A Study on Encoding and Security in the Databases

Vemuri Saranya, Ch.V. Phani Krishna

Abstract ***Security has become one of the important challenges in today's worlds that people are facing all over the world in every aspect of their lives likewise security in electronic world has a great significance. In this paper we study the security and encoding in the database. This is an area of firm interest in database because we know that, the use of database is becoming very important in today's enterprise. Databases contain lot of information that is major enterprise asset. This study will exhibit the issues and threats in database security, requirements of database security and how encoding (encryption) is used at different levels to provide the security in the databases.***

Keywords—Databases, Security, Encryption, Access Controls.

I. INTRODUCTION

Data or Information is an important asset in any organization. Almost all organization like social, governmental, educational etc..., have now automated their information systems and other operational functions. They have maintained the databases which contain the crucial information. So database security is a serious concern.

Protecting the confidential data stored in a repository is actually the database security. It will secure the databases from any form of illegal access or threat at any level. Database security demands prohibiting or permitting user actions on the database and the objects inside it. Enterprises or organizations which are running successfully demand the confidentiality of their database. They do not allow the unauthorized access to their information. And they also demand the surety that their data is protected against any malicious or accidental modification. Figure 1 below shows the properties of database security that are integrity, confidentiality and availability [6][7][8].

Confidentiality enforces 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.

Manuscript received on April, 2013.

Vemuri Saranya, Student, CSE Department, K L University ,Vaddeswaram, Guntur Dist, Andhra Pradesh, India.

Ch.V.Phani Krishna, Associate Professor, CSE Department, K L University, Vaddeswaram, Guntur Dist, Andhra Pradesh, India.

Access to the system ensures that all direct accesses to the system are authorized. A lot of time's happen that important information or data is leaked out or misused not because of defective access control but because of improper information flow. When information flows are not properly defined than the system data is less protected.

The cryptographic control secures the data by encoding it. [1][2]

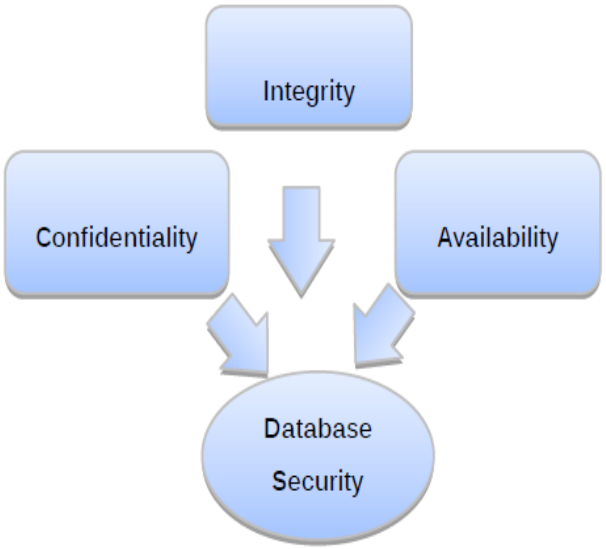

Fig 1: Properties of database security

There is another approach has been adopted for securing the databases. It has been discussed that to make the databases secure different services at organization level can be implemented; information is a most important asset for any organization whose security cannot be compromised. With the advanced 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 services have been anticipated. These services ensure the security features, privacy, confidentiality and integrity.

This study mainly focuses on issues in database security and measures taken to solve those problems. Securing sensitive data from illegal access, theft and forging becomes a big challenge for different organizations like government, no-government, and private sectors. Encoding of data in client or server side where data is shared between different parties is not sufficient. The real problem is to ensure that semi trusted database secure or not. [6] A new technique for database encoding (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 business and protect data privacy against both malicious outsiders and the distrustful database service users without need to know encoding details. [12]

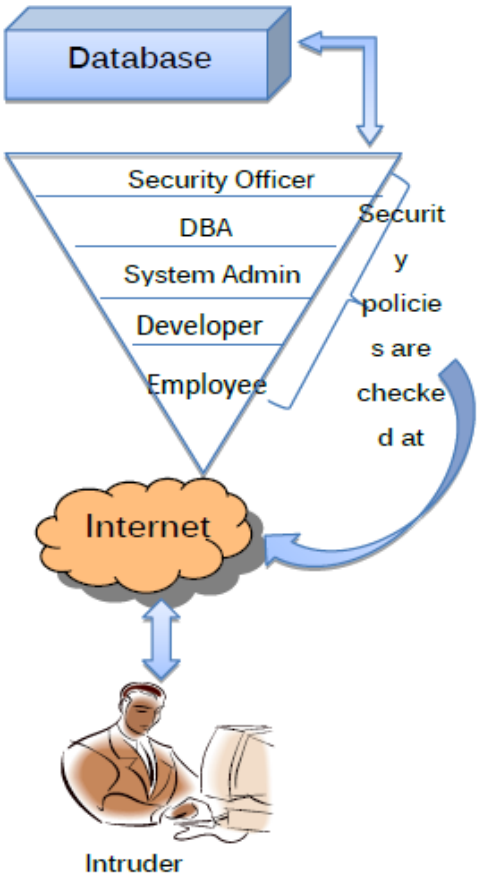

Fig 2: Security layer at organization level

Further in this study we can discuss what actually has been implemented to reduce or eliminate the security threats and how the database security was enhanced in the previous. And we shall see what needs to be performing for securing a valuable asset, the databases of organizations.

A. Organization of paper

This paper is organized into different sections. In section 2, related work to databases security is deliberated. Comparative analysis is presented in section 3 and conclusion is given in section 4. Sketches and future work in section 5

II. RELATED WORK

A. 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]

a. Excessive Privilege Abuse

When users are specified with the access rights that allow them to perform other tasks not included in their job, harmful intention can be discovered through such tasks which leading to misuse of such privileges. For this type an example of university can be quoted in which an administrator who is given access to all databases and holds the privileges 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: Database security risks

b. 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. But it is not limited to any misuse of sensitive data or unjustified use of privileges.

c. 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.

d. Database Platform Vulnerabilities

Vulnerabilities in the previous operating systems versions like 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.

e. *SQL Injection*

Random SQL queries are executed on server by some powerful 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.

f. 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 this poses a serious risk to the organizations databases and may cause instability in operations.

g. Denial of Service (DOS)

It is the attack that prevents the legitimate users of a 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 major threat for any organization.

h. 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.

i. 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.

j. 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 discussed some important threats to database security.

B. Database Security Considerations

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

a. Access Control

Access control ensures that all communication 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 that can make impact as big as stopping firms 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.

b. Inference Policy

It 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 higher security level. It also determines how to protect the information from being disclosed.

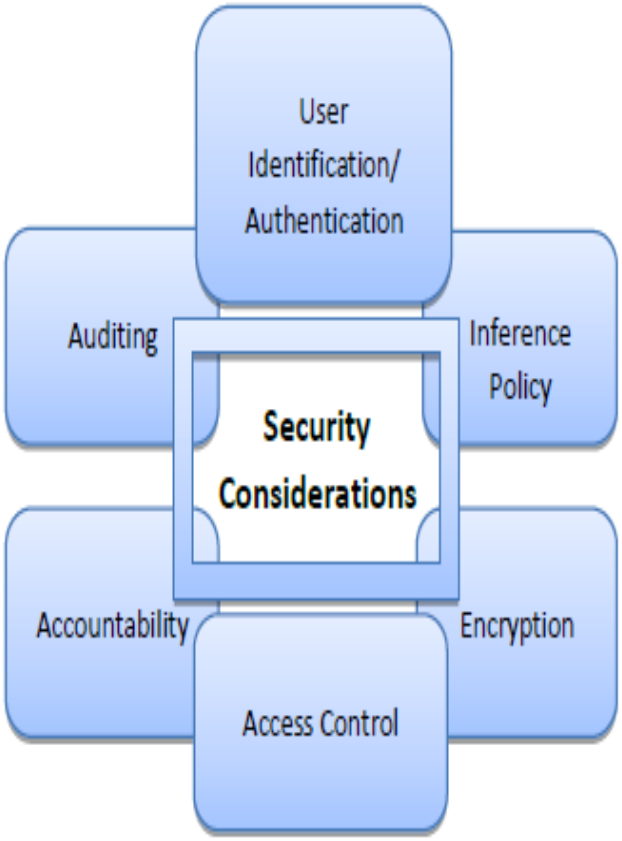

Fig 4: Critical areas under consideration

c. 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 form being modified by any ordinary user.

d. 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.

e. 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 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 view point. A new framework was proposed in which different keys are used different parties to encrypt the databases in assorted from that were named as mixed cryptography database (MCDB). [6]

Though encryption improves the protection but its implementation decisions are also very important. Following figure 5 shows where encryption takes place.

Developing the encryption strategies arises some important questions also, like how, when and where the encryption will be performed.

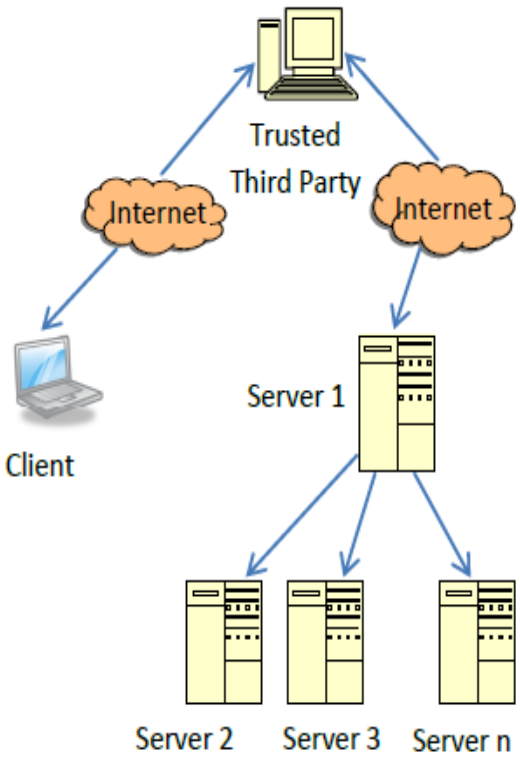

Fig 5: Three levels where encryption is performed

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 mixed cryptography database on performance and security perspectives; second, access control methods used to control access for all parties 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 out sourced 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. i.e. Storage–level encryption, database-level encryption and application-level encryption.

Storage-level encryption encodes 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. 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 at 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 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. 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.

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 whose 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 encryption databases on networks, hard disk and on any back up 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 2008 encryption. This study investigates what Microsoft SQL server 2008's 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. The next section will present the comparison of the study done so far.

III. COMPARATIVE ANALYSIS

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

a. 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.

Table 1: Encryption in databases

Paper	Methods/Techniques	Algorithm	Where encryption can 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 • Untrust 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 Leve
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	X	X

b.Empirical analysis

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

i.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" where as 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 2.

ii.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:

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

Table 2: Frequency of security parameters achieved using encryption methods

Security Bench Marks	Paper 1 [6]	Paper 2 [7]	Paper 3 [8]	Paper 4 [9]	Paper 5 [10]
Confidentiality	✓	✓	✓	✓	✓
Integrity	✓				✓
Access control		✓	✓		
Efficiency			✓		
Privacy	✓	✓	✓		

With the help of data obtained in table1 we can calculate the percentage and criticality.

Table 3: 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

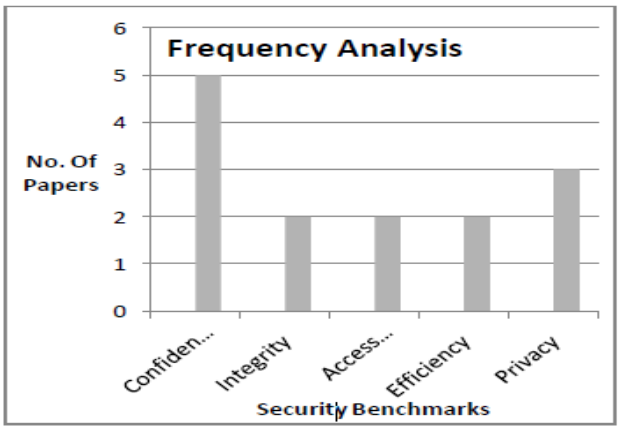

Fig 6: frequency of bench marks achieved using encryption methods

IV. CONCLUSION AND FUTURE WORK

Data to any organization is 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 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; Baraani- dastjerdi Josef Pieprzyk ; ReihanedSafavi-Naini, Security In Databases: A Survey Study, 1996
2. http://en.wikipedia.org/wiki/Database_security 27th Oct, 2010 1:00am
3. Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.
4. Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009
5. http://www.freetechexams.com/computers-tips/computer-tips/database-security.html
6. Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Frameworkfor Database Security based on Mixed Conference on; Publication Year: 2009, Page(s): 163- 1 7 0
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. 10thInternational 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 Transparentto Applications; Published in Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference Issue Date: 13-16 July 2008 On page(s): 135 – 140