Understanding the Concept of Data Encryption in Network Security: Review of Types, Algorithms and Methodologies

Mr. Vivek Sharma
Assistant Professor, Department of Computer & Communication Engineering,
Manipal UniversityJaipur, Rajasthan (India)

Abstract: - Data encryption is the process of security method which is also used to provide security in network. There are many security methods available. Data encryption is the latest and most commonly used security method in order to protect the data and sensitive information of the user. It depends upon the technical team to choose the best network security method so that they are able to protect the data and information of the organisation. The technical team need to understand the business goals and objectives and based upon the type of data and information of the organisation, should select the best and efficient network security methods which is also one of the major challenges of the team. The objective of data encryption is to encrypt the data in such a way that it is not easily understood by the anyone else other than the person who is authorised to have access and also have the key to access it. It is one of the best methods of data encryption. The paper will discuss the importance of data encryption, the methodologies available and also its benefits as well as challenges.

Keywords: - Introduction to data encryption, Types of data encryption, Methodologies, Advantages of Data encryption, Challenges and Limitations of Data encryption methods.

*****

Introduction: - [1]

In today's world of latest technologies and techniques, almost all the tasks and projects are done online using internet. It is important to have strong and continuous internet connectivity so that all the tasks can be conducted without any issues. Since, all the work is done online, there are also chances of the leakage of data and information and the sensitive and critical data have high risks involved like being attacked by intruder, hacker, cyber crime etc. Therefore, it is essential that the data and information which is exchanged through network should be protected in such a way that it is not easily attacked by the hacker. A variety of safety and privacy protocols are available to protect the data and make it safe to use. One such technique is data encryption. It is the technique of converting the actual data into a format which cannot be understood by the hacker. The sender sends the data in encrypted form to the receiver. The receiver will then convert it or decrypt it using the special key available with him. This way only the sender and receiver who have access to the special key can only access and encrypt and decrypt the data. The encrypted message usually looks like a long sequence of alphabets and numbers which is not possible to convert into the actual data, hence, securing it from the intruder attacks. The main element of data encryption is the proper encryption of the data which will make sure that if in case it is accessed by an unauthorised user still, he will not be able to understand it. This is due to the fact firstly; it is sequence of alphabets and numbers which is not easy to understand and also the unauthorised user will not be having the unique key to decode it. In a network, following elements should be made secure and safe using encryption: -

- The communication and the files which are transmitted in a network like e-mail FTP etc.
- The confidential data and also its back up.
- All the databases which is available in the servers of the organisation.
- All the devices which are portable for example tabs, phones, mobile devices, systems, laptops etc.

Importance of Data Encryption: - [2]

It is very important that the organisation should make sure that the data and information present in the business is secure and maintains its privacy so that the clients also does not loose trust in the business. It is very important to encrypt the data due to the following reasons: -

a. Security: -

- Making sure the that the data is safe and secure will help the organisation to protect the data from loose ends while the data is stationary or is being transmitted.
- For example, if the sensitive data containing pen drive or hard disk is lost, still it will be sure that the data will not be attacked as it is present in encrypted form in the hard disk.
- Encryption also helps to communicate or transfer the data without the fear of it getting hacked or also protects it against malicious activities.

b. Compliance: -

- Now-a-days it is a rule and policy which is made by the government which states that the business and

organisations which are having user's data and information should use proper data encryption techniques to ensure security and privacy of the data.
- For example, the compliance which enforces data encryption are HIPAA, GDPR etc.

c. Authentication: -
- Data encryption also make sure that the authentication of the data is maintained.
- It is possible with the use of public key and a private key.

d. Privacy: -
- Data encryption make sure that nobody is able to access or see data except the authorised user which has the keys to decrypt it.
- This will make sure that the data is safe from being attacked by intruder, hacker, internet service providers, spammers as well as the government from reading or accessing the personnel data and information.

Specifications/Requirements of Data Encryption: - [3]
Following are the special requirements to implement data encryption process: -
- Database servers: - All the database which is used to store the data and information of the user must be in alignment with the FIPS 140 which is Federal information processing standard.
- Data files and folders: - Secure sockets layers are present in the web-based tool which are used to transfer the data files and folders.
- Storage Devices and back up data: - Encryption programming that is on the National Institute of Standards and Technology's (NIST) endorsed merchant list should be introduced on each gadget on which classified information is put away.

Types of Data Encryption: - [3]
There are many types of data encryption techniques available. Broadly they are divided into following three types: -

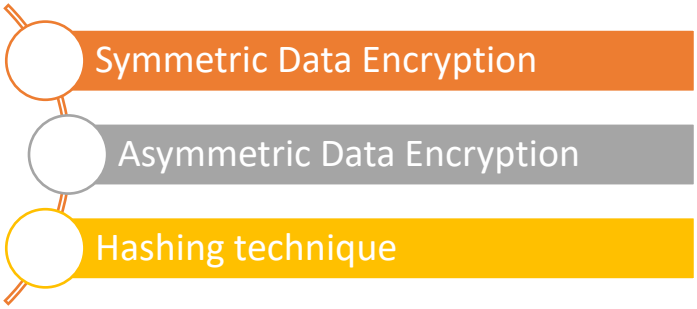

Figure 1 Types of Data Encryption method.

1. Symmetric Data Encryption: -
- This is also known by the name secret key algorithm or private key algorithm.
- The main objective of this technique is that both the sender and the receiver involved in the data transfer should have same unique key and can be accessed by both the parties.
- This method is used for a closed system. The receiver must have the private key so that they are able to access and decrypt the data.
- It is faster technique than any other technique but the drawback is that is the key is lost then they will not be able to access or it might be with hacker and he can misuse it.

2. Asymmetric Data encryption technique: -
- This method is also known by the name public-key cryptography.
- In this method two types of keys are used which are public key and private key which are connected to each other.
- One key is used for encrypting the data and the other key is used to decrypt the data.
- The public key is unreservedly accessible to anybody, though the confidential key remaining parts with the expected beneficiaries just, who need it to interpret the messages. Both keys are just enormous numbers that aren't indistinguishable yet are matched with one another, which is where the "unbalanced" part comes in.

3. Hashing data encryption technique: -
- Hashing is the technique which is used to generate a unique signature which contains fixed number length composed of numbers and letter for the data message.
- Each data message will have its own unique hash but the data which uses hashing cannot be converted into its original form.
- Due to this reason, it is only used to validate the data and it is not so commonly used for data encryption process.

Data Encryption Algorithms/Methodologies: -
Following are few available algorithms used for data encryption techniques: -

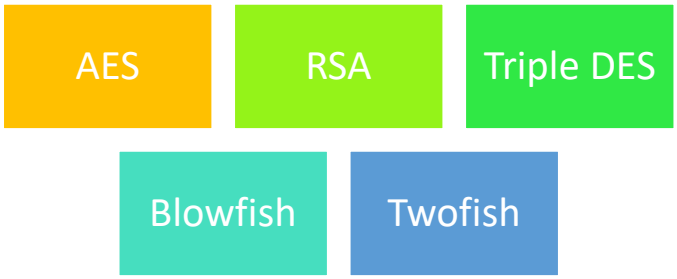

Figure 2: Types of Data Encryption algorithms.

1. AES (Advanced Encryption Standard): -
   - It is standard trusted algorithm which is widely used by state governments and many organisations.
   - The key formats used in this algorithm starts from 128-bit form, 192 form and 256 bit key.
   - Number of transformations are defined in data stored in the array.
   - The primary modification in the AES encryption method is done by replacing the information utilizing a replacement.
   - The modification is performed on each section utilizing other encryption key. Longer keys need more adjusts to finish.

2. RSA (Rivest- Shamir-Adleman): -
   - It is type of public key encryption asymmetric algorithm and is a standard which is used to encrypt information which is transmitted using internet.
   - It cannot be easily hacked or cracked by the hacker as it used gibberish format which takes a lot of time and effort by the hackers to crack it due to which hackers gets confused and tired to try to intrude the data.
   - In this method two different keys which are public and private keys are used to encrypt and decrypt the data.

3. Triple DES: -
   - This method is enhanced form of DES algorithms. This method is introduced as few hackers were able to crack the DES algorithm.
   - This technique uses the simple DES algorithm three times as the name suggests. It is applied in each data set.
   - It is used to encrypt UNIX passwords and ATM pins.

4. Blow Fish: -
   - This method is also used to replace the DES algorithm. In this method each data block is divided into 64-bit blocks and then encryption method is applied to each one of them.
   - It is popular for its speed, flexibility and cannot be easily hacked by the attackers.
   - It is mostly used in e-commerce platforms, to secure the online payments, and password management tools.

5. Twofish: -
   - Twofish is the replacement for Blowfish algorithm. It's sans permit, symmetric encryption that interprets 128-cycle information blocks.
   - Also, Twofish consistently encodes information in 16 adjusts, regardless of the size of the key. Twofish is ideally suited for both programming and equipment conditions and is viewed as one of the quickest of its sort.
   - Large numbers of the present record and envelope encryption programming arrangements utilize this technique.

Advantages of Data Encryption: - [4]

Following are few benefits of data encryption method: -

1. Low-cost implementation: - Data encryption is cost effective as most of the devices these days comes with the encryption methods which are in-built. For example, Microsoft windows provides program known as Bit locker.
2. Beneficial to remote workers: - The data and information is at risk when the employees are working from remote locations which is due to the fact that these employees save the data on their personnel devices. To overcome this, the encrypted data will be beneficial and also the employees should use VPN fir the security of the data.
3. Data integrity: - It is used to provide data integrity for the back up data. The integrity of the data which is in transit can be maintained by using digital signatures.
4. Improved customer trust: - If the customer knows that the organisation is using data encryption techniques than their trust in the business will increase and this way business will be able to retain the existing clients and attract more new clients.

Limitations of the Data Encryption techniques: -

Besides the advantages of the data encryption techniques, there are following challenges: -

1. Data recovery issues: - The challenge is to recover disk data where full disk encryption is done. For example, single file recovery like PST recovery is difficult to perform.
2. Slow speed of computer: - The speed to the computer is slow down due to the fact that each time we need to access file from the disk, it will involve decryption using key.
3. No security of data in transit: - The first is that it can't safeguard the information on the way. To be explicit, in

the event that you are dividing information among gadgets or sent information through messages, the information in communicate isn't being safeguarded. Programmers can take it easily.

Conclusion: - Information encryption is the course of safety strategy which is additionally used to give security in network. There are numerous security strategies accessible. Information encryption is the most recent and most generally involved security strategy to safeguard the information and delicate data of the client. It relies on the specialized group to pick the best organization security strategy so they can safeguard the information and data of the association. The specialized group need to figure out the business objectives and goals and in light of the sort of information and data of the association, ought to choose the best and productive organization security strategies which is additionally one of the significant difficulties of the group. The goal of information encryption is to scramble the information so that it isn't handily perceived by the any other individual other than the individual who is approved to approach and furthermore have the way to get to it.

References: -

[1]. https://www.cdc.gov/cancer/npcr/tools/security/encryption.htm#:
[2]. https://www.simplilearn.com/data-encryption-methods-article
[3]. https://www.cloudflare.com/en-in/learning/ssl/what-is-encryption/
[4]. https://www.lepide.com/blog/5-benefits-of-using-encryption-technology-for-data-protection/
[5]. https://teachcomputerscience.com/encryption/