Hybrid Encryption for Database Security

Ms. Priyanka Deore[1], Mr. Tushar Chaudhari[2]

[1] Lecturer, pursing ME (Computer Engineering) YTCEM, Maharashtra, India
[2] Lecturer, S.H. Jondhale Polytechnic, Maharashtra, India

---***---

Abstract - *Database is a collection of organized information. Data is organized in rows and columns format. We can perform insert, update, delete operation on database. Database is used by various areas like hospital, defense, school, college, government office, social media etc to store the sensitive information. As databases contains the sensitive information, security of such databases is a primary concern. cryptography is used to secure data. Hybrid encryption technique is more secure as compare to previous techniques. It is a combination of more than one cryptographic algorithms. It incorporates the combination of asymmetric and symmetric encryption. To secure data in databases hybrid encryption technique plays important role.*

Key Words: *Introduction1, Cryptography2, Asymmetric encryption3, Symmetric encryption4, Database System5, Hybrid Encryption Technique6, Proposed system: Hybrid Encryption for Database Security7, Advantages8, Conclusion9*

1. INTRODUCTION

In database Data is organized in rows and columns format. Databases are used by many areas to store information so it is necessary to provide security to data in databases. Hybrid encryption technique is more secure as compare to previous techniques. It is a combination of more than one cryptographic algorithms. This technique uses any one asymmetric encryption algorithms like Diffie-Hellman, RSA, ECC, ElGamal, DSA and any symmetric encryption algorithms like AES, Blowfish, CAST5, Kuznyechik, RC4, 3DES, Skipja etc. Hybrid encryption is considered as more secure because public keys and private keys are fully secured.

2. CRYPTOGRAPHY

Cryptography is an art of hiding data. To make secure communication cryptography plays vital role. It is the science used to try to keep information secret and safe. When information is send using cryptography, it is encrypted before it is sent. The encrypted text is called as ciphertext. To read the message again it is necessary to decrypt it.

3. ASYMMETRIC ENCRYPTION

Asymmetric cryptography is public key cryptography, this system uses pairs of keys public key and private key. Public key is a key which is publicly known, whereas private key is a key which is known only to the owner. Public key is used to encrypt the message whereas the pair private key is used to decrypt the message encrypted by the public key. In this technique, anybody can encrypt the message by using public key but only receiver can decrypt the message by using private key as private key is known only to the receiver. It is necessary to keep private key secure. There are various asymmetric encryption algorithms are available like Diffie-Hellman, RSA, ECC, ElGamal, DSA etc.

3.1 RSA

RSA is an algorithm used to encrypt and decrypt messages. I was first introduced in 1977 by Rivest, Shamir and Adleman. This is a asymmetric cryptographic algorithm which uses public key and private keys. RSA involves a public key and private key. The public key can be known to everyone; it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Select two large prime numbers p and q.
2. Calculate n=p*q. n should be minimum of 512 bits.
3. To find derived number select e. e must be greater than 1 and less than (p – 1)(q - 1)
4. The pair of numbers (n, e) form the RSA public key and is made public.
5. Private key d is calculated from p,q and e.
6. Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
7. Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).

4. SYMMETRIC ENCRYPTION

Symmetric encryption is secret key cryptography. This technique uses the same key for both encryption of plain text and decryption of cipher text. The keys, in practice, represent private communication between two parties. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (asymmetric key encryption). Symmetric key encryption is faster than public-key algorithm. There are two types of symmetric key algorithms stream cipher and block cipher. Stream ciphers encrypt a message as a stream of bits one at a time. Block ciphers take blocks of bits, encrypt them as a single unit, and sometimes use the answer later too. Blocks of 64 bits have been commonly used; though modern ciphers like the Standard use 128-bit blocks. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely. There are various symmetric encryption algorithms are available like Twofish, Serpent, AES, Blowfish, CAST5, RC4, TDES, and IDEA.

4.1 AES

AES stands for Advanced Encryption Standard. It is more popular and widely adopted symmetric encryption algorithm as it is found at least six time faster than triple DES. AES perform all its computation on bytes rather than bits. AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

AES performs following steps for encryption / decryption:

- First step is to generate round keys, round keys are generated using Rijndael's key schedule.
- The plaintext is converted to 4 x 4 state matrix.
- Each byte of the state is combined with the round key using bitwise xor.
- This is followed by ten rounds. In each of the first nine rounds, it performs four steps.
- Byte substitution in which each byte of state is replaced with the byte of S-Box in case of encryption and with the byte of Inverse S-Box in case of decryption depending upon its value.
- Shift rows in which first row of state matrix remains unchanged, second row shifts by 1 bit to the left, third row shifts by 2 bits to the left and fourth row shifts by 3 bits to the left. In case of decryption, shifting is to the right.
- Mix Columns in which each byte is replaced by a value dependent on all 4 bytes in the column.
- Fourth step is Add Round Key in which each byte of the state is combined with the round key using bitwise xor.
- In last round, it performs three steps only, the mixcolumns step is not performed in last step.

5. DATABASE SYSTEM

A database is organized set of information. Data in database is organized so it can be easily accessed, manage and updated. This data is organized into rows and columns. Database is used to store important information of various fields like education, military, government, industry etc. security of such a database is important. It is necessary to protect data against compromises of their confidentiality, integrity and availability. Hybrid encryption technique is more secure as compare to previous techniques. It is a combination of more than one cryptographic algorithms. It incorporates the combination of asymmetric and symmetric encryption. To secure data in databases hybrid encryption technique plays important role.

6. HYBRID ENCRYPTION TECHNIQUE

Hybrid encryption technique merges more than one encryption systems. It incorporates two encryption techniques, symmetric and asymmetric encryption. In hybrid encryption at the sender site first Data is encrypted by symmetric key that is secret key. In this same key is used for encryption and decryption both. Once data is encrypted by secret key that data is stores in encryption block. To improve the security, secret key is also encrypted by public key i.e. here system uses asymmetric encryption technique. This complete encrypted block which contains encrypted data and encrypted secret key is send to the receiver site. Once receiver receives this encrypted block first encrypted secret key is decrypted by using private key. Now decrypted secret key is used to decrypt encrypted data block.

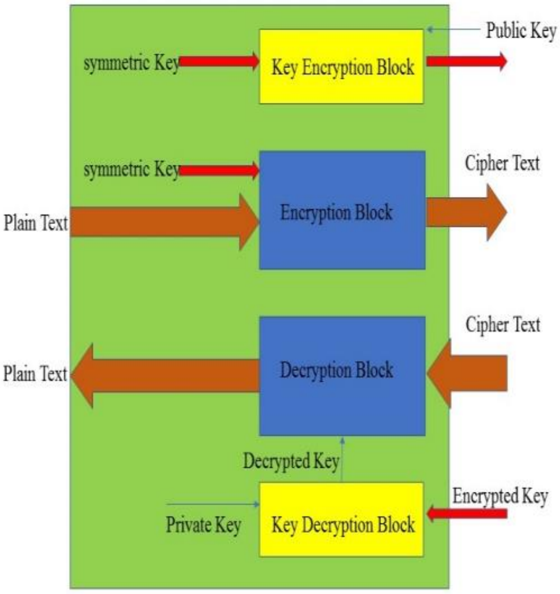

Fig -1: Hybrid Encryption Technique

7. Proposed system: Hybrid Encryption for Database Security

In database data is organized in rows and columns format. We can perform insert, update, delete operation on database. Database is used by various areas like hospital, defense, school, college, government office, social media etc. to store the sensitive information. As databases contains the sensitive information, security of such databases is a primary concern. cryptography is used to secure data. Hybrid encryption technique is more secure as compare to previous techniques. It is a combination of more than one cryptographic algorithms. It incorporates the combination of asymmetric and symmetric encryption. To secure data in databases hybrid encryption technique plays important role.

In this technique first, we encrypt plain text database by using symmetric key means secret key and stores that encrypted database in cipher text database. Then secret key which we have used to encrypt database now need to make secure by using public key. So here we are now using asymmetric encryption technique. This complete encrypted block which contains encrypted database and encrypted secret key is send to the receiver site. Once receiver receives this encrypted block first encrypted secret key is decrypted by private key. Now decrypted secret key is used to decrypt encrypted database.

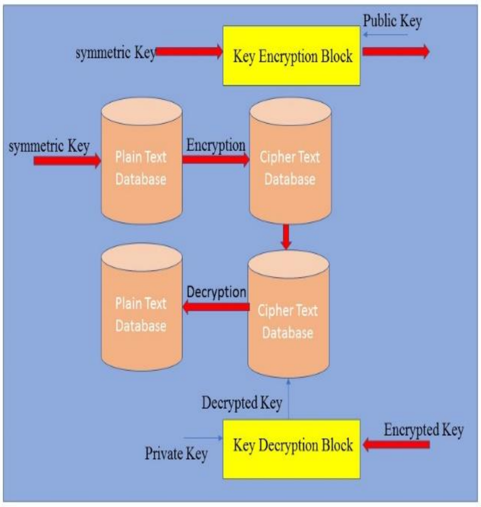

Fig -2: Hybrid Encryption for Database Security

8. ADVANTAGES

There are various advantages of hybrid encryption technique:

- Provides high level of security Hybrid encryption is a combination of symmetric encryption and asymmetric encryption so It provide high security as compare to other techniques.
- Encrypted data maintains integrity, Integrity means manipulation of data by unauthorized user or hacker. This technique Guarantees Data Integrity
- Transmit Securely Transmission of data become secure. Just as data security is ensured on all devices, encrypting data also provides security benefits during transmission.
- Secure database with hybrid encryption sensitive data can be stored in secure manner

9. CONCLUSION

As a database is a collection of sensitive data it is necessary to provide security to such a data. Here advanced encryption technique is used to provide high level of security as compare to previous techniques i.e. hybrid encryption technique. Hybrid encryption technique uses symmetric encryption to encrypt data and then uses asymmetric encryption to encrypt secret key. This technique provides two level of protection to the database.

REFERENCES

[1] “Ensuring data storage security in cloud computing based on hybrid encryption schemes”; by Mrinal Kanti Sarkar; Sanjay Kumar; Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on 22-24 Dec. 2016

[2] “Enhanced Security using Hybrid Encryption Algorithm” ;by Neha, Mandeep Kaur; International Journal of Innovative Research in Computer and Communication Engineering; Vol. 4, Issue 7, July 2016

[3] “A Hybrid Encryption Algorithm Based On AES and RSA”; by Ch.Vijayalakshmi , L.Lavanya , Ch.Navya; International Journal of Innovative Research in Computer and Communication Engineering; Vol. 4, Issue 1, January 2016

[4] “Enhanced Security Algorithm using Hybrid Encryption and ECC” ; by A. P Shaikh , V. kaul; IOSR Journal of Computer Engineering; Volume 16, Issue 3

[5] “A hybrid encryption model for secure cloud computing”; by Atewologun Olumide; Abeer Alsadoon; P. W. C. Prasad; Linh Pham; ICT and Knowledge Engineering on (ICT & Knowledge Engineering 2015)

[6] “Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm”; by Prakash Kuppuswamy , Saeed Q. Y. Al-Khalidi; IS Review; Vol. 19, No. 2, March (2014)