ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Various Schemes for Database Encryption - A Survey

S. Pothumani, M. Sriram, J. Sridhar*
Department of CSE, Bharath University, Chennai -73
***Corresponding author: E-Mail: sridhar.cse@bharathuniv.ac.in**

ABSTRACT

In this IT world, databases contain lot of confidential and sensitive details of different organizations all over the world. Database security is the most important one. Encryption secures data within database. All the data will be changed as cipher text. So, no use of hack it. There are number of methods and techniques are available to encrypt a database. This paper proposes a small literature about various techniques from different papers.

KEY WORDS: Database, Encryption

1. INTRODUCTION

Database encryption secures the data within the database. There are different types of database encryptions are available. In that, transparent database encryption encrypts the whole database. It provides security to the inactive data which is stored in physical medium. It uses symmetric key to encrypt the data. In column level encryption, each and every column of the database is encrypted in a specific way. Compared to transparent encryption, it is more secure. But different columns with different keys may cause to decrease the database performance. Encrypting file system is used to encrypt the database files. But due to some practical issues, EFS is not commonly used. In Symmetric Database encryption, a unique key is used to encrypt a database. This modifies the information to unreadable form. Encrypted data is saved. If it needed by client, then it will be decrypt. Problem in this encryption is that confidential data may be leak if the private key is spread to individuals. Asymmetric encryption uses two different types of keys, private and public keys. Anyone can be access the public key. Another one is secret key. It is unique for one user. To encrypt, public key is used. The user use private key to decrypt. The process of storing and handling keys is named as key management. If it is not handled properly (lose/leak), it affects the sensitive data. To improve efficient access of database, hashing is used. The hashing algorithm is used to convert the input into string. Generally, it contains fixed length. That string will b stored into database. Each an every time, when user gives password, it will convert to have string and check with the string stored in database. If it matches, he/she is authorized user.

Literature review: Paper.1.A Database Record Encryption Scheme Using the RSA Public Key Cryptosystem and Its Master Keys. This paper presents two different encryption schemes for database. Both schemes use RSA algorithm. The first one is field based encryption system. All fields are accessed by master key of user. Next, represents record oriented encryption. It uses only one master key. This method applied in subsets and integers group. To provide security to the database is one of the complicated problems. For this, asymmetric crypto system is commonly used. Basically encryption keys are used to write data in protected fields. Decryption keys are used to read the data. So it provides the access rights for user. The simple encryption method for database is RSA method. RSA master key pair contains two different keys. Encryption keys are used to represents the right of write operation. The right of read operation is represents by decryption keys. The key pair is maintains by database manager. All rights of fields are combined by RSA master keys. Database manager establishes each field of database in database encryption schemes. Access rights are allocated by using this method. This is used to allocate the access rights depend upon the user requirements. Generally, dynamic data storage is used. Read operation is the most frequent compare to other. Generally, write operations are move to write proxy for approval. The Scheme 2 establishes CRT. This method prevents from the outside attack. It prevents the traffic analysis also. To manage key management problems, both schemes use the RSA master key. Both provides the access rights to user and database security

Paper.2.Chip-Secured Data Access: Confidential Data on Untrusted Servers: Major aim of ubiquitous computing is to provide data anywhere, anytime, anyhow only. It is used to enhance the database connections to Internet. And also it should ensure about the data confidentiality. Day by day, malicious attacks and security threats are increased. So, Trusting traditional database security methods is somewhat danger. In this paper, a new method named C-SDA (chip secured data access) is proposed. This control the users' access rights and provides data confidentiality. And also act like a inter mediator between client and encrypted database. This element is embedded in a smartcard. This consists, combined hardware and software. It ensure against attacks. Query evaluation techniques are used mostly.

Paper.3. A Framework for Efficient Storage Security in RDBMS: Day by day, growth of E-business is tremendously increased. So everybody should be aware about data security and database security. Some RDBMS storage models (such as the N-ary Storage Model) stores records. Offset table is used at the end of the page. It is used to locate the starting point of record. If query is more sensitive, NSM provides tremendous performance. It is used to transfer data to and from secondary storage. This is suitable for online transaction processing. This paper proposes a novel protective model for storage and key management architecture. It consists of various encryption

methods. It ensures high level of database security. In this paper, TPC-H dataset is used with Partition Attribute across (PAX). A page will be divided into mini pages. So it increases cache performance. A mini-page contains one attribute of record. Depend upon plain and cipher text attributes, the plaintext and cipher text of PAX used to divide the page into two mini pages. So each record is dividing into two subordinate records. It reduces the cost of encryption as well as storage and computation costs. It takes benefits of NSM. It needs few modifications to page layout.

Paper.4.Fast, Secure Encryption for Indexing in a Column-Oriented DBMS: This paper deals with two major problems. First, security for the encryption. Next, fast performance of query. There are number of methods deals the same. The existing method ensures order preserving encryption techniques are suitable for databases. Compare to other methods this one is very simple and excellent method to build indices. But it creates problems on straightforward attacks. In this paper, a new column oriented encryption is proposed. It ensures fast indexing operations. Block cipher is applied to encrypt tiny bytes per page. Two cipher texts are compares from the most significant byte. It compares byte by byte. Even though other block ciphers encrypt unit of 8 bytes or more, here it is possible to encrypt byte by byte.

Paper.5.The SSL Protocol Version 3.0: Major aim of this paper is to offers privacy, consistency to corresponding programs. This contains two layers. The lower layer consists of any reliable transport protocol like TCP. This protocol contains SSL record protocol on the top. This SSL is used to encapsulate different protocols of higher level. This encapsulated protocol, the SSL handshake protocol allows authorization methods of client and server. SSL Protocol contains higher level protocol on its top. It is used to provide private connection. After initial handshake, encryption describes a private key. Symmetric cryptographic algorithms like DES, RC4 are used to encrypt data. Asymmetric algorithms like RSA, DSS are used to authenticate the peer's identity. Reliable connection is established. Hash functions are used to compute MAC. These MAC methods used to transfer data with message integrity check.

A random number generator generates an output based on the cryptographic methods. This output is exclusive ORed with the plain text in stream cipher encryption. But block of cipher texts are encrypt every block of plain text in block cipher encryption. CBC (chain Block chaining) is used to encrypt all blocks.

Paper 6: The Transport Layer Security (TLS) Protocol Version 1.2: Between two different communicating programs, Data privacy and data integrity is offered by this protocol. There are two layers. First, this protocol is layered on top of transport protocol which provides private connection. To encrypt a data, symmetric key algorithms are used. Separate keys are produced for each connection. All are based on next layer protocol. This can function excluding a MAC and used without encryption. A Keyed MAC is used to transfer data with message integrity. To encapsulate different higher level protocols, TLS record protocol is used. Next, TLS Handshake protocol is used to authenticate client and server. With basic three properties, connection is established. Asymmetric or public key encryption algorithms are used to authenticate peer’s identity. A shared secure negotiation communication does not modify by attacker. This protocol is independent in application level. In this standard, the designers can decide how to initiate, how to interpret and how protocols add security with TLS.

Paper.7. A Novel Framework for Database Security based on Mixed Cryptography: Traditional techniques such as access control authenticate users, intrusion detection and other policies are securing data theft and intrusion. The previous methods don’t provide any guarantee for database encryption. Access control is used to provide security for data. Sometimes, unauthorized user can access the database. In database encryption, we have to concentrate on three aspects such as who will encrypt data, where it is done, how it is transferred. In this paper, there are three different models are used. There are, trusted database server, untrusted server and semi trusted server. In trusted database server, the database owner operates a database server. In untrusted server, a service provider stores owner’s database. This is not come under the control of database owner. In final model, More than one parties shares database. Here, a mixed cryptography database is proposed. Various parts of data is encrypted in three different models. So no one can easily get the details of database without three keys. And queries also encrypted by this three models. This is used in most of the applications like e-Com and e-banking. These are always carrying confidential data transmitted through different untrusted networks. This method ensures security on these environments.

Paper.8.A Secure Database Encryption Scheme: The proposed model consists of different layers. Two blocks, Level1 subjects and level2 subjects are in user interface layer. A private key is used to encrypt. Next, database management layer contain MAC (Mandatory Access Control) and tamper free controller.

Paper.9.Incorporating a Secure Coprocessor in the Database-as-a-Service model: This paper establishes a secure coprocessor at untrusted coprocessor. All sensitive data contains a secure perimeter. To provide this a SC is installed on a computer. It contains number of sensors are available to detect different physical attacks.

2. CONCLUSION

This paper reviewed nearly nine papers. Each and every paper contains different algorithms and different techniques to achieve database encryption. All the methods are very efficient. But the techniques are differs depend

upon the database performance, access time and key management. Future work is to review various methods more than this paper and find the best encryption method.

REFERENCES

Alan Freier O, Philip Karlton and Paul Kocher C, The SSL protocol, 1996.

Samba Sesay, Zongkai Yang, Jingwen Chen and Du Xu, A secure database encryption scheme, Consumer Communications and Networking Conference, IEEE, 2005, 49 - 53

Bala Iyer, Sharad Mehrotra, Einar Mykletun,Gene Tsudik, and Yonghua Wu, A Framework for Efficient Storage Security in RDBMS, Advances in Database Technology - EDBT 2004Volume 2992 of the series Lecture Notes in Computer Science, 2004, 147-164

BrinthaRajakumari S, Nalini C, An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, 7, 2014, 44-46.

Chin-Chen Chang and Chao-Wen Chan, A database record encryption scheme using the RSA public key cryptosystem and its master keys, ICCNMC '03: Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (Washington, DC, USA), IEEE Computer Society, 2003, 345

Einar Mykletun and Gene Tsudik, Incorporating a Secure Coprocessor in the Database-as-a-Service Model, Innovative Architecture for Future Generation High-Performance Processors and Systems, 2005

Hasan Kadhem, Toshiyuki Amagasa, Hiroyuki Kitagawa, A Novel Framework for Database Security based on Mixed Cryptography, Fourth International Conference on Internet and Web Applications and Services, 2009.

Jayalakshmi V, Gunasekar NO, Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag /swell, 2013 International Conference on Energy Efficient Technologies for Sustainability, ICEETS, 2013, 1036-1040.

Kaliyamurthie KP, Parameswari D, Udayakumar R, QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, 6 (5), 2013, 4648-4652.

Kaliyamurthie KP, Udayakumar R, Parameswari D, Mugunthan SN, Highly secured online voting system over network, Indian Journal of Science and Technology, 6 (6), 2013, 4831-4836.

Khanaa V, Thooyamani KP, Saravanan, T., Simulation of an all optical full adder using optical switch, Indian Journal of Science and Technology, 6 (6), 4733-4736.

Khanaa V, Thooyamani K.P, Using triangular shaped stepped impedance resonators design of compact microstrip quad-band, Middle - East Journal of Scientific Research, 18 (12), 2013, 1842-1844.

Kumaravel A, Dutta P, Application of Pca for context selection for collaborative filtering, Middle - East Journal of Scientific Research, 20 (1), 2014, 88-93.

Luc Bouganim and Philippe Pucheral, Chip-secured data access:confidential data on untrusted servers, VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases, VLDB Endowment, 2002, 131–142.

Raj M.S, Saravanan T, Srinivasan V, A modified direct torque control of induction motor using space vector modulation technique, Middle - East Journal of Scientific Research, 20 (11), 2014, 1572-1574.

Saravanan T, Raj M.S, Gopalakrishnan K, VLSI based 1-D ICT processor for image coding, Middle - East Journal of Scientific Research, 20 (11), 2014, 1511-1516.

Sengottuvel P, Satishkumar S, Dinakaran D, Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling, Procedia Engineering, 64, 2013, 1069-1078.

Sundararajan M, Optical instrument for correlative analysis of human ECG and breathing signal, International Journal of Biomedical Engineering and Technology, 6 (14), 2011, 350-362.

Thamotharan C, Prabhakar S, Vanangamudi S, Anbazhagan R, Anti-lock braking system in two wheelers, Middle - East Journal of Scientific Research, 20 (12), 2014, 2274-2278.

Tingjian Ge and Zdonik S, Fast, secure encryption for exing in a column-oriented DBMS, Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, 2007, 676–685.

Udayakumar R, Khanaa V, Saravanan T, Saritha, G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, 16 (12), 2013, 1781-1785.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and fabrication of dual clutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1816-1818.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and calculation with fabrication of an aero hydraulwicclutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1796-1798.