Data Encryption Techniques Utilized In Social Media Networks

Madhusanka D.N.V
IT20613518
Sri Lanka Institute Of Inforamtion Technology
Malabe, Sri Lanka
it20613518@my.sliit.lk

Badullege P.H
IT20613372
Sri Lanka Institute Of Inforamtion Technology
Malabe, Sri Lanka
it20613372@my.sliit.lk

Anuradha E.K.R
IT20297404
Sri Lanka Institute Of Inforamtion Technology
Malabe, Sri Lanka
it20297404@my.sliit.lk

Thisitha K.L.D
IT20618872
Sri Lanka Institute Of Inforamtion Technology
Malabe, Sri Lanka
it20618872@my.sliit.lk

Herath H.M.T.D
IT20627928
Sri Lanka Institute Of Inforamtion Technology
Malabe, Sri Lanka
it20627928@my.sliit.lk

***Abstract*— Social media enables users to quickly make and distribute content to the public. Social media includes a variety of websites and apps. Many people in the modern world utilize social media for a variety of purposes. As a result, malicious actors have a new surface to attack against because of social media. security teams need integrated external cybersecurity to prevent attacks and secure platforms. Social media networks utilize data encryption as a security measure to protect users' data.This research paper focuses on current data encryption methods, importance of data encryption for social media and popular social media platforms data encryption techniques.**

Keywords—Social media, Data encryption, Symmetric encryption, Asymmetric encryption, Plain text, Cipher text

I. INTRODUCTION

Data encryption changes data form into a different format. This format data can only be decrypted by someone who has the secret key. Before encryption, data called as plain text. An encryption method and encryption key are used to encrypt plaintext. The end consequence of this encryption operation is cipher text. The term "cipher text" refers to encrypted data. If the right key is used to decrypt it, this can only be seen in its original plain text. When digital data is being kept on computer systems and being transferred via the internet or other computer networks, data encryption is employed to protect its confidentiality. Modern encryption techniques have replaced the dated data encryption standard, which is necessary for the security of IT systems and communications (DES). (1)

This encryption algorithms provides confidentiality, integrity, authentication, and non-repudiation. By performing authentication, a message integrity can be verified. The sender of a message cannot change their acts because of non-repudiation. In modern world, encryption is one of the most popular and effective data security strategies used by businesses. The two fundamental techniques for data encryption are symmetric encryption and asymmetric encryption.

II. DATA ENCRYPTION METHODS

1) Symmetric encryption

Symmetric-key ciphers use the same secret key to encrypt and decrypt data. The recipient cannot decrypt a communication until the sender and recipient have exchanged the encryption key. symmetric key encryption is quicker than asymmetric encryption. (2)

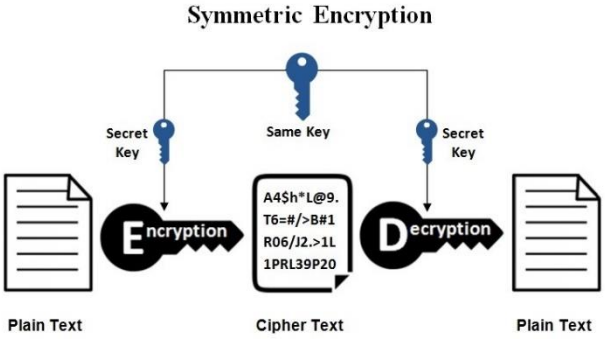
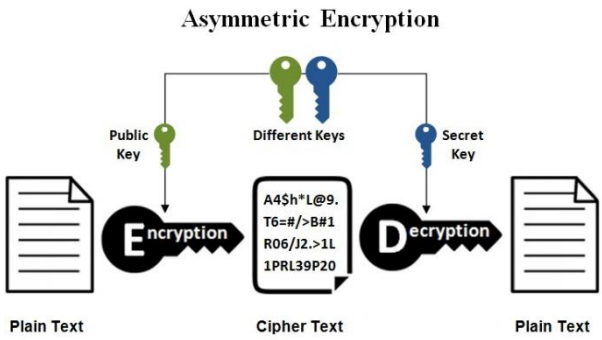


Figure1: shows symmetric encryption

The most widely used symmetric encryption algorithms are 3DES, AES, IDEA, Blowfish, Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), and Rivest Cipher 6 (RC6). (3)

2) Asymmetric encyption

Data is encrypted using two keys: a public key and a private key in asymmetric encryption. These two keys are mathematically connected. The user uses one key for encryption and the other for decryption, therefore it doesn't matter which key selected first.



Asymmetric encryption is used by the daily communication channels. Those channels are connected to the Internet. The elliptic curve methods, RSA, DSA, EIGamal, and PKCS asymmetric key encryption algorithms are well-known. (3)

III. IMPORTANCE OF DATA ENCYPTION

Encryption is crucial to each commercial enterprise these days as it allows them to guard private records with the aid of using changing it into ciphertext, a shape this is unreadable without an encryption key. This is called "Encoding." Encryption makes it almost impossible unimaginable for cybercriminals or other unapproved gatherings to take and abuse the information since just those with an encryption key can unravel the data and uncover the true data. In this topic, we are covering why importance of encryption. (4)

- *Protection from hackers*
- *Encryption protects privacy*
- *Encryption protects data across devices*
- *Maintain data integrity*

A. Social media importance

Social media enables you to connect, encourage, and engage with your interest group wherever they may be. When a company can connect with its audience through virtual entertainment, it can use that connection to generate brand awareness, leads, sales, and revenue. In today's environment, social media is everywhere. Popular platforms include Facebook, What's App, Instagram, Snapchat, Telegram and TikTok.

IV. SOCIAL MEDIA PLATFORMS DATA ENCRYPTION TECHNIQUES

A. Facebook

1) What is hashing?

Hashing is a one-way mathematical function that can't reverse. This is some kind of encryption but can't decrypt and get plain text. This hash function uses to ensure data integrity by using digital signature. Facebook employs the widely used SHA-256 secure hashing method, which is a standard in fields like online banking. Any email addresses or phone numbers from your list are first "hashed" locally on your computer before being sent to Facebook. As a result, Facebook only receives the hashed values and not the original list. (5)

2) Secured Connection

a) Digital certificates

A certificate contains information like the user's email address, country, and public key. In addition to the name of the business and the organization that issued also include in the certificate.

The opposite side answers to a network inquiry by sending a copy of the certificate when a server and client need to communicate. The public key of the opposite party is included in the certificate. A certificate can also be used to specifically identify its owner. SSL/TLS employs both symmetric and asymmetric encryption; take a quick look at digitally signed SSL certificates issued by credible certificate authorities. (3)

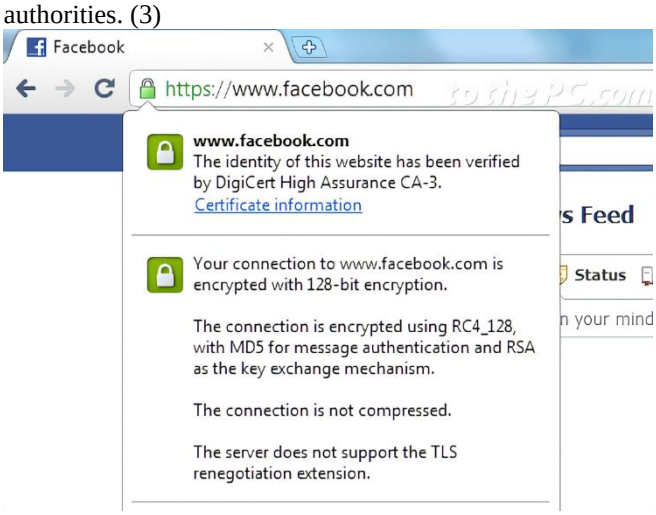


Figure 3: showing facebook encryption information.

B. Whatsapp

The most popular messaging app worldwide is WhatsApp, easily exceeding competitors like Messenger, Signal, and Telegram. The open-source Signal protocol from Open Whisper Systems has been a component of WhatsApp's end-to-end encryption technology since 2014. End-to-end encryption safeguards practically all user conversations on the platform. Calls, voicemails, media, status updates, and texts are included in this. (6)

1) What is end-to-end encryption(ETEE)?

Data cannot be accessed by other parties while it is being transferred from one end system or device because of end-to-end encryption (E2EE). This is a secure communication method. Data in an E2EE transaction is encrypted on the sending system or device and can only be decrypted by the designated recipient. Outside parties like internet service provider (ISP), an application service provider, a hacker, or any other communication cannot be read or changed while in transit. (7)

You may use WhatsApp to check the end-to-end encryption of your individual chats and calls. To verify that, simply tap the "Encryption" label after selecting the contact's name in a chat window within the app. A 60-digit number and a QR

code will be displayed to you. Compare the results after repeating these steps on the recipient's phone. (8)

Your chat is properly end-to-end encrypted as long as the number matches on both devices. (8)

C. Telegram

With improved encryption and privacy, Telegram is a free cloud-based instant messaging service that can be used on any devices. In addition, the service offers extra services including VoIP, file sharing, end-to-end encrypted chats, and video calling.

The basis for the encryption of Telegram messages is the Diffie-Hellman secure key exchange, 2048-bit RSA, and 256-bit AES encryption. Client-to-server encryption was once the norm for Telegram communications, however end-to-end encryption is now utilized for messages in Secret Chat. The MTProto protocol used by Telegram for its cloud messaging service encrypts data as it travels to its servers, and its end-to-end encryption for "Secret Chats" is also based on this protocol. No matter what kind of data it is - text, media, or files — it is all encrypted in the same way. (9)

On one of his devices, a user can start a secret chat with another user, but only that device can access the chat. This special feature called as device specific chat. Once the user signs out, all private conversations are lost. The user is able to make as many unique secret chats as they want with the same contact. When a secure conversation is formed, the participating devices exchange encryption keys via the Diffie-Hellman key exchange.
After establishing a secure end-to-end connection, the encryption system generates a picture that serves as the encryption key for user communication. If this image and the one that another user has are identical, the individual can be sure that the private discussion is secure. (9)

D. Snapchat

Snapchat is a well-known social media tool that lets users exchange material that is only kept for brief periods of time. For its data transmission, Snapchat employs SSL and TSL to ensure data integrity and privacy. Using symmetric key encryption and message authentication codes to guarantee integrity, all data sent over the internet is encrypted. Additionally, public key encryption is used to validate the identities of the persons conversing. The methods rely on dependable third-party certificate authority to confirm the validity of digital certificates, which are often used as evidence of public key ownership. (10)

V. CONCLUTION

The typical encryption techniques now in use have been researched and analyzed in this paper. Data encryption is critical thing in modern security. Therefore, Social media platforms also use data encryption techniques to secure users' data. This research paper mainly focuses on four main social media platforms data encryption techniques and their process. In addition, there are importance of data encryption.

VI. REFERENCES

1. GROOT JD. Digital Guardian. [Online].; 2022 [cited 2022 10 09. Available from: https://digitalguardian.com/blog/what-data-encryption.
2. Techslang. What is Symmetric Encryption? [Online].; 2022 [cited 2022 10 09. Available from: https://www.techslang.com/definition/what-is-symmetric-encryption/.
3. SSL2BUY. [Online].; 2022 [cited 2022 10 10. Available from: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences.
4. Robinson P. Lepide. [Online].; 2022 [cited 2022 10 10. Available from: https://www.lepide.com/blog/5-benefits-of-using-encryption-technology-for-data-protection/.
5. Facebook. Facebook. [Online].; 2013 [cited 2022 10 10. Available from: https://www.3qdept.com/wp-content/uploads/2016/06/facebook_audiences_data_security_overview.pdf.
6. Whatapp. Help Center. [Online]. [cited 2022 10 11. Available from: https://faq.whatsapp.com/791574747982248/?locale=en_US.
7. Lutkevich B. Tech Target. [Online]. [cited 2022 10 10. Available from: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE.
8. Wankhede C. Android Authority. [Online].; 2022 [cited 2022 10 10. Available from: https://www.androidauthority.com/whatsapp-encryption-safe-3087607/.
9. Bahar Z. NordVPN. [Online].; 2022 [cited 2022 10 10. Available from: https://nordvpn.com/blog/is-telegram-safe/#:~:text=While%20all%20Telegram%20messages%20are,end%20encryption%20is%20so%20important.
10. Snap Inc. [Online]. [cited 2022 10 11. Available from: https://snap.com/en-US/privacy/privacy-by-product.