International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Security Implications in Database in Web Based Environment

Surya Pratap Singh
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009

Avinash Singh
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009

Upendra Nath Tripathi
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009

Manish Mishra
Department of Electronics
DDU Gorakhpur University
Gorakhpur(U.P.) -273009

***Abstract* - The used of database is very common these days and so as the security of the database is a very important aspect that the current researchers and database professionals are facing. The database becomes more vulnerable to security attacks when we use web based database because different types of hackers and attackers are trying everything to break the security of database. Traditionally the database is assumed to be trustworthy. Under this assumption, the goal is to achieve security against external attacks (e.g. from hackers and attackers) and 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. In this paper we identify the issues and threats in database security, requirements of database security, and how encryption is used at different levels to provide the security and address the problem of defining and achieving security in a context where the database is not fully trusted.**

Keywords* - *Distributed database security, cryptography, biometrics, hashing technique

1. INTRODUCTION

Information or data is the most valuable asset in any organization and is also vulnerable to attacks. Almost all organizations whether it is social, governmental, educational etc. have now automated their information systems and other operational functions.[5][6] They have maintained the databases that contain the crucial information. So database security is a serious concern.

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.[11] Figure 1 below shows the properties of database security that are: confidentiality, integrity and availability

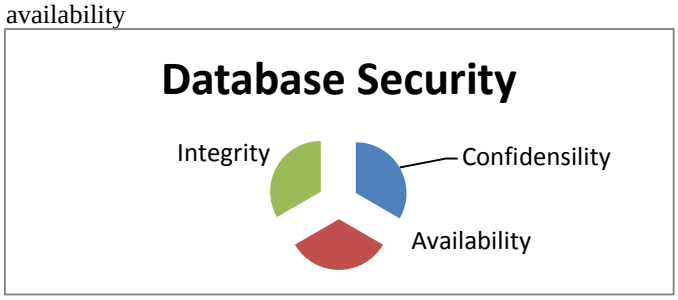

Fig -1 Database security

Classical database security (e.g. see [3]) 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, [8]digital signatures, and other cryptographic mechanisms and protocols. It seems desirable to develop a systematic understanding of database security problems and their solutions and to come up with a framework. Ideally, such a framework should give some assurance that all relevant security problems have been addressed, and it can possibly point out new security issues not previously considered.[9] It is a goal of this extended abstract and the corresponding talk to contribute to developing such a framework and identifying new research directions for fruitful collaborations of the database, the information security, and the cryptography research communities.[15]

2. SECURITY THREATS IN DATABASES

The database organization is subject to variety of threats. Some serious threats are explained in this document.

2.1. 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.[2]

2.2. 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.

2.3. 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.[10]

2.4. 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.

2.5. Weak Audit Trail

A database audit policy ensures automated, timely and proper recording of database transactions.[4] 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.

2.6. 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.

3. REVIEW OF LITERATURE

[1] Zongkai Yang, Jingwen Chen, Du Xu explained no matter what degree of security is put in place, sensitive data in database are still vulnerable to attack. To avoid the risk posed by this threat, database encryption has been recommended. However encrypting all of database item greatly degrades the performance of the database system. As an optimal solution they presents a database encryption scheme that provides maximum security, whilst limiting the added time cost of encryption and decryption

[2]Gang Chen; Ke Chen; propose a novel database encryption scheme for enhanced data sharing inside a database, while preserving data privacy. It is characterized by both the fast speed of the conventional encryption and the convenience of key distribution of public key encryption. It also provides secured storage for security related data and effective key management, which enables the encrypted data to be shared conveniently.

[3] Wen-Chung Kuo, Dong-Jin Jiang proposed the block division method and one bit to record the change of the selected minimum point to replace the record data method using in HKC. According to our proposed method and experience analysis, this reversible data hiding scheme is not only to improve the original data hiding capacity but also to reach the goal of data recovering.

[5]Kadhem, H.; Amagasa, T.; proposed Mixed Cryptography Database (MCDB), a novel framework to encrypt databases over un-trusted networks in a mixed form using many keys owned by different parties The encryption process is based on a new data classification according to the data owner. The proposed framework is very useful in strengthening the protection of sensitive data even if the database server is attacked at multiple points from the inside or outside.

4. CRYPTOGRAPHY IN DATABASE SYSTEM

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.[12][13]

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.[14]

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

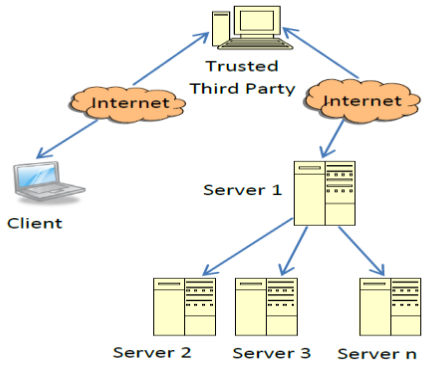

Fig 2- Three tier encryption

5. PROBLEM IN EXISTING SYSTEM –

To protect the database from various types of security threats different types of database researchers proposed different techniques but none of them is fully able to prevent the database from all types of security threats , there are various key areas of the security where they are lacking –

5.1. Most of the existing cryptography system relies on the concept of link encryption which requires a large cost in securing the database as every link have to be secured.

5.2. Another problem with the current crypto graphical system is it relies on the mathematical keys to encrypt and decrypt the data stored in the databases. Although it is hard to break the security of such crypto graphical keys at this time but as the computing system and processing speed are increasing after some years it is possible to break the security of such system.

6. PROPOSED SOLUTION –

To overcome from the problem we explained earlier we propose the following solution

6.1. *Biometrics based cryptography with hashing technique* – in this approach the data in the database are encrypted in the normal way as it is encrypted in the earlier time but additionally the biometrics credentials are used to dually encrypt the data. the data will be encrypted according to the following steps –

Step 1 – the data which is already encrypted is again secured with the biometric credentials.

Step 2 – now the data will be encrypted by using the traditional encryption algorithm.

Step 3 – now hash function will be computed on the data which is now available and the result will be stored in the form of hash value.

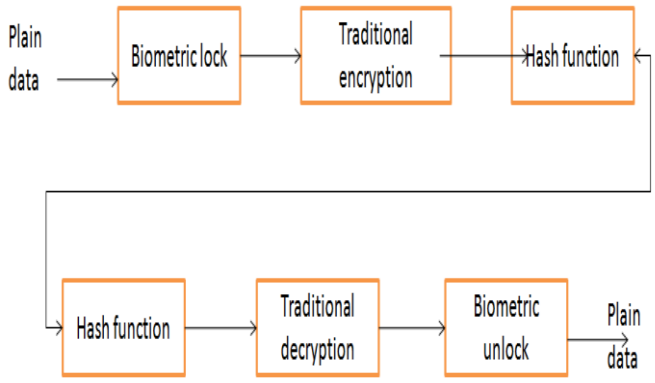

Fig 3 – Cryptography using biometrics

The decryption of the data in the reverse order of the encryption .the benefit of this approach is that if any tempering with the data is done then the hash value computed will not match to that which is stored in the database. As well as if the hash value is right and somehow the attacker decrypts the data but the biometrics will protect the data.

7. CONCLUSION –

The need of the database security is of the prime concern in the current information processing environment because the data is very valuable asset of any organizations. Various techniques are provided for securing the data in the databases but none of the approach is fully able securing the data in every expected threats and vulnerabilities.

In this paper we explain some of the problems in the database and also proposed an biometrics based cryptography system with hashing to secure the database.

8. REFERENCES –

(1) Zongkai Yang, Jingwen Chen, Du Xu, ―A Secure Database Encryption Scheme‖, second IEEE Consumer Communications and Networking Conference (CCNC), 3-6 Jan. 2005, pp. 49- 53.

(2) 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

(3) Samba Sesay, Zongkai Yang, Jingwen Chen, Du Xu, ―A Secure Database Encryption Scheme‖, Second IEEE Consumer Communications and Networking Conference (CCNC), 3-6 Jan. 2005, pp. 49- 53.

(4) Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, ―A Reversible Data Hiding Scheme Based on Block Division‖, Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369.

(5) Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009.

(6) Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol.36, June–July 1929, pp. 306–312.

(7) Lianzhong Liu and JingfenGai; A New Lightweight Database Encryption Scheme Transparent to Applications; Published in Industrial Informatics, 2008.

(8) M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proc. 20th ACM Symposium on the Theory of Computing (STOC),

(9) R. Canetti. Security and composition of multi-party cryptographic protocols. Journal of Cryptology, vol. 13, no. 1, pp. 143{202, 2010.

(10) Q Wang, T Yu, N Li, J Lobo, E Bertino, ―On the Correctness Criteria of Fine Grained Access Control in Relational Databases‖, Proceedings of the 33rd international conference on Very large data bases, 2007, pp. 555-566.

(11) W. G. Halfond and A. Orso. Combining Static Analysis and Runtime
Monitoring to Counter SQL-Injection Attacks.2005

(12) The contents are available at: www.wikipedia.com

(13) Vulnerability Management in Web Applications R. Thenmozhi, M. Priyadharshini, V. VidhyaLakshmi, K. Abirami http://www.ciitresearch.org/dl/index.php/dmke/article/view/DMKE042013007

(14) David Litchfield: Web Application Disassembly with ODBC Error Messages

(15) C. Gould, Z. Su, and P. Devanbu. Static Checking of Dynamically Generated Queries in Database Applications. In Proceedings of the 26th International Conference on Software Engineering (ICSE 04), pages 645–654, 2004.

Author's Profiles

Surya Pratap Singh is MCA and UGC-NET qualified and pursuing Ph.D. In the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Database Security, Networking. Mr. Surya Pratap Singh has published 10 papers in different national and international conferences/ Journals.

Dr. Upendra Nath Tripathi is Assistant professor in Department of computer science DDU Gorakhpur University, Gorakhpur (U.P. India). He has 13 years of teaching and research experience. He has published 45 papers in various National and International Journals/conferences. His area of research interest is database systems, networking.

Avinash Singh is M.Sc. Computer Science, M.Tech and M. Phil and pursuing Ph.D. in the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Database Security, Networking. Mr. Avinash Singh has published 20 papers in different national and international conferences/ Journals.

Dr. Manish Mishra is Assistant professor in Department of Electronics DDU Gorakhpur University, Gorakhpur (U.P. India). He has 13 years of teaching and research experience. He has published 50 papers in various National and International Journals/conferences. His area of research interest is Computer Technology, fast processor design.