ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Dependable sharing approach with creation of Encrypted database

Monika Sharma*
Lecturer in Information Technology
SDDIET,
Barwala, India
Monikamtech123@gmail.com

Meenakshi Sharma
Assistant Professor in CSE
H.C.T.M,
Kaithal, India
minnyk@gmail.com

Abstract: Database security is important for every organization to protect their data from unauthorized users. In this dissertation Encryption plays a major role for protecting the data and securely sharing the data in the database. Encrypting the whole data in the database is not advisable because of the time it takes to encrypt the data. So only the sensitive data is encrypted and stored in the database. Whenever any malicious attacks happen on the database even if he opens the database the data in the database is encrypted which that malicious user / unauthorized user can't understand.[1] So any attacks on the database become useless for those who are attacking. There are different kinds of users out of which administrator is one of the user and the administrator can give permissions to the other users. Whenever any authorized user enters with his valid id and password to view data according to the permissions given by administrator the data is decrypted then retrieved and shown to the user.[4],[6]. Even the user who is the owner of his details can give permissions on his details which he wishes to other users. So sharing also becomes more secure because only the owner and the administrator have the right to give different combination of permissions. In this paper we have discussed the dependable sharing approach of encrypted database.

Keywords: Database, Encryption, Database Security, Data Encryption

I. INTRODUCTION

There are many database security techniques but each of them having their own vulnerabilities. Many organizations are suffering from these vulnerabilities and are in immediate need of some database security technique that can ensure both data privacy and should be able to protect the database from the attacks caused by intruders and malicious users. Encryption is the only technique that provides both data privacy and protects the database from the attacks caused by intruders and malicious users. So there is an immediate need for the organization for a database security technique that can defend all kinds of attacks. Time also plays an important role in the organizations so encryption of the whole data is also not advisable and only data that is confidential / sensitive is encrypted [1]. Sharing of the data should also be secure only the authorized persons who are permitted should only view the data. This is technique that provides both the protection from malicious user keeping the time constraint in mind and secure sharing of data

II. DATABASE SECURITY

Databases have been protected from external connections by firewalls or routers on the network perimeter with the database environment existing on the internal network opposed to being located within a demilitarized zone. Additional network security devices that detect and alert on malicious database protocol traffic include network intrusion detection systems along with host-based intrusion detection systems. 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. 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. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

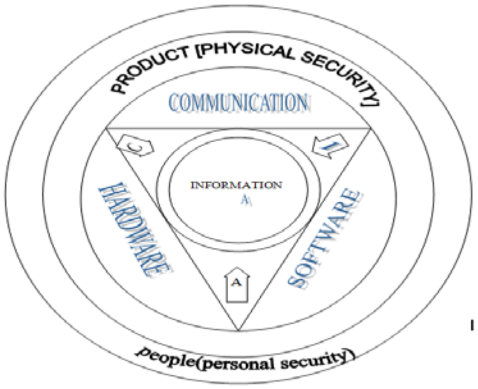

Figure 1. Components of Information Security

III. ENCRYPTION

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted). Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers, networks (e.g. the Internet e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption is also used in digital rights management to prevent unauthorized use or reproduction of copyrighted material and in software also to protect against reverse engineering.

IV. ENCRYPTION ALGORITHM

A mathematical procedure of performing encryption on data through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form. In this dissertation the encryption algorithm used is Data Encryption Standard (DES).

A. Data Encryption Standard (Des) Algorithm

The Data Encryption Standard (DES) is a cipher (a method for encrypting information) that was selected by NBS as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric key algorithm that uses a 56-bit key. DES consequently came under intense academic scrutiny which motivated the modern understanding of block ciphers and their cryptanalysis [9]. DES is now considered to be insecure for many applications. This is chiefly due to the 156-bit key size being too small. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

V. WORKING OF DES

Encryption of a block of the message takes place in 16 stages or rounds. From the input key, sixteen 48 bit keys are generated, one for each round. In each round, eight so-called S-boxes are used. These S-boxes are fixed in the specification of the standard. Using the S-boxes, groups of six bits are mapped to groups of four bits. The contents of these S-boxes have been determined by the U.S. National Security Agency (NSA). The figure in the next page should hopefully make this process a bit more clear. In the figure, the left and right halves are denotes as L0 and R0, and in subsequent rounds as L1, R1, L2, R2 and so on. The function f is responsible for all the mappings described above. DES is the archetypal block cipher an algorithm that takes a fixed- length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular keyused to encrypt.

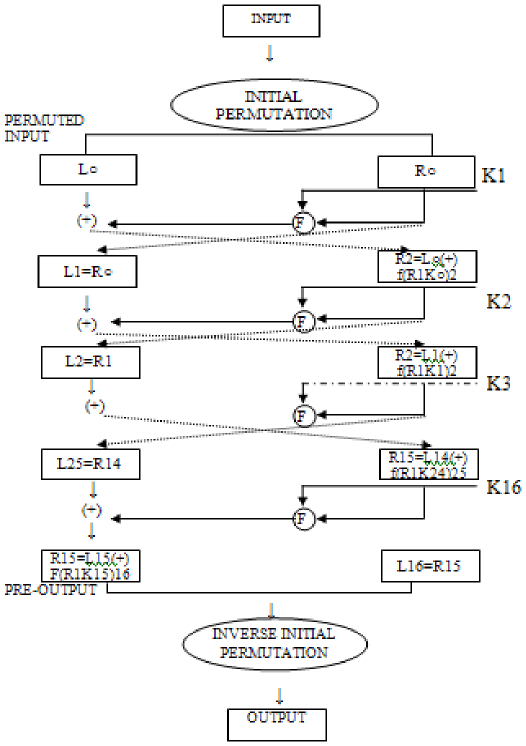

Figure 2: Data Encryption Standards Algorithm

VI. CONCLUSION

Encryption by itself can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. But if all the data in the database is encrypted then it reduces the performance. Therefore, only the sensitive/personal data is encrypted. For retrieval that data is decrypted. The no sensitive/common data is not encrypted and is retrieved immediately while authorized user requests for it according to the permissions given to them. Encryption is the only technique that provides both data privacy and protects the database from the attacks caused by intruders and malicious users. So there is a immediate need for the organization for a database security technique that can defend all kinds of attacks. Time also plays an important role in the organizations so encryption of the whole data is also not advisable and only data that is confidential / sensitive is encrypted. Even sharing of the data is also secure because only Administrator has right to give permissions and owner has the right to change the permissions. This increases the performance of the system. In this paper the encryption algorithm used is D.E.S (Data Encryption Standard) for encrypting the data. The model can be extended for different kinds of encryption algorithms such as AES (Advanced Encryption System) encryption algorithm, RSA (Rivest- Shamir- Adelman) encryption algorithm.

VII. REFERENCES:

[1] Sesai S, Yang Z, Chen J and Du Xu, “A Secure Database Encryption Scheme”, Proceedings of IEEE, pp 49-53, 26, Nov 2004.

[2] Lihua Yu,Chen G, Ke Chen,Dong J, “Securely Sharing

Data in Encrypted databases", Proceedings of the 10th International Conference on Computer Supported Cooperative work in Design, 2003.

[3] Yong Zhang, Wei-Xin Li, Xia-Mu Niu, "A Secure Cipher Index over Encrypted Character Data in Database", Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, pp 1111-1116,12-15 July 2008,

[4] Ian Somesville, "Software Engineering Pearson Education Asia", Sixth edition 2001.

[5] Raghu Ramakrishna, Johannes Gehrke, "Database Management Systems", McGraw Hill International Editions, Second Edition 2000.

[6] Java Server Pages Technology, "Sun Developer Network",1994, [online document] Available at: http://java.sun.com/products/jsp/index.jsp

[7]] http://en.wikipedia.org/wiki/HTML

[8] Apache Tomcat,"WIKIPEDIA", June 2009, [online document]Available at:http://en.wikipedia.org/wiki/Apache_Tomcat

[9] Data Encryption Standard, "WIKIPEDIA", June 2009, [online document] Available at:http://en.wikipedia.org/wiki/Data_Encryption_Standard

[10] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[11] Data Encryption Algorithm (DEA), ANSI X3.92-1981, American National Standards Institute, New York.

[12] Horst Feistel, Cryptography and Computer Privacy, Sci. Am. 228 (5), 15-23 (1973).

[13] Horst Feistel, Block Cipher Cryptographic System, US Patent 3,798,359, March 19, 1974.

[14] Whitfield Daffier and Martin E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, Computer 10 (6), 74-84 (1977).

[15] Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design, O'Reilly & Associates, Inc., Sebastopol, CA (1998).

[16] Miles E .Smid& Deniss. K. Brantstad, "Data Encryption Standard (DES), Federal Information Processing", Proceeding of IEEE, vol.76, pp.550-559, May, 1988.

[17] Gobinath, Subramaniam, Kalyani Subramanian, Senthil Raja Balakrishnan,Baskaran Kaliaperumal, "DES Enabled Fingerprint System", Proceedings of the International Conference on Man-Machine Systems (ICOMMS), , Batu Ferringhi, Penang, Malaysia, 11 – 13, October, 2009.

[18] Amit, Dhir, "Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs" , White Paper-115 (v1.0), March 9, 2000.

[19] Paul. A.J, Varghese Paul, P. Mythili, " A Fast and secure encryption for message communication", IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007),Dr. M.G.R. University, Chennai, Tamil Nadu, India. pp. 629-634, Dec. 20-22, 2007.

[20] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html.