ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Enhanced Approach for Security in Database Using Encryption Technology

Ms. C. Divya
Assistant Professor, School of Information Technology and Science,
Dr G R Damodaran College of Science, Coimbatore,
Tamilnadu, India
mercy_twin@yahoo.com

Abstract - In traditional database security research, the database is usually assumed to be reliable. Under this assumption, the goal is to achieve security against external attacks, for instance from hackers and possibly also against users trying to obtain information beyond their privileges, for instance by some type of statistical inference. Therefore the database cannot necessarily be assumed to be fully trusted. Data in a database is very important. We must assure their security completely. It points out that it is difficult to ensure the security of the system by using a single encryption technology. This paper introduces the basic technologies of symmetrical encryption, asymmetrical encryption and then the hybrid encryption thoughts of combining the both are promoted. By using this method, the security of databases is enhanced.

Keywords: Database security, symmetric encryption, asymmetric encryption, hybrid encryption.

I. INTRODUCTION

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. Database security is also a specialty within the broader discipline of computer security.

Database security can begin with the process of creation and publishing of appropriate security standards for the database environment. The standards may include specific controls for the various relevant database platforms; a set of best practices that cross over the platforms; and linkages of the standards to higher level polices and governmental regulations.

Encryption technology is one of the most effective technologies used in database security. Classical database security relies on many different mechanisms and techniques, including access control, information flow control, operating system and network security, prevention of statistical inference, data and user authentication, encryption, time-stamping, digital signatures, and other cryptographic mechanisms and protocols.

However a simple encryption technology, such as symmetrical encryption or asymmetrical encryption, is very difficult to guarantee the security of network databases. It is possible to combine the both and through hybrid encryption we can create a safe, efficient database system.

Contributions: This study is aimed at analyzing the various encryption techniques which are used to enhance the database security.

Organizations: The remaining section of this paper is organized as follows. In Section 2, we review symmetric, asymmetric and hybrid encryption techniques and their pros and cons and Section 3 conclude the paper.

II. ENCRYPTION TECHNOLOGY

A. Symmetric Encryption Technology

Figure 1 is a schematic diagram of symmetric encryption. When sending information, it will be encrypted through certain algorithms and keys and the original information will be changed into cipher text. When receiving information, it will be decrypted with the same algorithms and keys and cipher text will be restored.

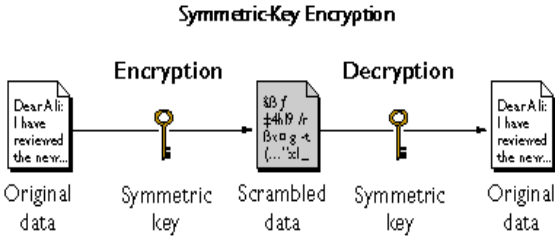

Figure 1: Schematic diagram of Symmetric Encryption

At present the most widely used symmetric encryption algorithm is DES (Data Encryption Standard) algorithm proposed by the IBM company [1,2]. DES uses a 56-bit key. In fact, the 56-bit key is divided into eight 7-bit blocks and an 8th odd parity bit is added to each block (i.e., a "0" or "1" is added to the block so that there is an odd number of 1 bit in each 8-bit block). By using the 8 parity bits for rudimentary error detection, a DES key is actually 64 bits in length for computational purposes (although it only has 56 bits worth of randomness, or entropy).The basic process is as follows:

a) Initial permutation: Replace the location of ciphertext of 64 bits and get an out-of-order explicit group of 64 bits. It is divided into two paragraphs of 32 bits. L0 and R0 are respectively used to express.

b) Execute the following iterative transformation to L0 and R0:

Li = Ri-1

Ri. = Li-1 ⊕ f (Ri-1, Ki) i = 1, 2…16

c) Two parts output after the 16th transform exchange order, do inverse initial permutation and then ciphertext will result.

a. Advantages and Disadvantages

The advantages of symmetric encryption are fast speed, high efficiency. It is widely used in encryption of large amount of data. The disadvantages are that keys are easily intercepted when they are transmitted on the network which will pose a threat to information security.

Therefore when using symmetric encryption the security of key transmission need to be guaranteed.

B. Asymmetric Encryption Technology

Figure 2 is a schematic diagram of asymmetric encryption. From it we can see that in the asymmetric encryption technology key is decomposed into a pair (private key and public key). There into private key belongs to the owner of key pair and others do not know. Public key is open and everyone can know. Information encrypted by public key can be decrypted only by the corresponding private key. Information encrypted by private key can be decrypted only by the corresponding public key.

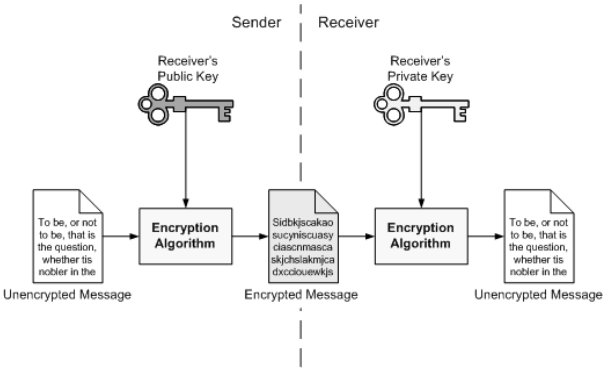

Figure 2: Schematic diagram of Asymmetric Encryption

Typical asymmetric encryption algorithm is the RSA algorithm [3]. The algorithm is proposed by R. Rivest, A.Shamir and L. Adleman from the Massachusetts Institute of Technology. It builds on the basis of the theories of decomposition of large numbers and detection of prime numbers. To create an RSA public/private key pair, here are the basic steps:

a) Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = pq.
b) Select a third number, e, that is relatively prime to (i.e., it does not divide evenly into) the product (p-1) (q-1). The number e is the public exponent.
c) Calculate an integer d from the quotient (ed-1)/ [(p-1) (q-1)]. The number d is the private exponent.

The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.

To encrypt a message, M, with the public key, create the cipher text, C, using the equation: $C = M^e \bmod n$.The receiver then decrypts the cipher text with the private key using the equation $M = C^d \bmod n$ .Now, this might look a bit complex and, indeed, the mathematics does take a lot of computer power given the large size of the numbers; since p and q may be 100 digits (decimal) or more, d and e will be about the same size and n may be over 200 digits.

a. Advantages and Disadvantages

The advantage of asymmetric encryption technology is ease of key management. Disadvantages are the complexity and slow encryption. It does not apply to the encryption environment of large amount of data. Therefore in data transmission, using symmetric encryption technology to encrypt data can be considered first and using asymmetric encryption technology to transmit symmetric encryption key as second. Thus both strengths of each other can be exerted.

C. Hybrid Encryption Technology

Through fully considering the strengths and weaknesses of symmetric encryption and asymmetric encryption we can combine the two and realize hybrid encryption [4].

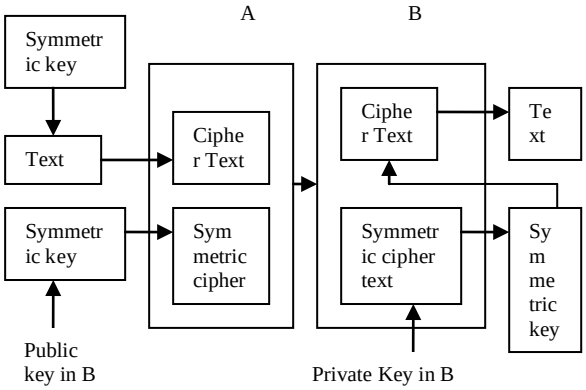

Figure 3: Schematic diagram of Hybrid Encryption

a. Use symmetric encryption algorithm to encrypt text. In order to guarantee transmission security of symmetric key use public key of B to encrypt symmetric key. This can ensure that only B correctly knows symmetric key. Even if others get the key of cipher text they cannot decrypt.
b. First of all use its own private key to decrypt key cipher text and get symmetric key which encrypts documents. Using the symmetric key can untie cipher text. Finally get the original information.

III. CONCLUSION

The hybrid encryption technology gives full play to the respective advantages of two kinds of encryption algorithm and provides more reliable and efficient security. The hybrid encryption technology used in the paper can also be used to enhance the security of other network databases.

We can also conclude that hybrid encryption technology overcomes not only the difficulties that symmetric encryption transmits keys but also the disadvantage that asymmetric encryption does not apply to large amount of data. The advantages of both can be fully integrated.

IV. ACKNOWLEDGMENT

The author wish to sincerely thank the management of Dr. G R Damodaran College of Science, Coimbatore for their constant encouragement and financial support rendered during the course of this research work.

V. REFERENCES

[1]. S. H. Qing, Cryptography and Computer Network Security. Beijing:Tsinghua University Press, 2001.

[2]. Y. P. Hu, Y. Q. Zhang, Symmetric Cryptography. Beijing: Machinery Industry Press, 2002.

[3]. S. Z. Guan. Public Key Infrastructure PKI and Certification Authority. Beijing: Publishing House of Electronics Industry, 2002.

[4]. X. J. Tong, W. Jiang, "Research of Secure System of Electronic Commerce Based on Mix Encryption," Microprocessors, 2006, vol. 4, pp. 44-47.

AUTHOR PROFILE

Ms. C.Divya has passed MCA degree in 2006 from Bharathiar University. She has completed her M.Phil in Computer Science in 2008.She is working as an Assistant Professor in School of Information Technology and Science, Dr G R Damodaran College of Science, Coimbatore, Tamilnadu since June 2006.Her research areas include Network Security and Cryptography and Database Management System. She has presented research papers in UGC sponsored National Conferences and IEEE International Conference.