International Journal of Scientific Research & Engineering Trends
Volume 9, Issue 3, May-Jun-2023, ISSN (Online): 2395-566X

The Evolution and Impact of Cryptography in Ensuring Data Privacy

Parth Mathur, Saksham Saxena, Yasha Mishra
Indore,MP,India
parth.mthur@gmail.com, Saxenasaksham202@gmail.com, yashansi0312@gmail.com

Abstract- Any type of digital information that is stored is known as data. To prevent unauthorized access to computers, websites, and personal data, we need protective digital privacy measures, which refer to data security. Cryptography is an evergreen security development used to protect our assets. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data, allowing us to save more data. Cryptography is essential for protecting users by providing authentication and data encryption. There are popular ways of cryptography for securely sending vital information. In the modern era of computers, cryptography has become a crucial tool to secure various types of digital data. Security of information, especially on the World Wide Web, is a significant concern, involving editing internal confidential documents, authentication during access, and ensuring integrity and confidentiality.

Keywords- Cryptography, Data Privacy, Security, Encryption.

I. INTRODUCTION

Data can be transferred via the internet, and compression is used to secure the data by reducing disk space usage and increasing transfer speed. Data security aims to achieve security goals such as authentication, confidentiality, non-repudiation, and integrity. Cryptography is increasingly adopted by IT organizations to protect valuable information and address growing security concerns. Challenges faced by IT organizations include the increasing costs of storage and the need to secure storage data while meeting current and future demands. Data compression is known for reducing storage and communication costs. The transformation of data from a readable state (source message) to a smaller-sized format (code word) is achieved through data encryption, which protects information from eavesdropping.

Encryption and compression methods are performed separately. In the pre- modern era of cryptography, the conversion of information from a readable state to apparent nonsense was synonymous with encryption. Modern cryptography is heavily based on computer science practice and mathematical theory, designed around assumptions of computational hardness to make breaking such algorithms infeasible through practical means, although theoretically possible. The growth of cryptographic technology has raised legal issues in the information age, leading many governments to classify it as a weapon and restrict its use and export, as cryptography also has the potential for espionage.

II. CRYPTOGRAPHY

The art of writing that is intended to be kept secret is considered the art of cryptography. As civilizations evolved, human groups, tribes, and kingdoms organized themselves, leading to battles, power struggles, politics, and the pursuit of supremacy. The continuous evolution of cryptography arose from the natural need of people to communicate secretly with selective recipients. The roots of cryptography can be traced back to Roman and Egyptian civilizations.The importance of communication and information systems for society and the global economy has intensified with the increasing quantity and value of stored and transmitted data. However, these data and systems are also increasingly vulnerable to various threats, such as alteration, destruction, misappropriation, and unauthorized access. Encryption refers to hiding information, while decryption refers to revealing hidden or previously encrypted information.

The transformation of plaintext (original text) into ciphertext (encrypted text) is accomplished using a cipher. Merriam-Webster's Collegiate Dictionary defines a cipher as "a method of transforming a text to conceal its meaning." The information being hidden is the plaintext, and once it has been encrypted, it becomes the ciphertext.Steganography and cryptography are two main techniques for hiding data. In this paper, cryptography is used as it is the science of protecting data and provides methods for converting data into an unreadable form, allowing authorized users to easily access the information at the destination. Cryptography utilizes mathematical principles for data encryption and decryption.

III. BASIC TERMINOLOGY OF CRYPTOGRAPHY

Millions of people use computers for various purposes such as student records, banking, military operations, and shopping, among others. Privacy is a critical issue in many

of these applications, and it is important to ensure that unauthorized parties cannot modify or read messages.

Cryptography is used to secure data and transform it into an unreadable form. The word "cryptography" comes from the Greek words "kryptos" (hidden) and "graphikos" (writing). It refers to the methodology of concealing messages. The information we want to hide is called plaintext, which represents the original text. It can be in the form of executable programs, numerical data, pictures, characters, or any other type of information. The ciphertext refers to the encrypted text that nobody understands except the intended recipients. Multiple algorithms can transform plaintext into ciphertext, creating data that can be transmitted through a network.

A cipher is an algorithm used to transform plaintext into ciphertext, and the process is known as encryption. It converts understandable and readable data into "meaningless" data. The encryption algorithm takes an input key and transforms the plaintext into ciphertext.

Different keys yield different ciphertexts. In decryption, the inverse of the key is used inside the algorithm to recover the plaintext. Information transmission over interconnected networks requires procedures and measures to protect data. Network security refers to activities designed to protect the reliability, integrity, usability, and safety of data during its transmission.

It involves both software and hardware components, such as firewalls, anti-spyware and antivirus software, virtual private networks, and intrusion prevention systems. Computer security is a generic term encompassing tools designed to protect data from corruption, natural disasters, theft, hackers, while ensuring data availability to users. Antivirus programs are examples of such tools.All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

IV. CRYPTOGRAPHY GOALS

Cryptography serves various goals, which can be achieved individually or simultaneously in a single application:

1. Confidentiality:
This is the most important goal, ensuring that only those with the decryption key can understand the received message.
2. Authentication:
It verifies the identity of the communicating entity, confirming that the system or user is who they claim to be. This allows entities to prove their identities to other parties who do not have personal knowledge of them.
3. Data Integrity:
It ensures that the received message has not been altered from its original form. Data may be unintentionally or intentionally modified by an unauthorized entity. The integrity service verifies the correctness of the data as long as it was last transmitted, created, or stored by an unauthorized user. Hashing is often used at both the sender and recipient sites to create a unique message digest that can be compared to ensure data integrity.

4. Non-Repudiation:
It provides evidence that the sender indeed sent the message, and the intended recipient received it. This prevents the recipient from denying that the message was sent, ensuring accountability. For example, if non-repudiation is enabled in a transaction, a purchaser cannot refuse the purchase order once it is placed electronically.

5. Access Control:
It prevents unauthorized use of resources by controlling who can access them and under what conditions and restrictions. Access control determines permission levels for accessing resources.

6. Data Encryption:
Data encryption involves the creation of a random string of bits to scramble and unscramble data. It ensures that each key used for encryption and decryption is unique and unpredictable. Cryptography employs two types of keys: symmetric and asymmetric.

V. SYMMETRIC KEY CRYPTOGRAPHY

It uses a single secret key for both encryption and decryption of ciphertext. Both the sender and receiver must possess the secret key to encrypt and decrypt messages. It is also known as private-key cryptography.

VI. ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography, on the other hand, utilizes a two-key system. One key is used for encrypting information, while the other is used for decrypting it. The computer automatically generates a private key, which is never shared, to encrypt a message. The recipient's public key is used to encrypt the information, and the recipient can decrypt it using their private key. This method allows both parties to communicate securely and maintain message confidentiality. It is also known as the public-key system.

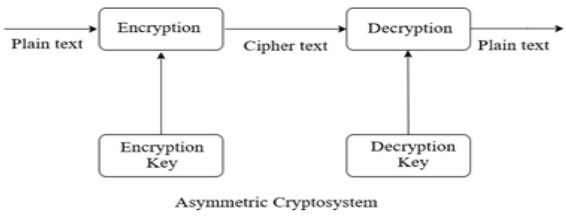

Fig 1. Asymmetric Cryptosystem.

VII. CONCLUSION

Cryptography is employed to ensure the confidential transmission of information without alteration. Only individuals possessing the decipher key can decrypt the received message. It serves goals such as confidentiality, authentication, data integrity, non-repudiation, and access control. Network security and computer security play vital roles in protecting data during transmission and storage.

Data encryption involves the use of symmetric or asymmetric keys to convert plaintext into ciphertext, and decryption is the reverse process of converting ciphertext back to plaintext.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who have contributed to the successful completion of this research paper.

REFERENCES

[1] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[2] J. Katz and Y. Lindell, Introduction to Modern Cryptography, London: Taylor & Francis Group, LLC, 2008.
[3] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability" in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.