Social Media. In: Cybersecurity for Information Professionals: Concepts and Applications. *Taylor & Francis Group CRC Press*. 153-171.

Zernetska, O. (2016). Cybersecurity on US social networks. *American history and politics*, (1), 207-214.

Zhang, H., Yao, D. D., Ramakrishnan, N., & Zhang, Z. (2016). Causality reasoning about network events for detecting stealthy malware activities. computers & security, 58, 180-198. https://doi.org/10.1016/j.cose.2016.01.002.

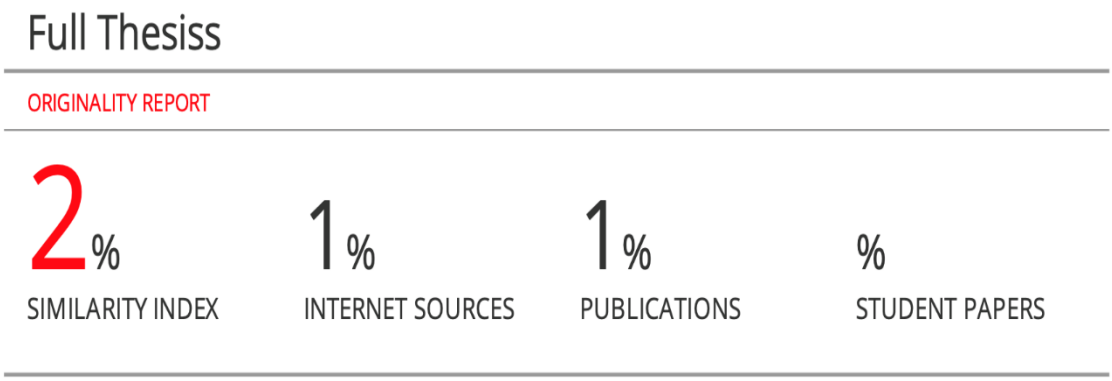
Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. *Future Generation Computer Systems, 86*, 914-925. http://dx.doi.org/10.1016/j.future.2016.10.007

Zhou, Y., Kim, D. W., Zhang, J., Liu, L., Jin, H., Jin, H., & Liu, T. (2017). Proguard: Detecting malicious accounts in social-network-based online promotions. IEEE Access, 5, 1990-1999. DOI: 10.1109/ACCESS.2017.2654272.

APPENDIXES

APPENDIX 1

TURNITIN REPORT



APPENDIX 2

ETHICAL APPROVAL DOCUMENT

ETHICAL APPROVAL DOCUMENT

Date 30.05.2021

To the Institute of Graduate Studies

For the thesis project entitled as "Cybersecurity Issues in Social Media," the researchers declare that they did not collect any data from human/animal or any other subjects. Therefore, this project does not need to go through the ethics committee evaluation.

Titled**: Assist. Prof. Dr.**

Name Surname: **Damla Karagözlü**

Signature:

Role in the research project: **Supervisor**