International Journal of Database Theory and Application
Vol.8, No.3 (2015), pp.49-56
http://dx.doi.org/10.14257/ijdta.2015.8.3.05

# Analytical Approach for Security of Sensitive Business Database

Anusha Gupta[1] and Sanjay Kumar Dubey[2]

*Computer Science & Engineering Department*
*ASET, Amity University, Noida (U.P)*
*[1]anushagupta520@gmail.com, [2]skdubey1@amity.edu*

## Abstract

*Sensitive database security is an integral part to meet the company's abeyance. Securing the sensitive data in mixed database environment has increased over the past few years. This paper conducts the literature review about providing solutions to secure all databases. This will help the users to know what all things are required to be protected when they are planning to protect the database. Sometimes in some of the business it requires highest level of security even if the performance is being compromised. So, this paper will help user to choose appropriate security mechanism to for the sensitive database according to their business requirement. A brief view of securing the network, server and operating system is also provided in the present paper. Aim of this research is to provide the security to sensitive data at all the three levels physical security, network security, information security from unauthorized user.*

**Keywords:** *Sensitive database, Business data security, Network Security, Operating System Security, Server Security.*

## 1. Introduction

Over the past few years the assemblage of sensitive data in database has accomplished terabyte in many business organizations. Many users and the applications from inside and outside are accessing the sensitive data from the database. Sensitive data in business includes employees personal details such as PAN card number, passport number, bank account, medical records, employee credit card details, identification details of employee etc and most importantly the company details such as financial details, tender details, contract information, configuration of firewalls etc. [1]. Database and the data within them specially is the primary target for most of the intruders. In the current scenario the database security is the major security issue that is to be considered especially when it comes to the need of enhanced security of sensitive data in business [2].

Database security does not mean securing the information present in the database but instead it means physical security, network security, information security etc. from unauthorized user. Physical security means securing the server and the system. It is one of the important parts of securing the information technology. Physical security includes the security of the hardware of the system, servers, back-up media and any other elements required for system operation such as laptops, computers and also other computing devices as well which are required to be protected from theft. Extreme care and security required for the device containing sensitive data and personal information. Network security includes security of the assets of the organization and the entire network traffic. It covers a wide variety of computer networks both public and private which are used every day. It includes transactions and communication among business, government agencies and individuals. Due to various active and passive attacks these days it is subjected to the need of network security. Information security is the act of providing protection to information from unauthorized user, its disclosure and modification.

ISSN: 2005-4270 IJDTA

So database security is very much needed in business whether the data is in use or at rest, especially when it is in use it needs to be handles carefully [3]. Database managers are required to do a lot of task for the maintenance of a secure database.

**Table 1. Levels of Security**

| Security levels | Involves |
|---|---|
| Physical level | Securing server system, wiring locations used for connection |
| Network level | Securing assets of organization and network traffic |
| Informational level | Security of information from unauthorized access. |

There are several issues that are related to business database security such as broken databases, windows operating system flaws, deployment failures, lack of segregation management of user passwords, application spoofing and various methods of security for applications, stolen database backups, post upgrade evaluation, data leaks ,daily maintenance, abuse of database features etc. The simplest way to avoid such problems is to hire qualified person and assign individuals the separate responsibilities from daily maintenance responsibilities.

Sometime it happens that companies have several types of databases so in order to ensure total security across database they hire third party database security vendors as their first option. Those companies have solutions for DAM i.e. Database Activity Monitoring. Another option is data masking that means buying a fake data set for testing and development. The next section of the paper includes literature review, Section III, discusses about the research methodology adopted to extract the relevant information. Database security is needed to prevent the data access from unauthorized user and misuse, data corruption, preventing the database from programming bugs, protection from malware functions and data leakage. Sensitive data is the confidential information of organization thus it requires highest level of security. This review paper will provide the idea of how to identify sensitive data from database and what all things requires security such as security of network, server, and operating system.

## 2. Research Methodology

The method being used for finding out the multiple ways of securing the security to the sensitive database from the available research work done by various researchers relevant to the specific area of interest. In order to do research done following steps are being carried out.

(i) Selection of the relevant research papers by various authors. It provides the relevant information about the sensitive data and its security.
(ii) Gathering the useful information
(iii) Extraction of relevant information.
(iv) Data Deduction in tabular form.

## 3. Literature Review

Now a days security of sensitive data is the major issue of concern as reported in the earlier incidents in the form of loss of data, unauthorized access of sensitive data. And since the data is being shared among various server digitally here arises the need of better understanding of sensitive database security, Traian Popeea and their co researchers have stated in their work[1]. The data which we are storing in the database or computer is growing very rapidly and the people who want to access those databases are also growing rapidly therefore the database security has become essential day by day. Database security has become the popular computer research area since 20th century [5].

### Table 2. Comparison Table of Various Techniques and Methods for Secure Database

| S. No. | Reference | Year | Techniques used | Dataset used | Methodology | Analysis |
|---|---|---|---|---|---|---|
| 1. | [6] | 2004 | Data Encryption Standard | DBMS layer: MAC and trusted subjects, unique key | (i)Encryption of sensitive data before being stored.<br>(ii)Only cryptographic keys are to be protected. | Security maximized, whilst limiting and reduction of time in encryption and decryption |
| 2. | [7] | 2006 | Advanced Encryption Standard | Public keys are being used for encryption in column and cell of the table. | (i)Key management and mechanism of security catalog.<br>(ii)Encryption and decryption in column and cell. | Preserves confidentiality of sensitive data, resist attacks, high security performance and easy sharing of encrypted data |
| 3. | [8] | 2008 | Encryption decryption engine, threat model | Metadata in Security dictionary to keep metadata safe. Indexing for fast query processing. | (i)Encryption is being used as service to applications.<br>(ii)Encrypted data, catalog at DB side and encryption/ decryption processing in the outer module and metadata at trusted middle side. | Data protection without encryption details, flexible data granularity and safe key management for high performance, security and also lightweight encryption, fast query processing capability. |
| 4. | [9] | 2008 | Policy based frame work | Policy based request for accessing or making changes in the database. | (i)Before allowing or rejecting or reflecting the change embedded capability is being used for comparing security configuration parameter and pre defined security rules. | Autonomic capability of self database security. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5. | [5] | 2008 | Security model applied to Logic SQL DB | Mandatory Access Control (security rules and security model axiom) | (i)Lock and logical concurrent control. | Security and integrity are joined in Logic SQL DB security model, reasonable security level, secure OS and other systems. |
| 6. | [11] | 2009 | Fine Grained database access control model | Security criterion abstraction and object, user generation etc. | (i)Controlled access to handle network security.<br>(ii)Prime access is merged within the firewall functions and fine grained access is based on user's digital details such as IP address. | Improves efficiency, network security, Access termination of user at earlier stage avoids unnecessary request processing. |
| 7. | [12] | 2009 | Security model | Grant and revoke request for access. | (i)Emerging security used in distributed system tools.<br>(ii)Proper integration of all Operating System, server, applications, web, network | Multi level access control, easy recoverability, reliability and integrity. |
| 8. | [13] | 2009 | Object oriented concepts. | MAC and DAC | (i)Access based on content of data.<br>(ii)Role based access control. | Flexible way of managing |
| 9. | [14] | 2010 | Security monitoring system based on IDS. | Intrusion detection, tolerance and static data protection sub system. | (i)Combined static and dynamic protection.<br>(ii)Detection and tolerance capable. | Intrusion tolerance and detection , static data protection, system service continuity. |
| 10. | [15] | 2010 | Gateway to detect SQL attacks. | Module for attack protection, audit, to monitor etc | (i)Secure rule library<br>(ii) Improvement in Sunday pattern matching algorithm.<br>(iii)Filtering SQL statement. | Transparent security gateway, detects SQL injection attacks, efficient pattern matching. |
| 11. | [16] | 2011 | Logic SQL DB System. | Logic log protocol for concurrent control, protocol for parallel | (i)Concurrency control by logic log protocol.<br>(ii)Parallel access control with centralized | Audited events increase the security of search system. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | access. | access control. | |
| 12. | [1] | 2012 | Multi layer approach | Split queries. | (i)Inference detection for secured communication.<br>(ii)Anonymity of data. | Prevent inference base attacks, multiple layers of security . |
| 13. | [18] | 2012 | Graphics processing unit. | Keys, encryption algorithm, initialized vector, block cipher modes | (i)Applying graphics processing model to database. | Parallel data processing, improved performance. |
| 14. | [19] | 2013 | TSFS algorithm | Transpose substitute folding and shifts | (i)TSFS algorithm to all including special characters.<br>(ii)Substitution and shifting | Fast data access and storage, improved performance without compromising processing time. |
| 15. | [20] | 2014 | RSA and AES encryption algorithm. | Public key, private key and secrete key. | (i)Hybrid encryption<br>(ii)Upload and download of data in cloud. | Secure upload and download of data in cloud even integrity is maintained. |

## 4. Analysis

After the intensive identification of relevant information by using research methodology the analysis is provided in following sub sections:

### 4.1. Identification of Sensitive Data

One of prime task in sensitive database security will be the identification of the sensitive data. There are several factors which can classify the data to be sensitive. First is that the value of data itself is so confidential and revealing that it becomes sensitive. Second one is that the data belongs to some sensitive source. Third is that a particular attribute or record have been already declared as sensitive in database. Fourth is that some data becomes sensitive in relation to the previously disclosed data. Fifth is that the owner of the data has explicitly declared it as sensitive.

### 4.2. Prevention of Misuse of Data Leakage

It is well said that the prevention is better than cure so if possible one should try to protect the data from being misused. But of course every data leakage and misuse cannot be prevented thus comes the need of data leakage and misuse detection.

### 4.3. Misuse Detection

Next step will be misuse detection and further securing the database. For detecting the misuse in database misuse detection system can be used. DEMIDS (Detection of Misuse in Database Systems) is the system being used which contains set of tools to derive users profiles from audit logs. Such profiles actually describe distinctive access patterns of system users by specifying the typical values of features that are audited in the audit logs. The profiles are used for detecting the misused behavior. It is used to detect both inside and outside misuse. DEMIDS is used to detect malicious behavior of legitimate users who tries to misuse the privileges. Misuse detection in database can be done for host as well as for the network. Host misuse detection will focus upon the daily activities performed by the user. Network misuse detection will focus on DB query, file system access etc.

Another ways to prevent data leakage and misuse detection from authorized user is misuse ability weight concept for data leakage and misuse detection[8].Once the misuse or data leakage is being detected the next step will be to provide the security to the sensitive database throughout starting from its creation to transmission to its deployment till its destruction.

### 4.4. Securing Database Using Encryption

The sensitive data stored in the database are vulnerable to attacks no matter up to what level of security is being provided. There will always be some security leakages which are being used by the intruders to penetrate database. If encryption of sensitive data is done before storing security leakage can be eliminated to a certain extent. And the only protection required will be of protecting the cryptographic keys. One of the best ways to secure database is through encryption. But since it is the sensitive database therefore it requires an extra more care while its encryption. We can encrypt the database using any of the encryption algorithms such as DES (Data Encryption Standard) or RSA (Rivest Shamir Adleman). In DES encryption algorithm same key is being used for encrypting and decrypting the message so that the same private key is being used by the sender and receiver. In RSA both public and private keys are used to encrypt the message, the opposite from the one used to encrypt a message is used to decrypt it. Because of this reason RSA is popularly used asymmetric algorithm. Another way could be to use "A new light weight database encryption scheme transparent to applications." according to which encryption can be provided as service to applications to order to avoid excessive access to database and in order to keep encryption metadata safe security dictionary is used [3].

### 4.5. Database Security Using Watermarking

Sensitive data cannot always be the text but it can also be the images one of the way to secure sensitive image based data the water marking. Watermarking is the process of hiding the digital information in a carrier signal.

### 4.6. Securing Operating System

Security of operating system is equally important. If the Linux operating system is being used then it provides security to user by making use of authentication features such as protection of password or controlled access of particular file by maintaining ACL(Access Control List) and also by giving access permission to certain users and the encryption of data using RSA key exchange algorithm. Security in Linux operating system is one of its key features [16]. Else if we are required to give the security to the MAC address based operating systems such as windows operating system then "A Formal Multilevel Database Security Model" can be used according to which multilevel database security model is applied in LogicSQL database management system[5]. This multilevel model increases integrity. It is applied in LogicSQL DBMS systems. Direct access control and mandatory access control is applied. The formal multilevel security model can also used to secure OS and other systems

### 4.7. Securing Network

Due to the excessive use of internet, web, distributed database and intranet it has become essential to handle the web and network security properly. The proposal given by Leon Pan can be used for securing the network. They proposed the integration method of network security and fine grained web based data access control simultaneously. Due to this the efficiency will be improved. In this case firewall junction and preliminary access control is being combined, and access permission is provided on the basis of users digital details and other factors such as IP address[11]. Transmission of data is done through SSL (Secured Socket Layer) [1].

### 4.8. Securing Server

Most important assets that the company owns are servers [6]. Securing the server is the yet another issue. In Linux, security mode is chosen in Samba server. Share level and user level are two types of security. Collectively they are known as security levels. User level security can be set by smb.conf as security=user. And share level security can be set by smb.conf as security=share.

## 5. Conclusion

Securing the sensitive database in business involves securing the server, network , wiring , information everything. It is not an easy task to provide multiple security levels at each place but if required it becomes necessary to do so. Especially when there is the need to secure the financial details of the company and its employees and their personal information then securing everything is really important. Sometimes in some of the business it requires highest level of security even if the performance is being compromised. But in some of the business performance is much more important. In that case the security can be compromised to a certain level. Apart from that the security of sensitive data in database is equally important. Thus it is the need of securing the database at all the three levels that is physical level, network level and informational level.

## References

[1] T. Popeea, A. Constantinescu, L. Gheorghe and N. Ţăpuş, "Inference Detection and Database Security for a Business Environment", International Conference on Intelligent Networking and Collaborative Systems, **(2012)**, pp. 612-617.

[2] P. Wang, L. Xing, X. Gu1, C. Zhu, "Design and Implementation of Security Enhanced Module in Database", International Conference on Internet Computing for Engineering and Science, **(2013)**, pp. 60-62.

[3] L. Liu and J. Gai, "A New Lightweight Database Encryption Scheme Transparent to Applications", International Conference on Industrial informatics, **(2008)**, pp. 135-140.

[4] K. K. Hingwe and S. M. Saira Bhanu, "Two Layered Protection for Sensitive Data in in Cloud", International Conference on Advances in Computing, Communications and Informatics (ICACCI) **(2014)**, pp. 1265-1272.

[5] W. Baohua, M.A. Xinqiang, L.I. Danning, "A Formal Multilevel Database Security Model", International Conference on Computational Intelligence and Security, **(2008)**, pp. 252-256.

[6] S. Sesay, Z. Yang, J. Chen and D. Xu, “A Secure Database Encryption Scheme" In Second IEEE Consumer Communications and Networking Conference (CCNC), **(2005)**, pp. 49-53.

[7] G. Chen, K. Chen, J. Dong, "A Database Encryption Scheme for Enhanced Security and Easy Sharing", International Conference on Computer Supported Cooperative Work in design, **(2006)**.

[8] R. K. Bhat and N. V. Mahajan, “A Technique for Avoiding Data Leakage and Misuse", IJARCSMS, **(2008)**, pp. 260-265.

[9] D. A. Menasc´e and G. ‘Gus’ Jabbour, "Policy-Based Enforcement of Database Security Configuration through Autonomic Capabilities", International Conference on Autonomic and Autonomous Systems, **(2008)**, pp. 188-197.

[10] A. Zahid, R. Masood, M. Awais Shibli, "Security of Sharded NoSQL Databases", International Conference on Information Assurance and Cyber Security(CIACS), **(2014)**, pp. 1-8.

[11] L. Pan "A Unified Network Security and Fine-Grained Database Access Control Model”, International Symposium on Electronic Commerce and Security, **(2009)**, pp. 265-269.

[12] Z. S. Zubi, "On Distributed Database Security Aspects", International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, **(2009)**, pp. 231-235.

[13] S. Imran and I. Hyder, "Security Issues in Databases", International Conference on Future Information Technology and Management Engineering, **(2009)**, pp. 541-545.

[14] Z. Xing, H. Wei, "The Structure Design of Database Security Monitoring System based on IDS", International Conference on Computer Engineering and Technologyv (ICCET), **(2010)**, pp. 450-453.

[15] X. R. D. Liwu and G. Jian "A Database Security Gateway to the Detection of SQL Attacks", International Conference on Advanced Computer Theory and Engineering, **(2010)**, pp. 537-540.

[16] X. Ma, Y. Huang and D. Li, "Study on LogicSQL Database System in Security Problems", International Conference on Database security, **(2011)**, pp. 532-536.

[17] D. Liu and S. Wang. Programmable "Order-preserving Secure Index for Encrypted Database Query" in International Conference on Cloud Computing, **(2012)**, pp. 502-509

[18] I. Jeun, H.-C. Jung and N. K. Lee, "Database Encryption Implementation using Graphics Processing Unit", International Conference on Mobile, Ubiquitous, and Intelligent Computing, **(2012)**, pp. 109-113.

[19] H. A. Al-Souly, A. S. Al-Sheddi, H. A. Kurdi, "Enhanced TSFS Algorithm for Secure Database Encryption", Science and Information Conference, **(2013)**, pp. 328-334.

[20] V. S. Mahalle and A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", International Conference on Power, Automation and Communication (INPAC), **(2014)**, pp. 146 – 149.

[21] T. Ge and S. B. Zdonik, "Secure Encryption for Indexing in a Column-oriented DBMS", International Conference on Data Engineering, **(2007)**, pp. 676-685.

## Authors

**Anusha Gupta** is pursuing her Master of Technology from Department of Computer Science & Engineering, Amity University, Noida (U.P). Her area of interest is Database Security, Data Mining and Big Data Analytics.

**Sanjay Kumar Dubey** is Assistant Professor in Department of Computer Science and Engineering in Amity School of Engineering and Technology, Amity University Uttar Pradesh, India. He has 13 year of teaching experience. He is member of IET and ACM digital library. He has a rich academics & research experience in various areas of Computer Science. His research areas include Object Oriented Software Engineering, Soft Computing, HCI, Cloud Computing and Data Mining. He has published more than 55 research papers in indexed National & International Journals and in Proceedings of the reputed International/ National Conferences. These publications have good citation records. He has authored 2 books also. In addition, he has also served as a Technical Program Committee Member of several reputed conferences.