EXPLORING THE APPLICATION AND DIFFERENT ALGORITHMS OF DATA ENCRYPTION

K P Saurabh
Research Scholar, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

Dr. Kailash Patidar
Supervisor, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

ABSTRACT
The emergence of China's computer sector in the 21st century may be attributed in large part to the country's fast technological advancements and its ubiquitous computer network. While there are many positive effects of computers on society, there are also many dangers. For instance, significant costs have been incurred by human civilization due to the loss or corruption of critical data, the leaking of private information, and the abuse of individual privacy. Maintaining computer network security and reducing the likelihood of information tampering or theft necessitates the development and effective application of data encryption technologies and an increased defensive line for computer network security. Currently, the most reliable method of ensuring computer security is to employ data encryption technology during the transfer of sensitive information.
Keywords: Technology, Computer Network, Plaintext, Database, Encrypted

I. INTRODUCTION

The search for the best solution to offer the necessary protection against the attacks of data thieves while also providing these services in a timely manner is one of the most active subjects in the security related communities due to the growing importance and value of data exchanged over the Internet or other media types.

Encrypting data means encoding it in such a manner that it can only be decoded, or accessed, by someone who has the corresponding encryption key. Unauthorized parties are unable to decipher encrypted information because it seems garbled. Encrypting data involves transforming it from its original, legible form into an unintelligible mess. This is done so that sensitive information can't be viewed by anybody while it's being transmitted. Almost everything transmitted across a network may benefit from encryption, including files, communications, and documents.

Encryption is a crucial technology whose importance cannot be emphasized in ensuring the security of our data. Whether it's a website or an app, almost everything we encounter online has been encrypted at some point. According to the experts at Kaspersky Lab, a leading provider of antivirus and endpoint protection software, encryption is "... the conversion of data

from a readable format into an encoded format that can only be read or processed after it has been decrypted."

They go on to state that encryption is the backbone of data security and is utilized by everyone from governments to corporations to individuals. It's the simplest and most important method of securing data in transit from client devices to backend servers. The increased risk of cybercrime nowadays means that everyone who uses the internet should be conversant with and use even the most fundamental forms of encryption.

II. DATA ENCRYPTION

Simply put, encryption is the transformation of plaintext into encrypted form. It also protects data when transmission via an unreliable wireless connection. This data bridges the gap between the two previously separate collections. An advanced type of encryption is used for the initial connection. This method is now often used to encrypt data in transit. Before information is sent, it is usually encrypted by the sender.

The foundation of encryption is made up of three main components, each of which has a specific function:

- Plaintext as an input.
- Encryption Algorithm as an interface.
- Cipher text as an output or desired result.

A data-protection algorithm is often known as an encryption key. Every algorithm uses a "key," or a series of bits, to do the calculations. The more you think about it, the more you realize how tough it is to decipher the code and figure out what it means.

Encryption is the process of encoding data or information in a way that makes it unreadable to a third party. Typically, a parameter or key is used to encrypt the data before it undergoes the transformation. It's important to note that not all encryption algorithms require a key of the same length as the encoded information; some may be optimized for use with much shorter keys. It's often held that encryption and decryption are diametrically opposed processes. If you encrypt some information and then decode it, you'll get back the original data.

Encryption is an indispensable tool for today's advanced civilization. It is most typical to use encryption while conducting business through an unsecured medium of communication like the internet. Cryptography is used to protect data in transit between devices such as ATMs, mobile phones, and other similar devices. By utilizing encryption, it is possible to create digital signatures that may be used to confirm the legitimacy of a communication. When used properly, a digital signature can provide the receiver of a message the assurance that it came from the purported sender. Digital signatures are a useful tool for facilitating email and other types of electronic communication. Like traditional handwritten signatures, a signature that is more difficult to forge is a signature that is created in a more complicated manner. The two most popular forms of encryption are symmetric and asymmetric.

Importance of Data Encryption

When it comes to safeguarding data on the internet, both public and private networks rely heavily on encryption technologies. It is essential that sensitive information such as emails, medical records, trade secrets, consumer purchase habits, legal documents, credit histories, and government and regulatory agency databases be kept safe. Maintaining a feeling of safety while exchanging sensitive personal and business information depends on the integrity of this data. US law requires that all electronic communications be encrypted using government-approved

methods. Companies that provide services to the government, such as IT integrators and contractors, are increasingly seeking NIST accreditation in order to compete more effectively in government IT procurement. There is significant opportunity for VARs working with the government to implement NIST-certified AES technology into legacy IT systems beginning in 2005. Commercial sectors seeking the highest degree of data encryption and privacy, in addition to the government sector, are predicted to increase their demand for AES-certified equipment.

The information we have collected over the past few decades has become the most precious commodity of our time. When there is a strong demand for data, it means that people and organizations are prepared to pay to learn more about a topic. Encryption was the standard means of communication back when a third party could not listen in on a discussion between two people without using special software. Encryption is used for more than merely communicating securely; it also safeguards information from malicious parties like hackers. Companies that use digital technologies have a heightened awareness of the threats presented by cybercriminals, and as a result, they are more likely to use encryption, a relatively new method for keeping sensitive information safe.

III. APPLICATION OF DATA ENCRYPTION TECHNOLOGY IN THE COMPUTER SECURITY

The application of data encryption technology in database encryption

When compared to a regular file, a database is unique in that it stores many different kinds of data in a unified structure and can encrypt the entire thing by itself. Different from other common data encryption methods, database encryption necessitates specific hardware (a database that is built directly into a hard disk) and software (an OS that can be run on any computer). Database encryption is used primarily to stop unauthorized individuals from stealing, altering, or erasing critical information while yet allowing authorized users' access to proceed normally. Therefore, the primary requirement of data encryption technology is to ensure the safety of the data. Quick access: if a valid user is using the database, and each action includes the process of file encryption or decryption, then the execution efficiency will suffer. This is why the database's data encryption has to employ a quick random access mechanism. Capacity for storage: if the database has to store too much information, which takes a lengthy time, it makes it more vulnerable to unlawful access. Since ensuring the frequent replacement of keys is crucial, it is imperative that the encryption used for database storage employ a high-efficiency method. When encrypting a database, it's important to keep the data's structure in mind; however, if all the databases share the same key, it's simpler for criminals to figure out how to decrypt the data using a statistical rule. To prevent this, it's best to give each encryption unit its key.

The application of data encryption technology in the software encryption

Software engineers put in long hours perfecting their craft, which is why so many of them are focusing on encryption these days. There are two primary types of encryption, hardware and software, and both are used extensively in the industry. As a matter of fact, it's a matter of public record that the majority of the people who use the Internet are not as technically savvy as they claim to be. However, it is not possible to rapidly update software through the Internet if hardware manufacture is not optimized for controlling or extracting information from software developers. The most common method of software encryption involves entering a

serial number or activation code before using the program. Software can access information about the host ID of a computer and send it to software service providers over the internet. The software service providers can then use data encryption technology to generate a serial number or registration code that is specific to the host ID and send it to legitimate users over the internet.

The application of data encryption technology in e-commerce

In the course of conducting business online, it is crucial to guarantee the authenticity of both the transaction's subject and its goal, as well as the confidentiality of any personal information exchanged. The first assurance of electronic commerce is the ability to verify the legal status of the other party through the use of encrypted data. It's fair to assume that the user's private key is accurate, as it's the only way to know for sure. If the information's decryption can legitimately verify the sender's identity using the sender's public key, then the information is allowed to be encrypted using just the sender's public key. Digital signature technology is useful in data communication because it ensures that both parties involved have seen and understood the same information. The sender transmits a digital signature along with the data they wish to share, and the recipient uses the public key provided by the sender to decipher the signature and obtain the data. Because the technique employed is the same and the information content obtained is constant across the two sides, it is difficult for outsiders to disguise the transmission of encrypted data. The digital signature of both parties is encrypted with the sender's private key, others do not have access to the private key, and the digital signature cannot be faked; the sender's public key is public, so the certification institution can use this public key to decipher the digitized signature. This is similar to a managed approach, where the digital signature and information are submitted to the authoritative legal certification bodies.

IV. DATA ENCRYPTION METHODS

Triple DES

The Data Encryption Standard (DES) algorithm is the foundation of 3DES, often known as DES. The DES algorithm uses a 56-bit key to encrypt and decode 64-bit blocks.

Since the same key is used for both encryption and decryption, the two processes are symmetric. However, the 16 center repeats in decryption are performed in reverse order to preserve symmetry.

The NSA has specified that only 56 bits of key length be used in the DES symmetric block cipher in the United States. The remaining 24 bits are not used in any way, and only 8 are used for parity. The block size in 3DES stays at 64 bits but the key length is increased to 112 bits or 168 bits. After brute force attacks and cryptanalytic operations penetrated DES, a new block cipher, 3DES, was developed to fix the problem without rewriting or updating DES.

RSA

RSA (Rivest-Shamir-Adleman) uses prime numbers to generate a pair of keys, one for encryption and one for decryption (the private key). It is the private key that is used to decrypt information that has been encrypted using the public key.

Blowfish

It has been documented how to implement an algorithm with a key length range of 32 bits to 448 bits and a block size of 64 bits. It was created by Bruce Schneier in 1993 to compete with the existing encryption methods (DES and IDEA) that were slow and expensive. To encrypt

and decode information, a Feistel Network with 16 rounds is utilized.

International Data Encryption Algorithm (IDEA)

In the year 1991, the first time the term "cyberspace" was used, the term "cyberspace" was used to describe the Internet. Since then, the term "cyberspace" has come to mean the Internet. The IDEA algorithm is used to encipher the plaintext into a 64-bit block ciphertext. The key size is 128 bits. The method consists of eight identical iterations plus a ninth iteration that performs a "half" change. Since more recent cryptosystems like AES employ 128-bit blocks, IDEA is now considered to be rather out of date.

AES

This is one of the best methods for protecting sensitive information, and it can be implemented in both hardware and software.As a block cipher with 128 bits, AES does not require a Feistel key. The "As a matter of fact" key size used by the technique is 128-192 bits or 256 bits if the number of rounds is 10, 12, or 14.

V. DIFFERENT ALGORITHMS FOR DATA ENCRYPTION

RSA Cryptosystem

RSA is one of the first and most used methods of public-key encryption. The encryption and decryption keys can be kept in isolation using this method. The factoring issue, which is the difficulty of factoring the product of two large prime numbers, is responsible for the RSA requirement of parity. In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman made the discovery public. Their last names were combined to create the acronym RSA.

Elliptic Curve Cryptography

The ability to develop smaller, more efficient and more trustworthy cryptographic keys with the help of the elliptical curve cryptography technology is the key to success. ECC makes use of the properties of the elliptic curve equation as an alternative to the conventional method of key generation, which involves multiplying together extremely large prime integers. It's possible to use RSA and Diffie-Hellman cryptography with this system. Some researchers believe that ECC can offer security comparable to that provided by systems with a key length of 1,024 bits.

Cuckoo Search Algorithm

The heuristic algorithm finally came face to face with nature. Xin-She Yang and Suash Deb created Cuckoo in 2009. CS was inspired by both Lévy flying random walks and the brood parasitism of many kinds of cuckoo birds. Cuckoos have captivated scientists for decades due to their seemingly endless capacity for reproduction. To improve their chances of hatching, certain females of a species place their eggs in the nests of males of the same species. The cuckoo is one beautiful bird. Both their attractive sound and their disputed approach to replication contribute to their attractive appearance. Brood vermin refers to this species for its habit of laying eggs in structures constructed by humans.

VI. CONCLUSION

Since the purpose of data encryption is to safeguard the privacy of its users, even a simple keyword search on the encrypted data is next to impossible. Plaintext searching requires downloading and decoding the material first. Despite its simplicity, this method places a significant computational and communication burden on the user, reducing the perceived benefits of cloud computing. Encrypting data is beneficial to the cloud service provider since it reduces the burden on the provider's infrastructure. The widespread adoption of data

encryption technology, which is slowly making its way into fields including academia, healthcare, the financial sector, and the power industry, not only gives peace of mind for businesses and governments, but also safeguards the lives of ordinary citizens.

REFERENCES: -

1. Wang, Meilin. (2022). Application Research of Data Encryption Technology in Computer Network Information Security. Security and Communication Networks. 2022. 1-7. 10.1155/2022/6485195.
2. Zhang, Na. (2021). Research on the Application of Data Encryption Technology Based on Network Security Maintenance in Computer Network Security. Journal of Physics: Conference Series. 1744. 022060. 10.1088/1742-6596/1744/2/022060.
3. Krishna Chaitanya, Nosina&Suman, A. (2020). Simple And Efficient Data Encryption Algorithm. International Journal of Scientific & Technology Research. 8. 2520-2523.
4. Kumar, Sonu&Patidar, Kailash&Kushwah, Rishi &Chouhan, Sudeesh. (2017). A review and analysis on text data encryption techniques. International Journal of Advanced Technology and Engineering Exploration. 4. 88-92. 10.19101/IJATEE.2017.430003.
5. Singh, K. &Rajkumar, Manimegalai. (2015). Evolution of encryption techniques and data security mechanisms. 33. 1597-1613. 10.5829/idosi.wasj.2015.33.10.286.
6. Huang, Yi-Li & Dai, Cheng &Leu, Fang-Yie& You, Ilsun. (2015). A secure data encryption Method employing a sequential-logic style mechanism for a cloud system. International Journal of Web and Grid Services. 11. 102. 10.1504/IJWGS.2015.067158.
7. Kapoor, Bhushan&Pandya, Pramod. (2013). Data Encryption. Computer and Information Security Handbook. 663-687. 10.1016/B978-0-12-394397-2.00037-4.
8. Kenekayoro, Patrick. (2010). The data encryption standard thirty four years later: An overview. African Journal of Mathematics and Computer Science Research. 3. 267-269.
9. Bouganim, Luc & GUO, Yanli. (2009). Data Encryption.