Advanced Database Security and Encryption

Anil Dixit
Research Scholar
Jain University, Bangalore
Karnataka – 560027, India

Dr. Suchithra R
Jain Global Campus, Jain University
Jain University, Bangalore
Karnataka – 560027, India

Abstract: Data is more or less part of today's life of an Organization, Enterprise, State and Country. Top of agenda is to safeguard the data from getting into wrong hands. Choosing database for an entity is an important decision that could save from future embarrassments and loss - be it socially or commercially. Open source and Commercial databases are available in the market wherein the latter is not viable commercially. This survey paper describes about the database security threats, various ploys and suitable techniques to counter them. There are many threats in database which leaks the information for prohibited purpose. The main threats in database security are Excessive Privilege Abuse, Legitimate Privilege Abuse, Privilege Elevation, Database Platform Vulnerabilities, SQL Injection, Weak Audit Trail, Denial of Service, Database Communication Protocol Vulnerabilities, Weak Authentication and Backup Data Exposure. The main important method to secure database from attackers/intruders are Cryptography, Steganography and Access Control.

Keywords: Security, Threats, breaches, DoS, SQL, Cryptography, Encryption, Rootkits, Encryption, Database, Security, Encryption and Access Control.

I. INTRODUCTION

We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material. Information or data is a valuable asset in any organization. Almost all organization whether social, governmental, educational etc., have now automated their information systems and other operational functions. They have maintained the databases that contain the crucial information. So database security is a serious concern. To go further, we shall first discuss what actually the database security is? Protecting the confidential/sensitive data stored in a repository is actually the database security. It deals with making database secure from any form of illegal access or threat at any level. Database security demands permitting or prohibiting user actions on the database and the objects inside it. Organizations that are running successfully demand the confidentiality of their database. They do not allow the unauthorized access to their data/information. And they also demand the assurance that their data is protected against any malicious or accidental modification. Data protection and confidentiality are the security concerns. Figure 1 below shows the properties of database security that are: confidentiality, integrity and availability [6] [7] [8].

II. LITERATURE SURVEY

As discussed previously confidentiality imposes limits while retrieving the secure data and therefore averting the illegal access to the data. Integrity means that the data will not be tainted in any way. Availability of data on time is the property of secure databases. [1][5]

There are four types of controls mentioned by Denning [1] to obtain the database protection, those includes: access control, information flow control, cryptographic flow control and inference control.
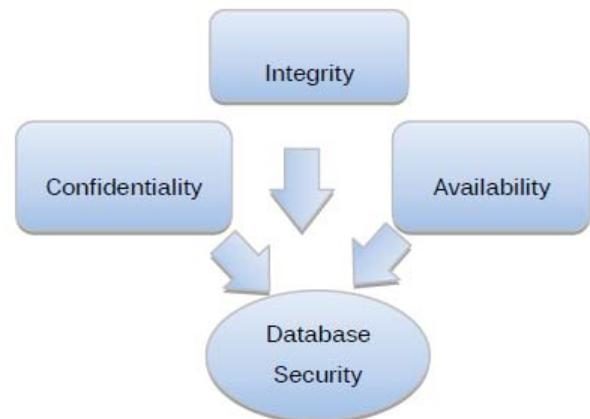

Fig 1: Properties of Database Security

Access controls ensures that all direct accesses to the system are authorized. The access controls governs that that can access the system's objects. Often it happens that important information or data is leaked out or misused not because of defective access control but because of improper information flow. When policies for information flow are not properly defined than the system data is less protected. The cryptographic control, controls (secures) the data by encrypting it. [1][2]. another approach has been adopted for securing the databases. It has been discussed that to make the databases secure different policies at organization level can be implemented. Data/information is always a most important asset for any organization whose security cannot be compromised. With the advances in technology, the risk to these valuable assets increases. So their security is a big challenge. In [8] different database

security layers are defined shown in figure (2) below. These layers are: database administrator, system administrator, security officer, developers and employee. For each layer some well-defined security policies have been anticipated.

These policies ensure the security features, privacy, confidentiality and integrity. This study mainly focuses on issues in databases security and measures taken to solve those issues. Securing sensitive data from illegal access, theft and forging becomes a big challenge for different organizations, like government, no-government and privates sectors. Encryption of data in client or server side where data is shared between different parties is not sufficient. Basically the problem is to ensure that semi trusted database is secure or not. [6]

A new hypothesis for database encryption is proposed in which database encryption can be provided as a service to applications with unified access to encrypted database. Using such an encrypted data management model, applications can concentrate on their core businesses and protect data privacy against both malicious outsiders and the untrusted database service users without need to know encryption details. [12]
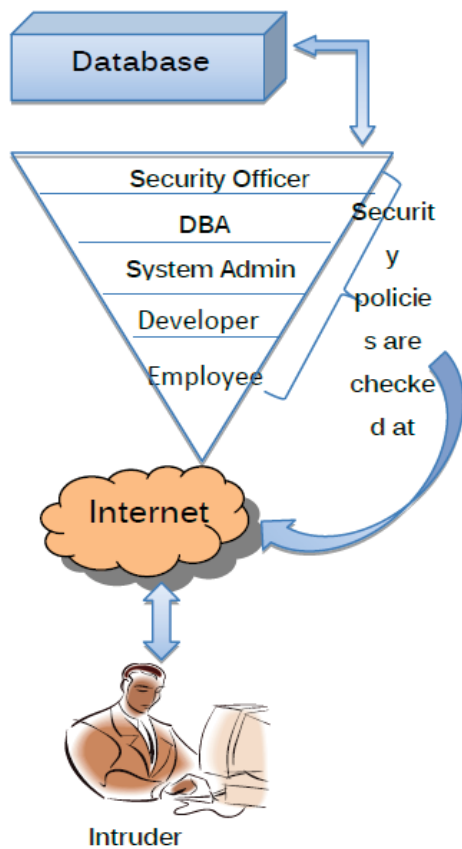

Fig 2: Security layer at organizational level

Further we shall discuss what actually has been implemented to reduce/eliminate the security threats and how the database security was enhanced in the past. And we shall see what needs to be done for securing a valuable asset, the databases of organizations.

Security Risks to Databases

The initiative database organization is subject to prodigious variety of threats. Some serious threats are envisioned in this document. This list is taken from a white paper presented by Imperva's Application Defense Center. [3]

Excessive Privilege Abuse - When users are specified with the access rights that allow them to perform other tasks not included in their job, harmful intent can be discovered through such tasks thus leading to misuse of such privileges. When we talk of such abuse, an example of university can be quoted in which an administrator who is given access to all databases and holds the privilege to change the records of any student. This may lead to misuse such as changing of grades, marks of students or change in the amount of fine charged to any student. As a result, all users who perform different tasks are given default level of privileges that grants access in excess.
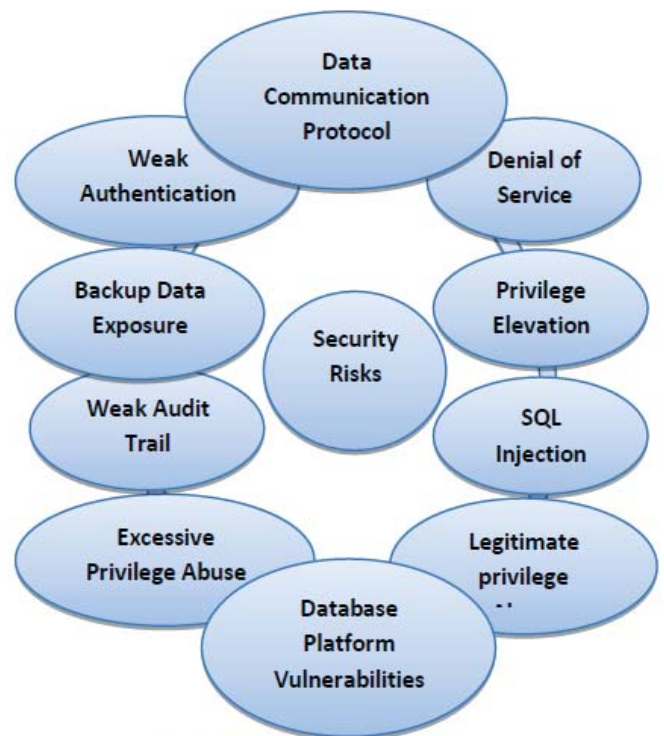

Fig 3: Databases Security Risks

Legitimate Privilege Abuse - Legitimate privilege abuse can be in the form of misuse by database users, administrators or a system manager doing any unlawful or unethical activity. It is, but not limited to, any misuse of sensitive data or unjustified use of privileges.

Privilege Elevation - Excessive exposure leads to discovery of flaws which is taken advantage of by attackers and may result in the change of privileges e.g. ordinary user given the access of administrative privileges. The loss of which could result in bogus accounts, transfer of funds, misinterpretation of certain sensitive analytical information. Such cases are also found to be in database functions, protocols and even SQL statements.

Database Platform Vulnerabilities - Vulnerabilities in the previous operating systems such as Windows 98, Windows 2000, etc. may create data loss from a database, data corruption or service denial conditions. For instance, the

blaster worm created denial of service conditions from a vulnerability found in Windows 2000.

SQL Injection - Random SQL queries are executed on server by some spiteful attacker. In this attack SQL statement is followed by a string identifier as an input. That is validated by the server. If it does not get validated it might get executed. Through these unobstructed rights may gain by the attackers to the whole database.

Weak Audit Trail - A database audit policy ensures automated, timely and proper recording of database transactions. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization's databases and may cause instability in operations.

Denial of Service - It is the attack that prevents the legitimate users of a program/application/data to use or access that specific service. DOS can take place using different technique. Attacker may get access to database and tries to crash the server or resource overloading, network flooding and data corruption can be the techniques for creating conditions of DOS attack. It is a serious threat for any organization.

Database Communication Protocol Vulnerabilities - Large number of security weaknesses is being identified in the database communication protocols of all database retailers. Deceitful activity directing these susceptibilities can varies from illegal data access, to data exploitation, to denial of service.

Weak Authentication - A weak authentication strategy renders the databases more vulnerable to attackers. The identity of database users are stolen or the login credentials are obtained through some source which then helps in modification of data or obtaining sensitive information and if authentication is not properly implemented and is weak, it helps the attacker to steal data.

Backup Data Exposure - Backup data exposure is an important threat that needs to be taken care of. Since backups on tapes, DVD's or any external media are exposed to high risks, they need to be protected from attack such as theft or destruction. So far we he discussed some important threats to database security.

Now we shall see what can be done to limit these risks and threats.

Database Security Considerations

To eliminate the security threats every organization must define a security policy. And that security policy should be strictly enforced. A strong security policy must contain well defined security features. Figure 2 shows some critical areas that need to be considered are explained below. [1][3][4]

Access Control - Access control ensures all communications with the databases and other system objects are according to the policies and controls defined. This makes sure that no interference occurs by any attacker neither internally nor externally and thus, protects the databases from potential errors-errors that can make impact as big as stopping firm's operations. Access control also helps in minimizing the risks that may directly impact the security of the database on the main servers. For example, if any table is accidentally deleted or access is modified the results can be roll backed or for certain files, access control can restrict their deletion.

Inference Policy - Inference policy is required to protect the data at a certain level. It occurs when the interpretations from certain data in the form of analysis or facts are required to be protected at a certain higher security level. It also determines how to protect the information from being disclosed.
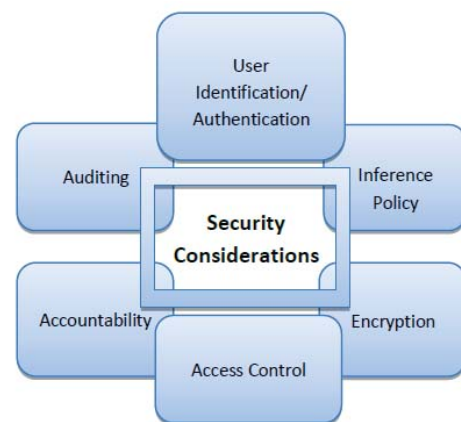

Fig 4: Critical Areas under Consideration

User Identification/Authentication - User identification and authentication is the basic necessity to ensure security since the identification method defines a set of people that are allowed to access data and provides a complete mechanism of accessibility. To ensure security, the identity is authenticated and it keeps the sensitive data safe and from being modified by any ordinary user.

Accountability and auditing - Accountability and audit checks are required to ensure physical integrity of the data which requires defined access to the databases and that is managed through auditing and record keeping. It also helps in analysis of information held on servers for authentication, accounting and access of a user.

Encryption - Encryption is the process of concealing or transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. The resulting encoded information is called as encrypted information.

Data is valuable assets of an organization. So its security is always a big challenge for an organization. In recent times security of shared databases was studied through cryptographic viewpoint. A new framework was proposed

Special Issue - 2016

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICRET - 2016 Conference Proceedings

in which different keys are used by different parties to encrypt the databases in assorted form that was named as Mixed Cryptography Database (MCDB). [6]

Different governmental, non-governmental, and private and many other organizations have sensitive data on web servers that really need to be protected from attacker or intruders. To make the databases secure different security techniques were developed. One of them is encryption techniques. Though encryption improves the protection but its implementation decisions are also very important. Like what, how, when and where is to be encrypted. . Following figure 4 shows where encryption takes place. Developing the encryption strategies arises some important questions also, like how, when and where the encryption will be performed.
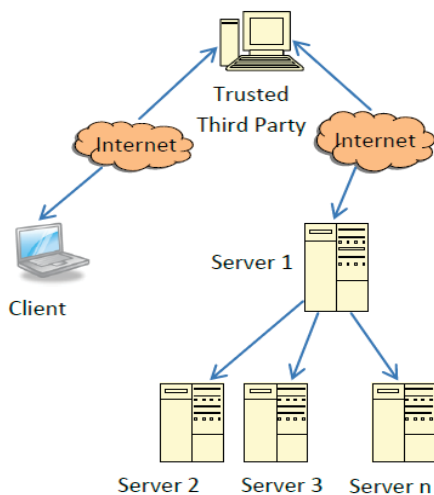

Fig 5: Three Levels where Encryption is performed.

Encryption algorithm, symmetric or asymmetric is not explained in this framework. Query processing performance is badly affected by these algorithms. The encryption algorithms affect the performance of query processing and security analysis. Other important research issues related to this framework: first, the best encryption algorithm used in the mixed cryptography database on performance and security perspectives; second, access control methods used to control access for all parities using the database; and finally indexing and joining between different databases.

According to [7], it does not matter which access control method is used; there are no of ways to avoid the authorization imposed by the database server. For instance, the information system can be intruded by stalker who tries to source the database impression on disk. Databases are being outsourced to database service providers (DSP) that also welcomes the threats. The database owner has no other choice than to trust the DSP's. Than the database administrator can also miss use his rights and spay the database.

Three encryption levels are defined. Storage-level encryption, database-level encryption and application-level encryption. Storage level encryption encrypts the data in the storage subsystem. It is transparent thus avoids the risk of

any change in existing application. In storage level encryption it has to be guaranteed that there should be no copy left unencrypted so it is risky to selectively encrypt the files e.g., in temporary files,, log files etc. When the data is saved or recovered from the database then database level encryption is performed. It is part of the database design. Here encryption can be done at selective granularities, like on row or column or tables. For both storage level and database level encryption strategies, the encryption keys must be available ate server side to decrypt the data. The third application level encryption is performed within the application. When selection of keys and encryption granularity is made on application logic it provides highest flexibility.

Encryption algorithm, key size and keys protection are the parameters that ensure the security. The better the encryption algorithm is used the better will be the security. And with strong encryption algorithm, appropriate operation mode is also very important. To overcome the problem of unauthorized access of keys, two solutions were proposed. HSM and Security server approach. After the addition of security server or HSM that lessen the disclosure of encryption keys, database is still vulnerable to threats.

To make the databases protected, encryption techniques are widely used. Implementing encryption on databases is though not an easy task [9]. But it is generally known as solitary the key concerns of data security. However preserving data privacy providing boosted data sharing, an innovative encryption scheme is proposed. Secure data is protected and key management is done efficiently. That helps to share the encrypted data easily. Encryption provides the confidentiality in databases.

A model has been proposed that provides the threats are confronted by the database. Arbitrarily created working keys are used by the user to encrypt the data. Private Key is decrypted in order to see the encrypted data.

Evolutionary trend of technology has eliminated the notion of boundary to access of any medium of data. This limitless access has made this world smaller bringing it closer via click of a mouse but it also increases threat of breach of security especially for the global business environment. Responding to such issues Transparent Data Encryption technology has been formulated and evolved offering secure solutions. Encryption is defined as encoded information that is only readable and decoded by the persons whom the information is intended. This study discusses how the Transparent Data Encryption technology is utilized to secure against data frauds and theft. The basic technological meaning of Transparent Data encryption is encoding or encrypting databases on networks, hard disk and/or on any backup media to provide highly configurable, transparent, safe and secure environments for application development. Microsoft SQL Server 2008 uses this technology to encrypt database content stored on any network, disk or backup medium along with process of creation of a Master Key. This involves creation of key, protection by the certificate

and ways to set the database to use in Microsoft SQL Server encryption. This study investigates what Microsoft SQL Server configurable environment has to offer in terms of data safety, security and application development for developers. [10]

In [11], a new light weight encryption method is proposed that is used for columns stored in data ware houses with trusted servers. The new method is called Fats Comparison Encryption (FCE). Its overhead makes the comparison fats and efficient. So far we have discussed the work done on database security using Encryption. Now the next section will present the comparison of the study done so far.

Comparative Analysis

In this section comparative analysis is performed by taking three factors from each paper discussed in above literature survey.

Encryption in Databases

Following table 1 explains how encryption is performed in databases, what methods, and algorithms are used and where it is implemented. Different techniques or methods are identified in the table 1 below that is used to encrypt the data. The table 2 then gives the comparison of those methods/techniques.

Table 1: Encryption in Databases

Paper	Methods/Techniques	Algorithm	Where encryption can be performed
A Novel Framework for Database Security based on Mixed Cryptography [6]	Mixed Cryptography Technique based on data Classification methods	Any symmetric Encryption algorithm can be used	Encryption is done at -Client side -Untrusted database -Server
Database Encryption [7]	Hash Security Module Encryption Strategy	State –of-the art algorithm and mode of operation should be used.	Encryption can be at: -Storage Level -Database Level -Application Level
A Database Encryption Scheme for Enhanced Security and Easy Sharing [9]	Combination of the Conventional encryption and public key encryption, utilizing the speed of conventional encryption and convenience of public key encryption.	X	X
Transparent Data Encryption-Solution for Security of Database Contents [10]	Transparent Data Encryption used by Master database key	X	Page Level
Fast, Secure Encryption for Indexing in a Column-Oriented DBMS [11]	Fast Comparison Encryption	Symmetric encryption algorithm	DataWare houses

Comparison of Encryption Methods/Techniques

Methods/Techniques	Advantages	Disadvantages / Limitations
Mixed Cryptography Technique based on data classification methods	Sensitive data is protected from attacks even at multiple levels because of having many keys to different parties. Secure data storage and data transmission is performed to ensure the maximum protection of sensitive data.	Performance of queries and security analysis is affected because of encryption algorithms. Access control methods are not defined.
Hash Security Module Encryption Strategy	Security server is not tampered Encryption keys are never exposed.	Complex
Transparent Data Encryption used by Master database key	Provides protection to sensitive data on disk drives and backup media from illegal access. Cost of user management is reduced. Provide privacy management.	Encryption across communication channels is not provided. Database could not be opened if the certificate is not available and the backup of certificate and private key is not maintained. Database becomes inaccessible after altering the certificates to be password protected
Fast Comparison Encryption	Fast indexing operation Low decryption overhead	

Special Issue - 2016

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICRET - 2016 Conference Proceedings

The following section will give an empirical analysis.

Empirical Analysis

This empirical study is done by keen observation of the literature and then results are drawn. Frequency of benchmarks in different papers that were under consideration is shown below in a table.

Percentage	Criticality
10-20 %	Medium
20%-50%	Moderate
51%-80%	High
81%-100%	Very High

Frequency - Frequency is the number of occurrences of a repeating commonness .The frequency is calculated in such a way that the paper which has an issue not common in some other paper is evaluated as having frequency "1" whereas the papers which have the common issues have been given frequency equal to the number of papers having that issue. The frequency calculation has been shown in Table 3.

Table 3: Frequency of security parameters achieved using Encryption methods

Security Benchmarks	Paper 1 [6]	Paper 2 [7]	Paper 3 [9]	Paper 4 [10]	Paper 5 [11]
Confidentiality	✓	✓	✓	✓	✓
Integrity	✓			✓	
Access control		✓	✓		
Efficiency			✓		✓
Privacy	✓	✓	✓		

The Percentage out of 5 papers, frequency and criticality has been shown in Table 3.

Criticality - To find the measure of frequency of occurrence of an issue the Criticality factor is divided into four parts i.e.

Medium, Moderate, High and Very High. The percentage range for criticality is defined below:

Table 4: Empirical Analysis of security parameters achieved using Encryption methods

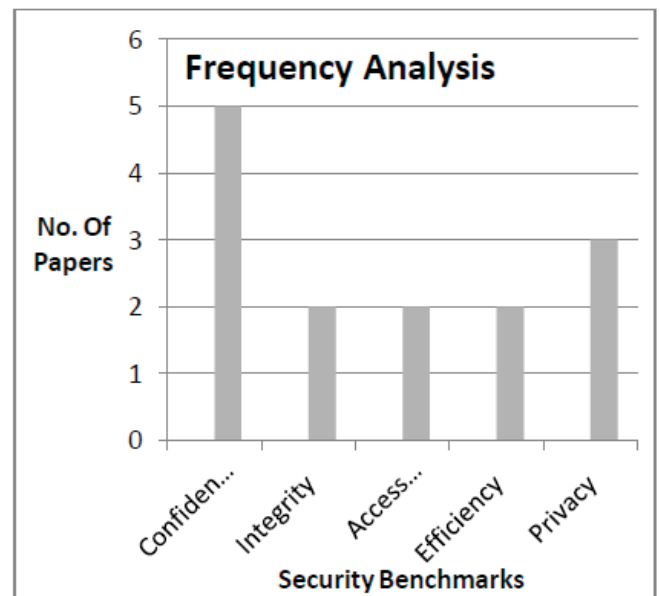| Security Parameters	Frequency	Percentage	Criticality
Confidentiality	5	100 %	Very High
Integrity	2	40 %	Moderate
Access control	2	40%	Moderate
Efficiency	2	40%	Moderate
Privacy	3	60 %	High

Fig 6: Frequency of security benchmarks achieved using Encryption methods

With the help of data obtained in Table 1 we can calculate the percentage and criticality also as shown in Table 2.

CONCLUSION

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database is vulnerable to hosts of attacks. In this study major security issues faced databases are identified and some encryption methods are discussed that can help to reduce

Special Issue - 2016

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICRET - 2016 Conference Proceedings

the attacks risks and protect the sensitive data. It has been concluded that encryption provides confidentiality but give no assurance of integrity unless we use some digital signature or Hash function. Using strong encryption algorithms reduces the performance. The future work could be carried out make encryption more effective and efficient.

REFERENCES

[1] Ahmad Baraani-Dastjerdi; Josef Pieprzyk; Baraanidastjerdi Josef Pieprzyk; ReihanedSafavi-Naini, Security In Databases: A Survey Study, 1996

[2] http://en.wikipedia.org/wiki/Database_security

[3] Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, White Paper.

[4] Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009

[5] http://www.freetechexams.com/computerstips/computer-tips/database-security.html

[6] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 – 170

[7] Luc Bouganim; Yanli GUO; Database Encryption;Encyclopedia of Cryptography and Security, S. Jajodia and H. van Tilborg (Ed.) 2009, page(s):) 1-9

[8] Khaleel Ahmad; JayantShekhar; Nitesh Kumar; K.P.Yadav; Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368-372

[9] Gang Chen; Ke Chen; Jinxiang Dong; A Database Encryption Scheme for Enhanced Security and Easy Sharing; Computer Supported Cooperative Work in Design, 2006. CSCWD '06. 10th International Conference on; Publishing year 2006, page(s): 1 - 6

[10] Dr. Anwar Pasha Abdul GafoorDeshmukh; Dr. Anwar Pasha Abdul GafoorDeshmukh; Transparent Data Encryption- Solution for Security of Database Contents; (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011

[11] TingjianGe, Stan Zdonik; Fast, Secure Encryption for Indexing in a Column-Oriented DBMS; 2007 IEEE 23rd International Conference on Data Engineering (2007) Publisher: IEEE, Page(s): 676-685.

[12] Lianzhong Liu and JingfenGai; A New Lightweight Database Encryption Scheme Transparent to Applications; Published in Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference Issue Date: 13-16 July 2008 On page(s): 135 - 140