# DIGITAL SECURITY ON SOCIAL NETWORKS


**A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science & Engineering.**

## Submitted by

**Jahidul Islam (CSE-190101322)**
**Neaz Ahamed (CSE-190101292)**
**Md. Asif Arifine (CSE-190101325)**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**
**NORTHERN UNIVERSITY BANGLADESH**

December, 22

# APPROVAL

This thesis "**Digital Security on Social Networks**" submitted by **Jahidul Islam (CSE-190101322), Neaz Ahamed (CSE-190101292) and Md. Asif Arifine (CSE-190101325)** to the Department of Computer Science and Engineering, Northern University Bangladesh, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science & Engineering approved as to its style and contents.

**Board of Examiners:**

1. **Md. Ruhul Amin** **….…..……..……**
   **(Supervisor)**

2. **…….** **……**
   **(Examiner)**

3. **…….** **……**
   **(Examiner)**

**……**
**Md. Raihan-ul-Masood**

**Associate Professor & Head**

**Department of Computer Science & Engineering**

**Northern University Bangladesh**

# DECLARATION

We hereby, declare that the work presented in this Thesis is the outcome of the investigation performed by us under the supervision of Md. Ruhul Amin, Assistant Professor, Department of Computer Science and Engineering, Northern University Bangladesh.

We also declare that no part of this Thesis has been or is being submitted elsewhere for the award of any degree or diploma.

## Candidates-Signature

……

**Jahidul Islam**
**ID:CSE190101322**

……

**Neaz Ahamed**
**ID:CSE190101292**

……

**Md. Asif Arifine**
**ID:CSE190101325**

# ACKNOWLEDGEMENTS

Starting with the name of Almighty Allah for giving us chance to complete and respect to our Supervisor Md. Ruhul Amin, Assistant Professor, Department of Computer Science and Engineering, Northern University Bangladesh (NUB), for this constant guidance, advice, encouragement and every possible help throughout the work and preparation this Thesis. Without his support this thesis would not be initiated. Last and most we want to thank our Parents who dedicated their love and unconditional support of our life for our education for filling with ambition and giving us inspiration.

# ABSTRACT

Social networks are the most popular platform in the current era. People of different ages use this social media. Social networks attract users and totally engage them. Most of the social networks are easily accessible to everyone. Digital security is being compromised due to careless use of it. There arises a number of vulnerabilities and threats, but most of the user is not aware of it. These vulnerabilities could be addressed by possible counter measures. This thesis is a comprehensive study on social networks, possible attacks on digital data, and various security measures that users should adopt to protect themselves from attackers.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER-1:
# INTRODUCTION

## 1.1 Introduction

Social networking has become a need of today's life. It seems that a person can forget to breathe, but doesn't forget to check notifications from various social media accounts. This is the way to connect with various people from different backgrounds, cultures, nationalities, domains, age groups, and gender.[1]

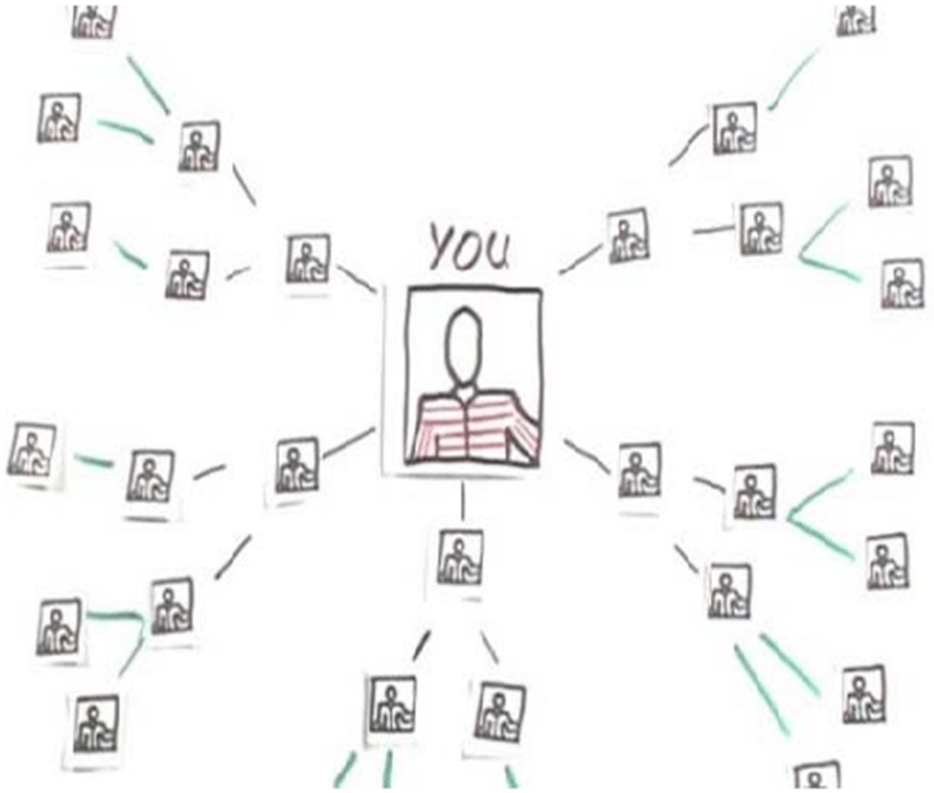


Fig.1.1: Connecting People through Social networking

**In figure 1.1,** we have shown a snapshot how people are inter connected with each other using social networks.

## 1.2 Objectives of the study

The objectives of this thesis are the followings

1. To conduct a comprehensive study on social networking sites.
2. To classify different types of attacks on social networking sites.
3. To test an encryption-decryption algorithm.

## 1.3 Layout of the thesis

- **Chapter 1:** Presents introductory information about the Thesis. Today social networks are very popular but Digital security is being compromised due to careless use of social networks. This chapter gives general idea about the thesis and its objectives.

- **Chapter 2:** Provides background data about our thesis. Social networking websites are currently the most widely used media in our daily lives. This chapter provides broad statistical data on social networking platforms used globally and in Bangladesh.

- **Chapter 3:** This chapter discusses digital security, provides a very brief summary of the information on the risks associated with social media. The most typical cyber Attacks on social media are discussed in this chapter.

- **Chapter 4:** Describes several network layer assaults on social networking sites with security measures and outlines the many categories of attacks with attack types.

- **Chapter 5:** Explains the security measures on text file while using social network. In this chapter we have tested an algorithm which converting data from plaintext to cipher text and cipher text to plain text.

# CHAPTER-2:
# BACKGROUND

## 2.1 Social Media:

Social media and social networking are used side by side to represent any activity socially using electronic medium. By definition, social media is used as a tool to convert your thought, idea, message or any other kind of information to particular set of audience or broadly. In social networking, people do engage Application and make a kind of network of people to communicate with each other and make relationships [2].

## 2.2 Social Networking Users:

As it is stated, social media and social networking are interlinked, so this can be at various platforms with the usage of applications or through simple websites. This is the era of mobility. So there exists more than one way to approach any social networking tool or social media website. Like Facebook can be accessed through website, through mobile application using any kind of computing device such as laptop, desktop computer, mobile, handheld device etc. Also they are being designed in such a friendly style that it doesn't require any kind of training to use it. It definitely enhances its usage by all age groups and from diverse background. Following (Fig.2) Is the data collected from www.statista.com representing number of social media in billions from 2010 to 2021(Expected) [3].

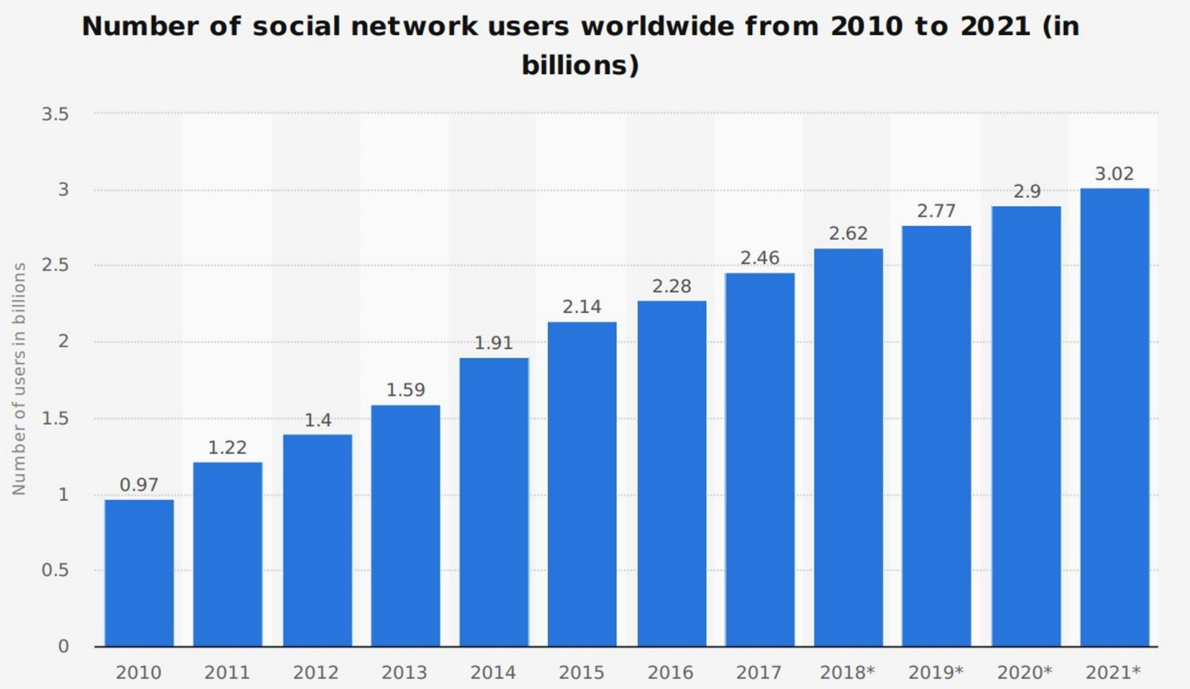


Fig.2.1 Number of Social media users worldwide

**In figure 2.1,** we have shown a statistics that number of social network users are increasing in every year.

TABLE 2.1: ACTIVE USERS OF SOCIAL NETWORKING

| Social Media | Active Users in millions |
|---|---|
| Facebook | 2930 |
| YouTube | 2240 |
| WhatsApp | 2440 |
| Messenger | 1300 |
| WeChat | 1288 |
| Instagram | 1393 |
| QQ | 595 |
| Qzone | 517 |
| TikTok | 732 |
| SinaWeibo | 521 |
| Twitter | 396 |
| Reddit | 430 |
| LinkedIn | 310 |
| BaiduTieba | 300 |
| Skype | 300 |
| Snapchat | 528 |
| Viber | 260 |
| Pinterest | 459 |
| Line | 169 |
| Telegram | 600 |

**In Table 2.1,** we have shown a statistic that shows the active users of different social networking sites all over the world.

## 2.3 User Statistics for Bangladesh

According to BTRC the Internet Subscribers has reached **112.715** Million at the end of February 2021. According to Data Report, there were **45.00 million** social media users in Bangladesh in January 2021. The number of social media users in Bangladesh **increased** by **9.0 million** (+25%) between 2020 and 2021[5].

According to Stat Counter, the distribution of social media plat form market share from March2020-March2021in Bangladesh is-

- Facebook-64.04%
- Twitter-31.45%
- YouTube-2.63%
- Pinterest-0.93%
- LinkedIn-0.71%
- Instagram-0.15%

## 2.4 Facebook

| Total user | % of Total population | Audience %based Of Gender | | Largest User Group | | Highest Difference between Men & Women | | |
|---|---|---|---|---|---|---|---|---|
| | | Male | Female | Age | Total Users | Age | Leading Gender | Lead By (User) |
| 46,420,000 | 27 | 68.9 | 31.1 | 18-24 | 20,000,000 | 25-34 | Male | 7,200,000 |

Table 2.2: Users of Facebook

**In Table 2.2,** we have shown a statistics on Facebook users of Bangladesh.

## 2.5 Messenger

| Total user | % of Total population | Audience %based Of Gender | | Largest User Group | | Highest Difference between Men &Women | | |
|---|---|---|---|---|---|---|---|---|
| | | Male | Female | Age | Total User | Age | Leading Gender | Lead By (User) |
| 41,580,000 | 24.2 | 30.2 | 69.8 | 18-24 | 18,000,000 | 25-34 | Male | 6,400,000 |

Table 2.3: Users of Messenger

**In Table 2.3,** we have shown a statistics on Messenger users of Bangladesh.

## 2.6 Instagram

| Total user | % of Total population | Audience % based Of Gender | | Largest User Group | | Highest Difference between Men & Women | | |
|---|---|---|---|---|---|---|---|---|
| | | Male | Female | Age | Total User | Age | Leading Gender | Lead By (User) |
| 3,732,300 | 2.2 | 68.9 | 31.1 | 18-24 | 2,000,000 | 25-34 | Male | 800,000 |

Table 2.4: Users of Instagram

**In Table 2.4,** we have shown a statistics on Instagram users of Bangladesh.

## 2.7 LinkedIn

| Total user | % of Total population | Largest User Group | |
|---|---|---|---|
| | | Age | Total User |
| 4,017,000 | 2.3 | 25-34 | |

Table 2.5: Users of LinkedIn

**In Table 2.5,** we have shown a statistics on LinkedIn users of Bangladesh.

# CHAPTER-3:
# DIGITAL SECURITY & ATTACKS

## 3.1 Digital Security

Digital Security is the protection of one's digital personality, as it represents the physical identity on the network you are operating on or the internet service in use [6]. Digital Security includes the tools which one uses to secure his/her identity, asset and technology in the online and mobile world. Simply put, let's think of digital personality as the human body. We have a duty to protect our body from harm which we could say is digital security. There are a number of methods (tools) that we use to protect our bodies. We eat and live healthy and put ourselves out of harm's way. The same applies to our digital personality [7].

## 3.2 Attacks on Social Media

There can be variety of portals. Here a brief description of attacks is being given.

### 3.2.1 Identify Theft

It causes the attacker to control the victim's profile and then misuse it for his own unauthorized use.

### 3.2.2 Spam attack

It makes attacker to capture information of the user and then send spam messages or data. The aim is to build network congestion and to consume maximum bandwidth which can lead to bottle neck too as sometimes complete unavailability of the legitimate information of the user, as well.

### 3.2.3 Malware attacks

They are the most common attacks that cause unauthorized access to the legitimate user device. Attacker can send URL or any image and text that contain malware. If user clicks on that link, malware will be installed on that particular device. Malware could be virus or a worm which will have propagating feature and will badly affect the computer in terms of performance, and efficiency.

### 3.2.4 Phishing

Here, attacker targets sensitive information of the user through any source like fake website, but for user, that fake website or email seems to be authentic. Like employee can receive any request data from another employee of the same organization, first 1employee doesn't know second employee but as used the fake information of the organization, can open the information sent by him and could become the victim of the attacker.

### 3.2.5 Impersonation

Attacker can target a particular user and create fake profile to show him as authentic and real user. It is very common attack in social media that not only affect the privacy of the user but also spoils contact list that the user have by sending unethical messages, images etc.

### 3.2.6 Hijacking

Hijacking is a kind of adverse attack that enable attacker to take complete control on user's profile. This is mainly possible because of taking access to authentication details by any source. Password could be guessed too if any particular user is targeted and attacker knows that person as normally we choose password that are not strong enough and based on some personal information. So there is more possibility of hijacking the account authorization details and become the victim of the attack.

### 3.2.7 Fake Requests

User has the attack of fake requests that are being sent by the attacker repeatedly with aim to screw the privacy of the user. If user accepts the request, the attacker will have the chance to view personal information, networks and sometimes other contacts too. So opening room, for further attacks, by fake requests and effect the privacy and security of the users.

### 3.2.8 Image Retrieval and analysis

This is advanced attack that enables the attacker to use various kinds of software for face recognition and image recognition, speech recognition and processing. Images could be collected from the target and then use them for various unethical causes that badly affect the privacy of the user as well as poor impact on social circle too.

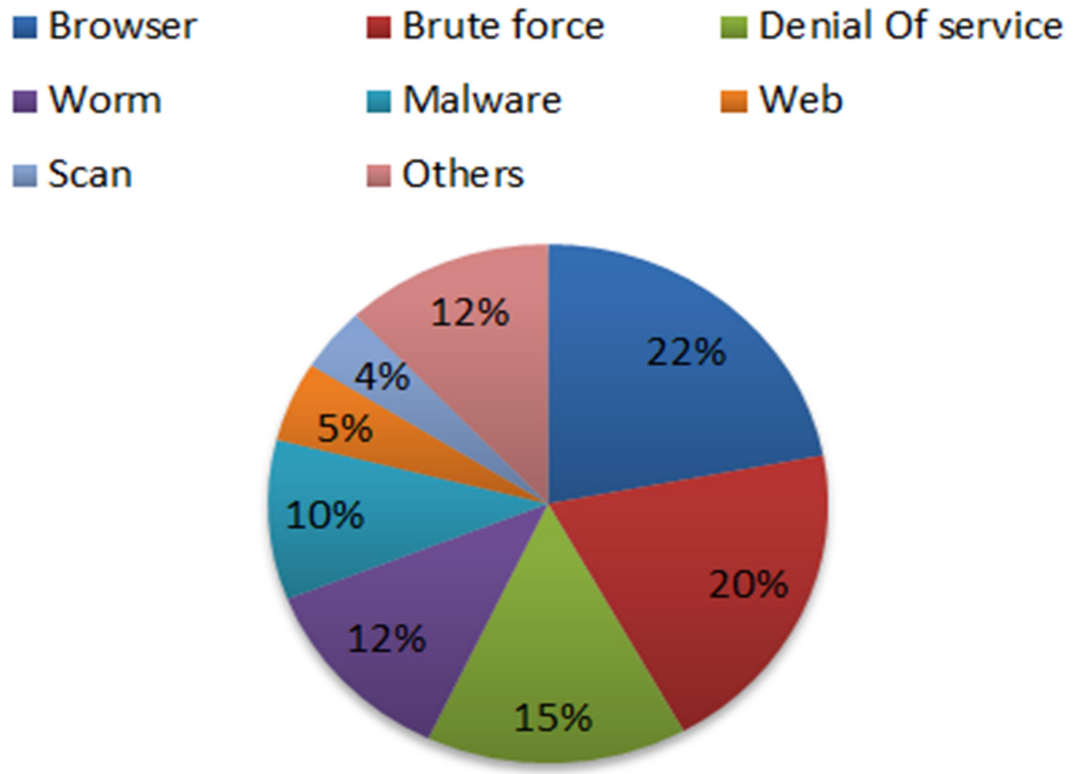


Fig. 3.1: Data of social media attacks

**Figure 3.1**, Shows us that data on various social media attacks. The most frequent assaults on browsers are browser, brute force, denial of service, malware, worms, web, scans, and others.

# CHAPTER-4:
# ATTACKS CHARACTERISTIC
# &
# SECURITY MEASURES

## 4.1 Attacks Characteristics

Security, privacy and performance that we are targeting in his paper and implementing on Social media. For any system to secure it must accomplish confidentially, integrity and availability [8].Block chain is one way to implement security to secure digital data. In [9], focus is on security of IOT and implement it, concept of consumer security index is being introduced. This is the work of the project where requirements have been gathered using Study methods have been conducted And for each study, aim, used methods/design, analysis are well elaborated. This introduces new idea to Implement any security measure on digital data through study approaches, same as discussed in [9].

MAC layer attack can be at wireless interface, hardware, software, on sensor input and on infrastructure. Jamming attack is very common that can cause denial of service. Node targeted flooding can happen. Data could be manipulated at sensor input to misguide the readings. It can lead to random number generation tempering. Reply messages can be generated. It causes bandwidth consumption too to produce latency. Overall confidentiality, integrity, authenticity and network availability is being compromised as result of MAC layer attacks [10]. Router is a device that works in layer 3 of OSI model and its main job is routing. Attacks at routing layer can affect routing by intrusion of wrong information of paths and misguiding in packet forwarding. Attacks at this layer can be denial of service, denial of node, man in middle to create falsified information, spoofing, emerging spam messages, and attack on reading of sensor input data, jamming, malware, black hole, grey hole, wormhole, reply, timing, unauthorized access and change in information of data[11].It main targets at hardware, software level by either spoofing or by intrusion of malicious entity either as a node or as outside attacker to create wrong information about route, drop any packet, act of malicious node like the original node, reply to the old messages, controlling the routing and effecting the network by any mean. This can cause consumption of bandwidth, Congestion of data pockets and even could fail the complete network as well as routing is one of the basic functions of wireless networks [12].

TABLE 4.1: CATEGORIES OF ATTACKS WITH ATTACK TYPE AND DESCRIPTION

| Category | Attack | Description |
|---|---|---|
| **Using wireless interface** | Location Tracking | Attacker locates the location of the user. |
| | Denial of Service | Attacker attacks to make services unavailable for the user. |
| | Distributed Denial of Service | Attack like Denial-of-Service (DDOS) but in distributed way; from different locations. |
| | Sybil | Using same identity, multiple accounts will be created. |
| | Malware | Attacker consumes network bandwidth by sending spam messages. |
| | Spam | Spam messages are sent in the network to consume bandwidth. |
| | Man in Middle | Middle malicious node has access to the communication in between two devices. |
| | Brute Force | Attacker uses trial and error approach to get access to password, identity or any protected data. |
| **Using hardware or software** | Spoofing & Forgery | Injection of wrong emergency warning messages for the user. |
| | GPS Spoofing | Attacks the GPS to mislead the network by wrong locations. |
| | Message change | Attacker either drops the packet or changes the contents of the packet. |
| | Replay | Reply to the old messages to mislead the network. |
| | Message injection | Attacker injects intentionally false information. |
| | Tampering hardware | Attacker tries to tamper the hardware. |
| | Routing | Attacker disturbs the routing by targeting network layer. |
| | Timing | Play with the time to delay the messages that should be received in the network when it is no more required. |
| **Attack to sensor input** | Illusion | Attack on the sensors to read wrong sensor readings. |
| | Jamming | Attacker attacks on radiofrequencies to create jam. |
| **Infrastructure attacks** | Unauthorized access | Unauthorized access deals with malicious access to any node, service or Network by any mean. During session hijack, attacker takes control of the session after authentication and controls the session in its own way. |

**In table 4.1,** we have summarized various attacks types and how each attack is carried out by the attackers.

## 4.2 Security Measures

Security is being implemented using three approaches; Using Security infrastructure, with security architecture and with the help of security standards. All three measures complement each other as infrastructure will help to design architecture and architecture will have set of standards to implement [13].For security infrastructure, concept of PKI exists that work with certificate authority CA to implement security. Based on PKI, many security architectures are being adopted by various originations to deal with security issues within their scope ETSI has introduced security for ITS communication ETS architectural layers [14].

NHTSA has introduced security architecture using basic safety messages and security information Messages based on bootstrap functions and pseudonym functions this architecture appears more secure as compared to others. Without standards and protocols, security cannot be implemented at all and more research is proceeding in this area to come up with more secure algorithms, standards and practices for network [15].

Support of cryptographic algorithm, routing protocol and certification authority together set the security of the network along with other optional security measures like data verification, detection rates, and involvement of specific authority, formal group formation, and location, architecture and individual access rights of a node within the network. So whatever security approach is used, focus is to avoid attack by targeting vulnerable threats available in the network and don't leave any loop hole for the attacker to intrude in the network and harm it with his malicious efforts, activities and actions [16].

# CHAPTER-5:
# ANALYSIS

## 5.1 Analysis

Security can be implemented on Text. Text security for simple user is to only follow officials account, trust only the member he/she knows and don't share private information with anyone. For high security, messages can be encrypted using Cipher, with any key, with hash code, message authentication code. We have tested an algorithm to encrypt and decrypt a textual file. Encryption of a data means converting the data from original form into a coded form. The coded form of original data can't be read by an unauthorized person. Decryption of a data means, converting data from coded form to its original form. Encrypted data can only be accessed by an authorized person. Authorized person knows the decryption key. Decryption key is a password or formula that is used to convert cipher text to plaintext. Encrypted data is known as cipher text, whereas decrypted data (original data) is known as plaintext [17].
Therefore in simple language, converting data from plaintext to cipher text is known as data encryption. Whereas converting data from cipher text to plaintext is known as data decryption.

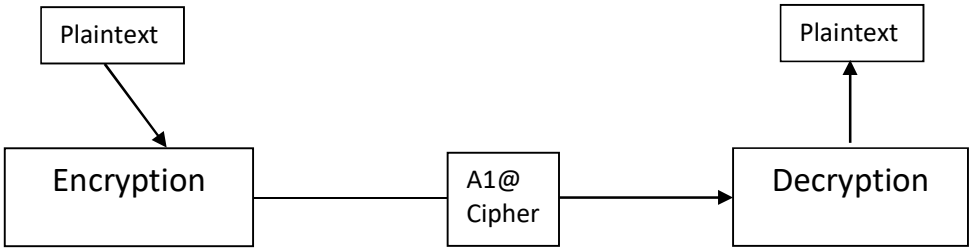


Figure 5.1: Encryption and Decryption.

**In figure 5.1,** The diagram shows encryption and decryption method.

## 5.2 Encrypt Message (Text File)

Step 1- Asks from user enter the name of file.

Step 2- Opens the file (in reading mode) entered by user.

Step 3- Creates a file.

Step 4- Reads content of file, in character-by-character manner.

Step 5- Reading the character.

Step 6- We have the same content as of the File. Instead each character is of ASCII value, example more than original one.

Step 7- Closes both the file stream.

Step 8- Opens the file, in writing mode.

Step 9- Opens the file in reading mode.

Step 10- Copies the content of file (encrypted content of file) file.

## 5.3 Decrypt Message (Text File)

Cipher text available in the file with decryption formula (subtracting 100 from each character), to decrypt the data of a file. After, when we opens the same file. Then our data will be in original form, or our data gets decrypted.

# CHAPTER-6:
# CONCLUSION & FUTURE WORK

## 6.1 Conclusion

Social media is used by diverse age groups but it is more commonly used by adults and females. Main concern is to protect user's security and privacy. This can be achieved by awareness to the common user about privacy options, with use of counter measures and adapting various security tools. During this study, we found that users are mostly attacked by browser, brute force, denial of service and malwares.

## 6.2 Future Work

In future, the following Security mechanisms will be studied

1. Digital signature, a type of electronic signature. It is a mathematical algorithm routinely used to validate the authenticity and integrity of a message.
2. Advanced Encryption System (AES), is a symmetric block cipher to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data.

# REFERENCE

[1]A. Doha, N. Elnahla, and L. McShane, “Social commerce as social networking,”J. Retail. Consum. Serv., vol. 47, pp. 307–321,Mar. 2019.

[2]Weaver, A.C, Social Networking,.,Computer (Long Beach, Calif.) ISSN: 0018-9162 Date: 02/01/2008 Volume: 41, Issue:2, Page: 97-100, DOI: 10.1109/MC.2008.61, IEEE Enterprise.

[3]Z.Zhang and B. B. Gupta, “Social media security and trustworthiness: Overview and new direction,” Future. Gender. Compute. Syst., vol. 86, pp. 914–925, Sep. 2018.

[4] W. F. Hsieh and P. Y. Lin, “Analyze the digital watermarking security demands for the Facebook website,” in Proceedings -2012 6th International Conference on Genetic and Evolutionary Computing, ICGEC 2012, 2012.

[5]http://www.btrc.gov.bd/?fbclid=IwAR02trvG196CMPUDMhAS0Kb06s_f9C0h-fpLl61ehcgSZpOBOfyrtsvjHx0.[Last accessed on June, 2022.]

[6] S. H. Han, and Chu, C. H, “Content-based image authentication: Current status, issues, and challenges,” International Journal of Information Security, vol. 9, pp. 19-32, 2010.

[7] P. Y. Lin, J. S. Lee, and C. C. Chang, “Dual digital watermarking for internet media based on hybrid strategies,” Circuits and Systems for Video Technology, vol. 19, pp. 1169-1177, 2009.

[8]S.Sicari, A.Rizzardi, L.A.Grieco,and A.Coen-Porisini,“Security, privacy and trust in internet of things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[9] J M Blythe, SD Johnson, The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices, March 2018,https://www.researchgate.net/publication/324088630.

[10]R.Rajadurai,N.Jayalakshmi,“Vehicular network: properties, structure, challenges, attacks, solution for improving scalability and security”, International Journal of Advance Research, IJOAR .org, Volume 1, Issue 3, March 2013.

[11] N.K. Chauley, “Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study”, International Journal of Security and Its Applications vol.10, No.5 pp.261- 274, 2016.

[12] H. Hasrouny, C. Bassil, A. Samhat, A. Laouiti, “Security Risk Analysis of a Trust model fzor Secure Group Leader-based communication in VANET”, Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC'2016.

[13] R. Raiya, Sh. Gandhi, “Survey of Various Security Techniques in VANET”, International Journal of Advanced Research in in computer Science and Software Engineering, Volume 4, Issue 6, June 2014.

[14] ETSI TS 102 867 V1.1.1- Security-Mapping for IEEE 1609.2

[15]P.Caballero_Gil,“Security_issuesin_VANET”,available:http://cdn.intechopen.com/pdfs-wm/12879.pdf, 2011.

[16]A.M. Malla, R.K. Sahu, “A Review on Vehicle to Vehicle Communication Protocols in VANETs”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[17]https://www.researchgate.net/publication/280556875_AN_ALGORITHM_ON_TEXT_BASED_SECURITY_IN_MODERN_CRYPTOGRAPHY?fbclid=IwAR0pEON1ZkRlJnNZ8lz2uHHx90nRlolJIy2FniesDcleZh_n_2fDJET1Rk4.[Last accessed on June, 2022.]