International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

Cryptography in Database Security

Sai Santhosh M L iamsaisanthosh@gmail.com
Seema A M Seemaam30@gmail.com
Supriya T R Raghupriya1997@gmail.com
Associate Prof. Dr. Suma S Suma-mcavtu@dayanandasagar.edu
Dept. of MCA
Dayananda Sagar College of Engineering
Bengaluru, India

***Abstract* –This is the time where Internet is ruling the world. Anyone who uses internet do not encourage the hackers or anyone who are irrelevant to read our messages or get our data. The need for this secured transaction of data is not a new concept, it was needed even when messenger used to carry messages across the town. Our important and private things are on the internet. It may be our banking related data, private images, etc. which is a threat to our privacy. Therefore, security is as important as the internet in the world. The security can be ensured for all our activities and communication through cryptography. Cryptography which is used as a method of security is not a new concept. This method is very ancient.**

***Keywords* - Cryptography, Encrypt, Decrypt, Cipher text, Cipher Database, Key Management, Hashing, Database Encryption, Security, Encryption Algorithms.**

I. INTRODUCTION

Today we are in the internet age where every day we turn on the internet before doing jobs. From news, entertainment, social life to our profession is with our internet. The news that we read in newspapers, watching television sometimes feels very ancient compared to the usage of the internet for news and YOUTUBE for entertainment. Our social life is mainly vested on the internet and without it forming new friendships is very difficult as generations are passing. We don't want the hackers or anyone who are irrelevant to read our messages or get our data. The need for this secured transaction of data is not a new concept, it was needed even when messenger used to carry messages across the town.

Let it be any medium for transmitting our information without security it's always a nightmare for any further communication. Imagining bank account hacked and emptied can give a heart attack to many or company's data in others hand can wreck the company or maybe a nation's secret data in the hands of a terrorist is enough to cause destruction to many lives of that nation. Our important and private things are on the internet. It may be our banking related data, private images, etc. which is a threat to our privacy. Therefore, security is as important as the internet in the world. The security can be ensured for all our activities and communication through cryptography.

II.CRYPTOGRAPHY

Cryptography which is used as a method of security is not a new concept. This method is very ancient. During ancient times, when there were no digital means of transmission of information people used secret codes and keys in their letters to hide the information from falling into wrong hands (unauthorized person or intruder). This gave rise to the technique of cryptography. The word cryptography is a Greek word that can be spilled into two main parts: 'cryptos' meaning hidden or secret and 'graphein' meaning 'to write'. During world wars, when the computer was used for sending and receiving the information further ways of sending the secret messages through digitalization started popping giving way to our present modern cryptography.

1. Symmetric key cryptography

In this cryptography, the sender and the receiver have the same key that is the key used to encrypt and decrypt are the same. Here the key has to be kept between the sender and receiver. This is also called private key cryptography. Block and stream ciphers are a part of this cryptography. Block ciphers have a fixed length of characters whereas stream ciphers have a continuous set of symbols or characters. Here there is a risk when the key is known to the unauthorized person.

2. Asymmetric key cryptography

In this cryptography, there are two different for sender and receiver that is the encryption and decryption keys are different. This is also called public key cryptography. Here two pairs of keys are used. one is private key known only to the owners of the message and public key to check to whom this message has to be matched in order to be received.

III.CIPHER

Cipher is resultant got after the encryption algorithm is applied to the data that has to be encrypted. These are usually in an unreadable format. The cipher mainly

depends on the key that is applied to the plaintext during encryption. The ciphers can be categorized into block and stream ciphers depending on the length or number of characters or symbols. Popular ciphers are as follows.

1.**Substitution ciphers**- Here the plaintext is replaced with the encryption key. It can be letters, numbers of any varying length. This is also called Caesar ciphers.

2. Polyalphabetic ciphers- This cipher was developed from substitution ciphers to increase complexity a group of alphabets was substituted in plain text. This is also called Vigenre ciphers.

3. Transposition ciphers- Here the letters in the plaintext are arranged in different order. Usually, this is a keyless cipher. This is also called rail fence ciphers.

4. One time pad ciphers- OTP is very difficult to crack and requires a one-time key that is needed to crack it. The key can be of the same length of the message or different.

5. Modern ciphers- The modern ciphers vary depending on the modern algorithms (DES, AES, etc.) used. They may be a combination of above ciphers or different depending on the algorithms.

IV. ENCRYPTION

Encryption is a method of converting the plaintext into an unreadable text (cipher). The encryption uses a key to transform the text into cipher. When the text is received by the unauthorized person he can't read unless he has the key for turning back into a normal text. This method is used in many of the social media messaging application, banking applications, and business application today. The encryption is divided into private and public key encryption.

1. Popular encryption algorithms

1.1 AES- The Advanced Encryption Standard is an algorithm which is used by the USA government first. This very popular algorithm that uses a block size of 128 bits and the key size of 128,192 and 256 bits for encryption.

1.2 DES- The Data Encryption Standard algorithm is a symmetric key algorithm that uses a key size of 56 bits and a block size of 64 bits for encryption.

1.3 DES- This is Triple Data Encryption Standard algorithm where the symmetric block size of 64bits and a key size of 168 bits, 112 bits, and 56bits. Here the block key algorithm is applied three times to each block of data.

1.4 Blowfish- This is also symmetric key algorithm which is substituted for the DES algorithm. The block size is 64bits and the key size is 32 to 448 bits.

1.5 Two fish- This is related to the blowfish algorithm and one of the AES passing algorithm. The block size is 128 bits and the key size is 128, 192 and 256 bits.

1.6 RSA- The Rivest–Shamir–Adleman algorithm is the first and most popular public key encryption algorithm. The key size is 1024 to 4096 bits.

1.7 RC- The Rivest Cipher is a series of algorithms developed. They are symmetric stream algorithms and block algorithms. The recent is the RC6 algorithm with block size is 128 bits and key size is 128, 192 and 25bits.

V.DECRYPTION

Decryption is the reverse of encryption. The text that is in unreadable format is converted back into plain text.

VI. KEY MANAGEMENT

The key in cryptography is a set of characters or string of letter that is applied on the normal text during encryption to get cipher text and vice versa in decryption to get plain text. Key management is a way of handling and administering the keys.

This is very important in cryptography as without proper monitoring the key can be handed to an unauthorized person making it risky or there are chances of losing a key. These keys are very specific data and key administering is involved different processes like technical control of hardware used for the key generation, procedures, and policies required for key usage, and, human and environmental factors should also be considered. Every key created follows a life cycle which is key generation (key is created), key establishment (process of confirming whether the keys have reached their usage ends), key storage (key is kept safe and even a back is kept) and key usage (tells how keys should be used and also exchanged). The public and private keys are managed differently. Since public key has two keys, it usually has a hierarchical digital structure for its management.

VII. HASHING

Hashing is a process where the plain text is converted into a very unique string of text or characters. The hashing function is usually a mathematical operation done on the text. The hashed string may be of the same length of characters as the plain text or different. The major difference between hashing and encryption is the hashed text cannot be converted back into plain text. Since hashing is usually done on passwords. When a password is entered that is processed by the hashing algorithm and checks the result with the stored hashed value. If both match then the user is given access. There are risks in this hashing as the hacker who knows the password can easily get access to the message or data, to avoid this there is a

method salting where more string or information is added to the hashed value. To protect it even further the pepper can also be added only to the salted hashed value and the pepper has to be the same for all the websites.

VIII. DATA BASE ENCRYPTION

Database encryption is a process of encrypting the database using the algorithms to secure the database from an unauthorized person who can be malleolus. Database encryption is the best measure we secure data in the case where the unauthorized has got to database.

IX. NEED FOR DATABASE ENCRYPTION

Internet has a lot of data and information stored that needs to be protected. A database is a way in which the data and the information is stored, retrieved, processed and exchanged. Many of these databases are very crucial for many IT structures around the world. The security in this matter is about authentication and authorization that is checking whether the database is in right hands and giving access to only to those right people or company respectively.

The database is very delicate and usually databases include investment details, taxation details, project details, medical records, banking information and much other information which when manipulated is destructive to the company or the individual to whom that database belong. Not only this most of the time databases are linked to one other and manipulations in one database can change the whole result whether desired or undesired depending on who is handling it. The emergence of cloud computing has further changed the view of the internet by putting even the services on the internet and creating a situation where the security of this databases and services are very crucial.

By encrypting the data before storing into the database we can provide the security. Just the data encryption has the disadvantages where data ends up with an unauthorized person. If the unauthorized person gets access into the database then the chances of undesired manipulations are what can be expected. If this the situation then databases encryption is very important.

X. METHODS OF DATABASE ENCRYPTION

1.External/transparent encryption- This encryption is used for the data that is stored on the storages devices and also backup data storages. This encryption does not work on the data that is used or processed. Transparency means the data is encrypted or decrypted depending on whether it is loaded into the system or stored back. For this encryption, there is no need of any changes of applications that handle the data for its correct process and also encryption here also done simultaneously on the backup storage saving the time to do it separately. This encryption is called TDE and this works on page level which helps to decrypt the data when the system calls it for any process. The symmetric key encryption is used here.

2.Column level encryption- Every database is divided into rows and columns. The columns of this database hold the major attributes for each of its rows. These attributes are delicate and, when manipulated can lead to an undesired result. In order to protect we can use column level encryption. The major advantage of this encryption is the flexibility it provides to choose the columns that need the encryption and ones that don't. It can be transparent and also different keys for each column can be used while encryption.

3. File-level encryption- This is a type of encryption where the files on the system or the storage area are encrypted by the file system of the operating system. Since the databases are managed by the DBMS software running on the operating system encryption and decryption of the files is handled by the operating system itself. This encryption is not handled by the database but file encryption system of the operating system.

4. Disk-level encryption- This encryption is done on the whole disk or storage device. This is done by the particular software or hardware on every little data on the storage disk. All the unauthorized access to the storage is cut off here. The disk encryption is a real-time transparent encryption which is also called here as the "on-the-fly" encryption.

5. Application level encryption- In this encryption, the data is encrypted by the application that generated the data. Here the data first is encrypted and then it's fed into the database. This encryption done before putting any data into the database reduces the need for encrypting it again the database. The unauthorized person accessing into this has to break into the application of where this data was generated making it a complicated way.

6. Private and public key database encryption- Similar to the private encryption of normal data the database is also encrypted using a private or symmetric key. The data in the database is encrypted when it's not in use and decrypted back while in use only if the user knows the key. Public key encryption is done similarly like the public or asymmetric encryption of normal here the public key is available to all and the private key is necessary to access the database to decrypt it.

XI. HASHING

Usually hashing methods is used for the password security but in databases is used improve the security of the referential database. The data that needs to be put into the database can be hashed and stored as a hashed text in the database. When retrieving the data from the database the value that is given is processed by the hash algorithms and checks for the same value that is stored. If processed and stored is similar that data from that database can be accessed. The advantage of salting and pepper can be used to the data here.

XII. KEY MANAGEMENT

Key management is very crucial in database encryption as the database holds a large amount of data and if the key is lost or mishandled it can lead very undesirable consequences. The key management is done according to the method of database encryption used.

XIII. CONCLUSION

The cryptography gives advantages of data confidentiality, integrity, authentication and authorization. But it also has the drawbacks of complexity, high time consumption rate, cost and not properly devised systems. The further development to increase the merits and finding the solutions for the disadvantages can make cryptography as the best method of security to the data and messages both, online and offline.

REFERENCES

[1]. Chey cobb, Cryptography for dummies.
[2]. Research gate and Techopedia, Online website.
[3]. Keith M. Martin, Everyday Cryptography: Fundamental Principles and Applications.
[4]. William Stallings, Cryptography and Network security, 4th edition.
[5]. Atul Kahate, Cryptography and network security.
[6]. Denise Sutherland and Mark E. Koltko-Rivera, “Cracking Codes & Cryptograms for Dummies