A

SEMINAR REPORT

ON

"Synergizing Quantum Computing and Artificial Intelligence: A Review of Trends and Opportunities"

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE

THIRD YEAR COMPUTER ENGINEERING

BY

Mr. Mustafa Murtaza Merchant
(Roll No: 74)

UNDER THE GUIDANCE OF

Mr. Sandeep G. Shukla

DEPARTMENT OF COMPUTER ENGINEERING
Guru Gobind Singh College of Engineering and Research Center, Nashik
Khalsa Educational Complex Guru Gobind Singh Marg, Wadala-Pathardi Road, Indira Nagar, Nashik, Maharashtra 422009
YEAR 2025-2026

DEPARTMENT OF COMPUTER ENGINEERING

Guru Gobind Singh College of Engineering and Research Center, Nashik

Khalsa Educational Complex Guru Gobind Singh Marg, Wadala-Pathardi Road, Indira Nagar, Nashik, Maharashtra 422009

Year 2025-26

CERTIFICATE

This is to certify that seminar report entitled

"Synergizing Quantum Computing and Artificial Intelligence: A Review of Trends and Opportunities"

Is submitted as partial fulfilment of

curriculum of the T.E. Computer Engineering

BY

Mr. Mustafa Murtaza Merchant

(Roll No: 74)

(Mr. Sandeep G. Shukla)	(Mr. Ajit R. Pagar)	(Mr.Sandeep. G. Shukla)
Seminar Guide	**Seminar Coordinator**	**Head**

Place: GCOERC, Nashik

Date:

Savitribai Phule Pune University

CERTIFICATE

This is to Certify that

Mr. Mustafa Murtaza Merchant
(Roll No: 74)

Student of T.E. Computer
was examined in Seminar Report entitled

"Synergizing Quantum Computing and Artificial Intelligence: A Review of Trends and Opportunities"

on .../... /2025

At
DEPARTMENT OF COMPUTER ENGINEERING,
GURU GOBIND SINGH COLLEGE OF ENGINEERING AND RESEARCH CENTER, NASHIK
YEAR 2025-26

....
Internal Examiner External Examiner

ABSTRACT

Quantum computing (QC) and artificial intelligence (AI) are coming together in an exciting way, shaking up the tech world, also called as Quantum Artificial Intelligence (QAI). AI is stepping up to improve how quantum systems are designed, fix errors, and fine-tune algorithms, while QC is turbocharging AI tasks like training machine learning models and tackling tough simulations. In this paper, I dive into how AI is making a difference in QC, think calibrating quantum processors, cutting noise with reinforcement learning, and blending quantum-classical models for big language processing. I also explore some key trends for 2025, the UN's International Year of Quantum Science and Technology, like scalable error-corrected qubits (check out Google's Willow chip!), modular setups with over 1,000 qubits, and quantum networks that enable distributed computing. This paper checks out some really cool real-world uses, like drug research, banking, and cybersecurity, while facing down challenges like qubit decoherence and a real crunch for skilled folks. From what I have found, AI teamed up with quantum computing might just give us a leg up in specialized areas by 2029, unlocking breakthroughs for those tricky problems. But honestly, cracking those scaling issues will take a group effort from all sorts of experts. This study lays out a solid picture for researchers and practitioners, with an eye on the exciting road ahead in this ever-changing field.

Keywords: Quantum Computing, Artificial Intelligence, Quantum AI Synergy, Error Correction, Reinforcement Learning, Hybrid Models, Qubit Scalability, Quantum Networks, Drug Discovery, Financial Optimization, Cybersecurity, Quantum Advantage, NISQ Devices, Fault-Tolerant Computing, Machine Learning Acceleration.

ACKNOWLEDGEMENT

It is my immense pleasure to work on this seminar **Synergizing Quantum Computing and Artificial Intelligence: A Review of Trends and Opportunities**. It is only the blessing of my divine master which has prompted and mentally equipped me to undergo the study of this seminar.

I would like to thank **Prof.(Dr). N. G. Nikam**, Principal, Guru Gobind Singh College of Engineering and Research Center for giving me such an opportunity to develop practical knowledge about subject. I am also thankful to **Mr. Sandeep G. Shukla**, Head of Computer Engineering Department for his valuable encouragement at every phase of my seminar work and completion.

I offer my sincere thanks to my guide **Mr. Sandeep G. Shukla**, who very affectionately encourages me to work on the subject and gave her valuable guidance time to time. While preparing this seminar I am very much thankful to him.

I am also grateful to entire staff of Computer Engineering Department for their kind co-operation which helped me in successful completion of seminar.

Mr. Merchant Mustafa Murtaza

GCOERC, NASHIK.

INDEX

List of Figures

Chapter 1

INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Today, almost everybody in the world uses social media but most of them do not always give concern to security. This is the procedure of analysis of social media dynamic data to save from ultimatum in business. Every industry has to face some sort of a special collection of risks on social. Many put themselves at the center of controversy or in the press of the organization. In the present, many people are using social media in a high percentage. They did not consider their data and information security. In the present time, Social media networks are always the main priority target of cyber security attacks. Because of their massive user base. There are many studies that explore vulnerabilities of security as well as issues of privacy in social networking sites. Those researches made better recommendations to diminish from security risks. Therefore this analysis focuses mainly on factors of study impact among users of public sector organizations for the protection of social media emphasis. Particularly in the education sector.

In current times many people are using social media. Every social media application asking personal details for signup. Every people give their all details depends with their privacy without considering whether they are using is more secure or less secure. Here is the breakdown of personal information that all social media platforms

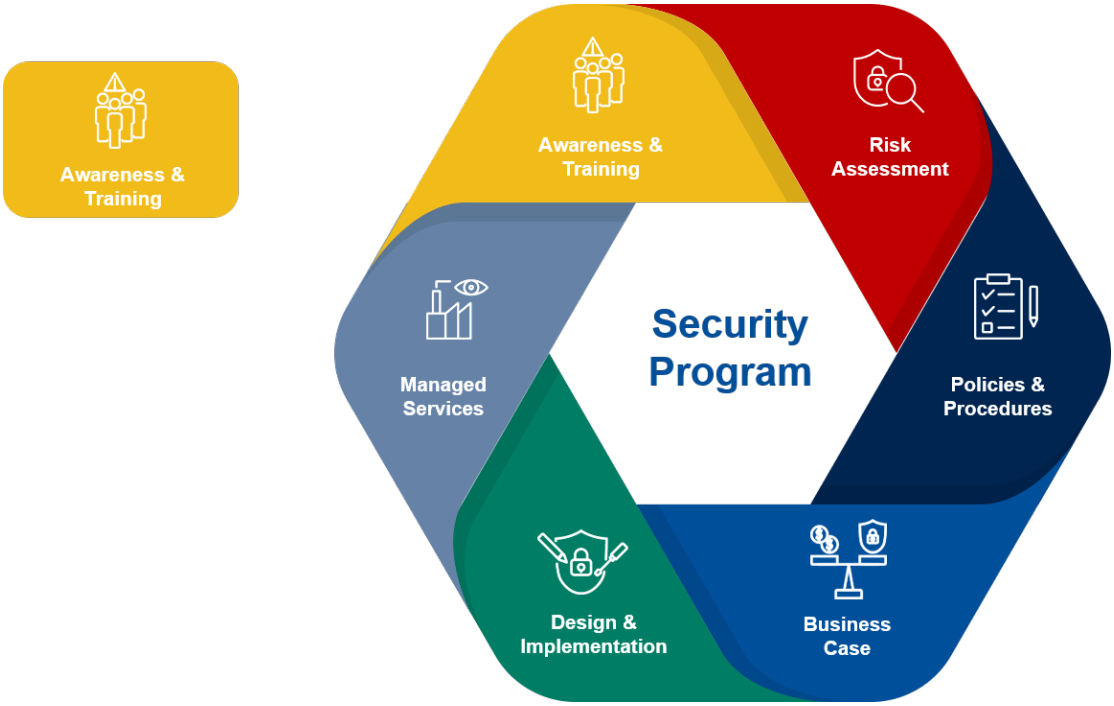

Figure 1.1: Security Program

are gained by users. Name, email, address book, credit card information, debit card information, language, etc. There are couple of tools in security tools. They are social media developers realized security tools and external web services realized tools. The combination of those two tools allow for a user to complete the security of accounts. There are some of them as an example; two-factor authentication, private account, security checkup, login notification, password strength Hiruni Fernando Department of Information Technology Sri Lanka Institute of Information Technology Malabe, Sri Lanka fernandohiruni55@gmail.com Shashipraba Perera Department of Information Technology Sri Lanka Institute of Information Technology Malabe, Sri Lanka shashipraba.56@gmail.com 2 checker, trusted contacts, periodic password changes, external application or site access checkup, email breaches checkup, identification code etc

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities

in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

Chapter 2

HISTORY AND EVOLUTION OF SOCIAL MEDIA

The use of the internet started to spread and people experiences new life since 1980 . Social media comprises communication websites that facilitate relationship forming between users from diverse backgrounds, resulting in a rich social structure . More specifically define social media as Social media is a means of contact for online interactions between the end users (viewers) and data generators (data owners) who build virtual communities using online social networks (OSN) .

Its being protected by internet-connected systems, including hardware, software and data, from cyber attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data,is a subset of cyber security.

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber threats, produce something together individual security technologies - one on top of another to safe their networks andthe valuable data within them. Not only is this method expensive and complex, butnews of damaging cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the area of group of people of data breaches, the topic of cyber security has launched to the top of the priority list for boards of directors, which they seeked as far as less risky way. Instead, organizations can a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection - on theendpoint, in the data centre, on the network, in public and private clouds, and acrossSaabs environments. By focusing on prevention, organizations can prevent cyber threats from impacting the network in the first place, and less overall cyber securityrisk to a manageable degree

The Cybersecurity checking began in the 1970s when researcher Bob Thomas created a computer program called Creeper that could move across ARPANET's network. Ray Tomlinson, the innovator of email, wrote the program Reaper, which chased and deleted Creepers. Reaper was the very first example of checking a malware an-

tivirus software and the first self-replicating program i.e. Viruses, as it made first-ever computer worms and trojans.

In 1971s, Programmer Bob Thomas made history by innovating a program that is widely accepted as the first incident ever computer trojan as the worm and trojan bounced between computers pc,which has groundbreaker at the time. The trojan was not at all malicious.Manke and Winkler the measures that create the greatest likelihood of security awareness success include the use of creativity in disseminating materials and participatory experiences.

Per NIST 800-50, an awareness program, unlike a security training program, specifically intends to change behavior and culture. It aims to provide information that impacts daily actions. That requires a drastically different approach than just providing information. While employees in some organizations get specific security training, for a vast majority of technology users (common people including college students and school kids), security awareness is limited to some tips for security available in some websites. This is why most security awareness programs fail. The increasing number of data breaches and other cyber-attacks clearly demonstrate that these tips are not enough to raise public security awareness to a level required to create a secure cyber culture.

project and the results of the pilot study that has been done. We have organized the paper in the following way. In next section, we describe related work on this topic. In section 3, we describe the project in details. In section 4 results of the pilot study are discussed. Finally, we draw the conclusion from our study and state our direction for future research on this topic.

Users exchange a huge amount of personal details on social networks, making them a target for different types of Internet attacks, including identity theft, phishing, cyber bullies, spamming, Web fraud, etc. Social networks provide hackers with vast opportunities to rob identity. In these types of attacks, a malicious individual may steal his or her personal details, including bank accounts, addresses, telephone numbers, etc., without the user's permission, and using it to commit cyber-crime. For example, a lot of social networks, including Facebook, give their users game apps [3].

To complete the registration process, such applications include personal details, like the user's credit card details, phone number, email, etc. Of course, when a user shares the phone number and credit card details the risk of personal details theft and phishing attacks is increased. In certain cases, apps that result in the user resorting to redirect the user's attention to harmful content and damage its credibility. Some of the most obvious potentially innocuous possibilities in the sense of social networking may be the illegal use for promotional purposes of personal details, the collection of possible friends

or the discovery of content that may be of interest. Such techniques are considered a common process within social networks, and everybody knows about the collection, review, and usage of personal information for various purposes, including commercial usage. For one thing, it has already verified the transfer of personal data from different social networks. One of the main issues for users is that numerous user specific data leakage can be observed as a consequence of the social network's failure within the framework of various initiatives. One causes of significant disruption is hacking user accounts or lack of accountability, and intercepting all personal information. When the problem is huge, there will be more serious issues. There are several possible risks to users, like computer bugs, malware, Trojan horse, phishing, and other malicious software, and they can be used to steal sensitive information from the user. According to experts, phishing attacks are one of the most common cybercrime attacks and the key focus is Internet payments, Internet banking, Internet stocks, online games, Web 2.0 technology used pages, and so on [3]. Beyond the danger of misuse of personal details, social networks are an instrument for mass demonstrations in the sense of threats to public security. The disruptive problems of social networks are revealed to outside intervention, creating tensions between the government and the people, demonstrations in a short time

Chapter 3

LITERATURE SURVEY

3.1 Need of Soial Media

Why do we need social media? Social media accept a bond building between users from distinct backgrounds, resulting in a tenacious social structure . However, according to currently websites of social networking have become an active ground for cybercriminals. So does social media have positive or negative effects? According to Social media is one form of communication which has both positive and negative effects for its users . This study has been able to convey both positive and negative effects of social media to users clearly[1].

3.2 Role of security in social media

One of the biggest disadvantages of social media is the issue of privacy and security. But why exactly we need security in social media. In spite of the security of social media is a now widely-studied subject, there still does not seem to be a consensus for exactly why we need social media security. It was checked that most consumers are generally unaware of the fact that the numerous privacy risks involved in posting personal information on social networking websites are widespread. But has mentioned that, Social media prominence is such that active social media users around the 3 world are projected to reach some 2.95 billion by 2020 . However, there's quite less information on why social media security is needed in this paper[3].

3.3 Access and usage of Social Media

In general, users may use their personal computers or mobile devices to access social media services through web based technologies [1]. Such accesses to websites of social media allow users to have an account or build their own accounts through some authentication and compliance with policies. The verification involves special information about an individual, such as a telephone number, email address, current location, etc. On the other hand, the social media policy's aim is to set standards for acceptable actions and

ensure that users do not expose social media platforms to legal or public humiliation issues. These regulations include guidelines on using the platform for social networking, and guidelines on what kinds of knowledge should be exchanged. Nearly all social media policies contain limits on disclosure of sensitive or proprietary company information or something that could influence others. The incorrect use of social media, particularly users who have no or limited cyber culture, may face the user to attack or hack. About 3.48 billion active social media users now exist, making social media an inevitable part of life strategy [1]. Social media network users can share various pieces of personal information with others when people upload their images, share their birth date, reveal their phone number and write their current address. Sharing such personal data will lead to misuse of the data. For example, some users exchange profile information that includes their full name, telephone number, and other sensitive details. Hacking uses one of the users ' social network account and the hacker can misuse the information for blackmailing the user. While comparing the most popular social networks, it's important to evaluate them by active account usage, not just by the number of user accounts. Research has shown that some social networks are rising faster than others, although others are in decline now. Popular examples of social media sites are Facebook, Twitter, Instagram, etc. Nowadays, Facebook is one of the most popular social media in use around the world. In 2019, Facebook announced that they have more than 2.38 billion active monthly users [1]. The network enables users to create profile pages where they can view themselves, post photos etc. Facebook also allows various apps to be used inside the network, from fortune cookies to messenger. Twitter is a microblogging website and up to one hundred forty characters of short messages may be added to her or his account[2].

3.4 Social media challenges and security risks

Users exchange a huge amount of personal details on social networks, making them a target for different types of Internet attacks, including identity theft, phishing, cyber bullies, spamming, Web fraud, etc. Social networks provide hackers with vast opportunities to rob identity. In these types of attacks, a malicious individual may steal his or her personal details, including bank accounts, addresses, telephone numbers, etc. without the user's permission, and using it to commit cyber-crime. For example, a lot of social networks, including Facebook, give their users game apps .

To complete the registration process, such applications include personal details, like the user's credit card details, phone number, email, etc. Of course, when a user shares the phone number and credit card details the risk of personal details theft and phishing attacks is increased. In certain cases, apps that result in the user resorting to redirect the user's attention to harmful content and damage its credibility. Some of the most

obvious potentially innocuous possibilities in the sense of social networking may be the illegal use for promotional purposes of personal details, the collection of possible friends or the discovery of content that may be of interest. Such techniques are considered a common process within social networks, and everybody knows about the collection, review, and usage of personal information for various purposes, including commercial usage. For one thing, it has already verified the transfer of personal data from different social networks.

One of the main issues for users is that numerous user specific data leakage can be observed as a consequence of the social network's failure within the framework of various initiatives. One causes of significant disruption is hacking user accounts or lack of accountability, and intercepting all personal information. When the problem is huge, there will be more serious issues. There are several possible risks to users, like computer bugs, malware, Trojan horse, phishing, and other malicious software, and they can be used to steal sensitive information from the user[2].

Chapter 4

CYBER SECURITY

cyber security refers to the practices and measures taken to protect computer systems, networks, and data from unauthorized access, attacks, and damage. It involves implementing various techniques like encryption, firewalls, and secure authentication to safeguard against cyber threats such as hacking, malware, and data breaches. Cyber security is crucial in ensuring the confidentiality, integrity, and availability of information in the digital world. It helps protect individuals, organizations, and even social media platforms from potential risks and vulnerabilities.

Social media takes a major role in the present society. People enable them keep to be connected with each other in a better manner and make new opportunities for their business. In the present, many people are using social media in a high percentage. Recently, the internet is the most growing technology for almost everyone's everyday uses. With Internet technology, everyone around the world can communicate, exchange information, play, and many other Internet uses in a simple and semi-free manner, even with very limited information technology experience . Social media is a series of Web pages focused on the Internet. Social media's purpose and the role is to facilitate the personal as well as business-focused engagement people of around the world. Social networking is a tool that enables content sharing between users. The contents are different types of information on a range of topics. In addition, the service also helps users to exchange new concepts, thoughts, and experiences with many people. Many social media forms, networks and services are available nowadays, including Facebook, Instagram, YouTube, LinkedIn, Twitter, and snapchat.

Cyber security is like having a digital bodyguard that protects your personal information, online accounts, and devices from cybercriminals. It involves using techniques such as encryption, strong passwords, and secure networks to keep your data safe. Cyber security also helps prevent unauthorized access, identity theft, and other cyber threats. It's like having a shield that keeps you safe in the digital world.

4.1 How does Cyber Security make working so easy?

No hesitation that the tool of Cybersecurity makes our work very easy by ensuring the obtainability of the capitals limited in any network. A commercial or society could look a huge damage if they are not honest about the safety of their online occurrence. In today's linked world, everyone aids from progressive cyber defence agendas. At a separate level, a cybersecurity outbreak can result in entirety from individuality theft, to blackmail attempts, to the damage of vital data similar family photographs. Everybody relies on dangerous structure like influence plants, infirmaries, and monetary service businesses. Securing these and other societies is essential to trust our civilization operative. One and all also remunerations from the work of cyberthreat investigators, similar the team of 250 risk investigators at Talos, whoever explore new and developing fears and cyber bout policies. They disclose new susceptibilities, teach the community on the position of cybersecurity, and toughen open source gears. Their work marks the Internet harmless for one and all.

4.2 Cyber Ethics

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

1. DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world.

2. Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

3. Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

4. Do not operate others accounts using their passwords.

5. Never try to send any kind of malware to other's systems and make them corrupt.

6. Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

7. When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

8. Always adhere to copyrighted information and download games or videos only if they are permissible. The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

Chapter 5

ROLE OF CYBER SECURITY IN SOCIAL MEDIA

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

5.1 Cyber Crime

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances

Chapter 6

ADVANTAGES AND DISADVANTAGES

6.1 Advantages

It helps protect your personal information from unauthorized access, ensuring your privacy

It reduces the risk of falling victim to cyber threats like phishing scams and malware.

By implementing strong security measures, it helps prevent identity theft and cyberbullying incidents.

cyber security measures provide a safer and more secure online experience while using social media platforms

6.2 Disadvantages

There are no specific disadvantages of cyber security for social media. However, some users may find it inconvenient to remember and manage strong passwords or adjust privacy settings.

Additionally, certain security measures might limit the functionality or accessibility of certain features.

One potential disadvantage could be that strict security measures may require additional steps for authentication or verification, which might be seen as time-consuming.

Chapter 7

CONCLUSION

social media includes high-security risks as well as risks to privacy. Because of their centralized infrastructure, their massive archive of all the personally identifiable data a hacker could ever need, and the general public's ignorance of how to properly use privacy settings to improve their online security [9], they run this danger. There is also a huge danger, because a lot of people, especially adolescents, always tend to trust other people quickly. So, they become extremely confident about others. Not only that they also share private details about themselves without a proper understanding of what kind of details they should share about themselves online.

Social media have some benefits, but in addition to these advantages, OSN's posed some similar concerns. Users' privacy and protection, and their information, are key issues in social media [4]. While there is some general opinion about what social media security and what it can help the online users, there are still many unanswered questions. We think that the headway of new technology as a rule and specifically, social sites will bring new security risks which may open the doors to vindictive performers, key lumberjacks, Trojan horses, phishing, spies, viruses and attackers [6]. However, there are many possible solutions presented to avoid the risks. Information security experts, government officials, and other intelligence officers need to develop new strategies that combat and adjust to the emerging future risks and threats [6]. Moreover in the technical aspect, for preserving the security of social media, techniques like K-anonymity and diversity can be used

References

1 S. R. Zeebareea, S. Y. Ameen and M. A. M. Sadeeq, "Social Media Networks Security Threats, Risks and Recommendation: A Case Studyin the KurdistanRegion,"2020.[Online].Available:https://www.researchgate.net /publication/342693220_Social_Media_Networks_Security_Threats_Risks_and_Recommendation_A_Case_Study_in_the_Kurdistan_Region. [Accessed 02 August 2020].

2 R. Shevchuk and Y. Pastukh , "Investigation of social media security : A CriticalReview". 439-442. 10.1109/ACITT.2019.8779963.," 2019. [Online]. Available:https://www.researchgate.net/publication/334891408_Improve_the_Security_of_Social_Media_Accounts. [Accessed 02 August 2020].

3 R. Alguliyev, R. Aliguliyev and F. F. Yusifov, "Role of SocialNetworks in E-government: Risks and Security Threats., " Online Journal of Communication and Media Technologies., 2018. [Online]. Available:https://www.researchgate.net/publication/328896849 _Role_of_Social5_Networks_in_E-government_Risks_and_Security_Threats.[Accessed 10 August 2020].

4 Z. Y. Alqubaiti, "The Paradox of Social Media Security: A Study of IT Students' Perceptions versus Behavior on Using Facebook.," [Online].Available:https://www.researchgate.net/publication/313566403_The_Paradox_of_Social_Media_Security_A_Study_of_IT_Students'_Perceptions_versus_Behavior_on_Using_Facebook. [Accessed 09 August 2020].K.Elissa, "Title of paper if known," unpublished.

5 P. Goud Kandikanti, "Investigation on Security Issues and Features in Social Media Sites (Face Book, Twitter, & Google+)", 2017.

6 A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

7 Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.