IJCTA, 9(12), 2016, pp. 5765-5769

Joint Threshold Administration Model in Relational Databases to Enhances the Security

***A.Yovan Felix **Pamila. A**

Abstract : Data mining is a subfield of computer science which is used to extract the necessary information from a large datasets. There are significant challenges adopted to enhance the security of the databases with the guidance of data mining. Moreover there are numerous illicit behaviours which possess leakage of sensitive data. The security is enhanced to an extent in the databases. When considered to the relational databases the security is not much enhanced. In the existing system, the relational databases have large number of tables under the administrator. If the admin password is hacked then all the sensitive information of the users can be accessed. To overcome this disadvantage, the Joint Threshold Integration Model (JTIM) is introduced which generates a 64 bit key. The 64 bit key is distributed among all the admins equally for accessing the information in the relational databases. The key is changed every time and sent as a email alert to the admins. For accepting a Request at least Two 3rd Majorities has to be proved. All the individual Keys are concatenated to form the Original Key which is compared with the Server. Thus a trusted hardware based relational database is generated to secure the confidential information.

Keywords : Data Mining, Security, Database, Administrator, Relational Database.

1. INTRODUCTION

The benefits of outsourcing the data and protection of the data is a great challenge. In a relational DB, the security of the data is not much concentrated. There are many chances by which the data can be hacked by insider or an third party. The privacy and confidentiality of maintaining the data are to be noted well. In the existing researches, the privacy access and searches are encrypted in the relational DB. But there are arbitrary functions which allow the computations of decrypting the input data easily. Thus it leads to lack of data Security. The main objective of the proposed work is to provide a trusted h/w (Bluetooth ID) which is generally based on the relational DB which ensures full data confidentiality and data security. The Joint Threshold Integration Model (JTIM) is implemented for obtaining the request from the admin. By implementing JTIM the server verifies the Username, password, w-ordinated bit key and Bluetooth ID of the admin and only if it is matched the data is provided. The co- ordinated bit key changes for every next upcoming request. So the method of hacking the data is reduced completely.

2. OBJECTIVE

A trusted hardware based relational database with full data confidentiality, Ensures Data Security and Finally Assures Request is handled & Processed by Correct Data Administrators only. We also implement Joint Threshold Integration Model (JTIM) for Obtaining Threshold based Request Acceptability.

* Associate Professor, Faculty of Computing, Sathyabama University, Chennai, India yovanfelix@gmail.com

** PG Student, Dept. of CSE, Sathyabama University,Chennai,India. ppamila3@gmail.com.

3. PROBLEM DEFINITION

We address several problem in security aspects, including access & Mishandling. The Problem is even a Hacker or an Attacker can act as a Original / Legitimate Administrator and can send the Illegal Request which can be updated in the Main Database. There is no Proper Security System is implemented so far. Only encryption Technique is Achieved. That too in Banking Sector Most Secure Process is required to be implemented.

4. LITERATURE SURVEY

G. Aggarwal et.al, has presented paper on "Two Can Keep a Secret: A Distributed Architecture for Secure Database Service". The recent trends towards database outsourcing are clearly explained. The laws governing the data privacy is clearly given to enhance the interest in enabling the secure DB Services. The existing system of the paper deals with the external DB Service. The data which is to be stored in external DB is first encrypted in the client side. This method enables the secure DB service. It decomposes the data from which they are optimized and then are executed in the distributed system. The attribute values are hidden to maintain privacy. But the disadvantage is that the viability of the architecture must be checked. Special techniques for optimization are not given. This must be enhanced in the future.

Alexander Iliev et.al, has presented the paper "Protecting Client Privacy with Trusted Computing at the server ".The paper discuss about the trusted computing architecture. The existing system shows the way of having a physically protected component in an external organization. The main aim of the paper is to design and prototype TC at the server which is to enhance the client privacy. Considering the privacy problems, the public key Infrastructure (PKI) is designed which provides Secured TC. The Square root algorithm is introduced which randomly permutes the contents of the record. This algorithm has the ability to retrieve I rewards at one time. The prototype design consists of three coprocessors which is used to handle retrievals. The method of enhancing the performance in the DB is given but the secure hardware has limitations. The system memory is low which is to be enhanced in the future.

Bishwaranjan Bhattacharjee et.al, has presented a paper on "Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis ". The paper discuss about the facts of using secure processors for traditional use. The secure coprocessorsystem eliminates the Physical Security measures. This is due to the hardware miniaturization which are very powerful. This paper brings out a solution for preserving the privacy in data sharing and mining by using cryptographically secure processors. But it has resource limited co-processors. The data which is transmitted through coprocessors is encrypted and is protected from eavesdroppers. Even when the data is decrypted at the trusted environment the data is secure. Further the process of joining, mining and analysing the data is done with the help of seared co-processor. These secure processors are more powerful and also provide better hardware miniaturization. The future work is to provide multiple secure processors with high speed and privacy.

Mustafa canim et.al, had presented a paper known as "Building Disclosure Risk Aware Query Optimizer for Relational Databases" which gives detailed information about the methods of building encryption techniques concerned to various organizations. The paper gives the solution which us quite effective in preventing data leakage from stolen storage devices. The cryptographic keys are used to decrypt the sensitive information. The disclosure risk is minimized by using encrypted data in relational DBMS. To reduce the effect of various attacks on sensitive data, the Transparent Data Encryption (TDE) method is used. TDE provides encryption applications. The cryptographic key known as database master key (DMK) guarantees the secrecy of the data. All the DMK'S are

protected by the Service Master Key (SMK). But this model does not prevent data disclosure if the attacker attacks the main memory itself. The future enhancement is to provide query optimization techniques which will provide protection to sensitive data at lower cost. Future a framework must be done which prevents the attacker from modifying the contents of main memory.

Yao chen et.al, has presented a paper "To Cloud or Not to Cloud? Musings on Costs and Viability" which helps us to know the way in which cloud computing is used in different types of application and to know the method of saving the cost. The paper mainly focuses on two scenarios. The first scenario is "unified client". It gives the result that applications are accessible by a single user. The savings of cost is in a high rate. The next scenario is "multi- client" There are many parties handling the same applications. The network integration must be fairly good for the multi-client scenario to work properly. In both the scenarios the computing is embedded. So they are very cheap and provides high speed communication infrastructure at different levels which is applied in global information exchange and interaction of cloud mitigation viability is clearly explained. The unified client applications has achieved the cost savings at sufficient level at the client cloud network distances. In the third-party client the feasibility equation changes dramatically. This is due to dominating cost of networking. The future enhancement is to increase the availability and the global distribution of the data.

5. EXISTING SYSTEM

There are several problems accessing the control access mishandling and security aspects. It is based on the act that the attacker or hacker can act as original or legitimate user. This leads to the process in which the illegal request is updated in the main database. The security system is not properly implemented in the relational database only. The encryption is being implemented. . The Relational database has lot of Administrators to Control Every Tables. Each Admin is authorized to control their own Corresponding Tables only. If the admin password is hacked, then Data Changes and Updating can be preceded by the Hacker himself.

Overall, despite the overheads and performance limitations of trusted hardware, the costs of running database are orders of magnitude lower than any (existing or) potential future cryptography-only mechanisms. Moreover, it does not limit query expressiveness. Tamper resistant designs, however, are significantly constrained in both computational ability and memory capacity which makes implementing fully featured data- base solutions using secure coprocessors very challenging. Databases achieve this by utilizing common unsecured server resources to the maximum extent possible. For example, databases enable the secure coprocessors to transparently access external storage while preserving data confidentiality with on-the-fly encryption. This eliminates the limitations on the size of databases that can be supported. Moreover, client queries are pre-processed to identify sensitive components to be run inside the SCPU. No sensitive operations are off-loaded to the untrusted host server. This greatly improves performance and reduces the cost of transactions.

6. DRAWBACKS OF EXISTING SYSTEM:

1. **Easy to hack the password :** Since there is a single administrator in a relational database, it is easy to hack the password. If the password is hacked, then all the important details can be stolen.
2. **Low security :** Generally in Relational Database, each database is connected to other database. If the password is hacked, all the databases can be easily accessed by the unauthorized user. This causes a lower security range in the relational database.
3. **Only Encryption is achieved so far :** Any request to be accessed is generally done by the query execution. Each query given by the user is encrypted and sent to the admin. No other security measures are done.

7. ARCHITECTURE DIAGRAM

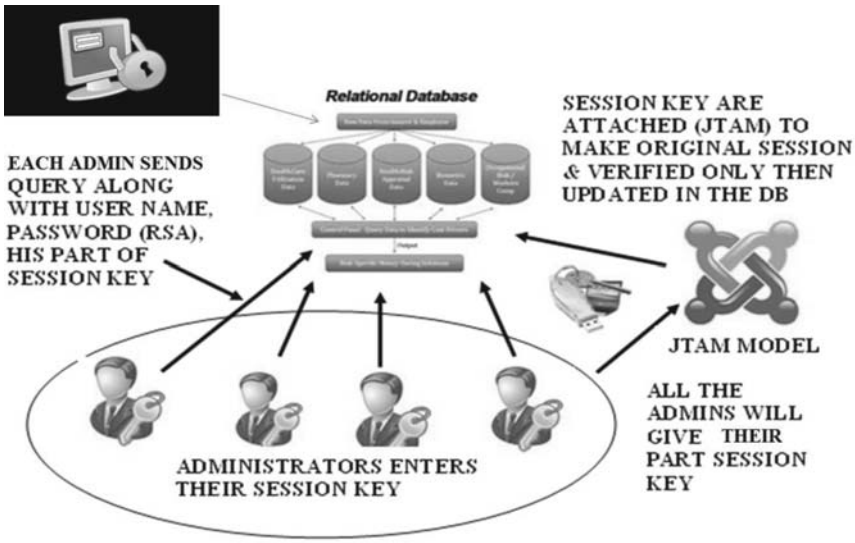

Fig 1. Architecture diagram of the Joint Threshold Administration Model

8. PROPOSED SYSTEM

The proposed system deals with the Joint Threshold Integration Model which provides security to the relational database. Data is Encrypted and the Query is verified with the corresponding Key and the Hardware ID of the Admin and only then the Data is Transmitted or updated to that Admin. The fig clearly explains the Joint Threshold Integration Model which generates a 64 bit key and is divided into smaller parts based on the number of admins present. The key is generated when the admin request is beyond the scope. The Session key provided by all the Admins are integrated and compared with the Original Session Key. The modification of the data can be done only if the session key is matched. The Bluetooth Hardware ID is used for user authentication. For Every Request made by different Admin 64

Bit Key is Generated and Divided into Smaller parts based on the available Admin users. As a part of Approval of the requested data all the Admins are supposed to get login and provide their 16 Bit Key along with their Bluetooth ID. Server verifies user name, password and generated session Bit key and Bluetooth ID used for authentication, only then the data is updated. This Generated 16 Bit Key is sent as E mail Alert to all the Admins. This 64 Bit key will be changed for every Request.

9. ADVANTAGE OF PROPOSED METHOD:

1. **More secure :** The proposed method show the way of protecting the queries in an encrypted and all the actions performed by the admin and the user are in a secured form.
2. **Prevention of Illegal Activity :** As all the queries are sent by the user as a request to the admin are in the encrypted form, all the illegal activities tried to be performed by the hacker are prevented.
3. **Data is accessed and updated securely :**Since all the data operations are performed in an encrypted format, the accessing and updating of the data is done in a secured way.
4. **Session key is updated for every request :** The session key which is generated changes for every request. This prevents the hacker from knowing the session key.

10. FUTURE ENHANCEMENT

Finger print based user authentication scheme can be included along with the normal User Name, password, Bluetooth ID, Session key. This system will ensure much more secured process of Authentication.

11. CONCLUSION

Thus the security in relational database is enhanced with the Joint Threshold Integration Model. The confidentiality of the data is provided by the encryption and the session key generation. A novel based approach is introduced which provides the information for the relational databases. A trusted hardware is implemented which provides the limited privileges even to the administrators to enhance the security to the Relational Databases. The information is encrypted from the hackers and every information are transmitted in a secure way. A trusted hardware is designed and developed with full data confidentiality and security.

12. REFERENCES

1. G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, and Y. Xu, "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services," Proc. Conf. Innovative Data Systems Research (CIDR), pp. 186-199, 2005.
2. A. Iliev and S.W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," IEEE Security and Privacy, vol. 3, no. 2, pp. 20-28, Mar./Apr. 2005.
3. B. Bhattacharjee, N. Abe, K. Goldman, B. Zadrozny, C. Apte, V.R. Chillakuru, and M. del Carpio, "Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis," Proc. Second Int'l Workshop Data Management on New Hardware (DaMoN'06), 2006.
4. M. Canim, M. Kantarcioglu, B. Hore, and S. Mehrotra, "Building Disclosure Risk Aware Query Optimizers for Relational Data- bases," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 13-24, Sept. 2010.
5. Y. Chen and R. Sion, "To cloud or Not to Cloud?: Musings on Costs and Viability," Proc. Second ACM Symp. Cloud Computing (SOCC '11), pp. 29:1-29:7, 2011.
6. R. Gennaro, C. Gentry, and B. Parno, "Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers," Proc. 30th Ann. Conf. Advances in Cryptology (CRYPTO '10), pp. 465-482, 2010.
7. V. Ciriani, S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining Fragmentation and Encryption to Protect Privacy in Data Storage," ACM Trans. Information and System Security, vol. 13, no. 3, pp. 22:1-22:33, July 2010.
8. T. Denis, Cryptography for Developers, Syngress, 2007.
9. E. Damiani, C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs," Proc. 10th ACM Conf. Computer and Communications Security (CCS '12), 2003.
10. E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th IFIP WG 11.3 Working Conf. Data and Applications Security, pp. 89-103, 2006.
11. T. Ge and S. Zdonik, "Fast Secure Encryption for Indexing in a Column-Oriented DBMS," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), 2007.
12. V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth Int'l Workshop Privacy and Anonymity in the Information Soc. (PAIS '11), pp. 8:1-8:10, 2011.
13. Indhumathi.V and Prakasham V "On Demand Security for Personal Health Record in Cloud Computing", Proc IEEE 2nd Int'l conf. on innovation in information Embedded and Communication Systems.(ICIIECS), 2015.
14. Sharmila R. and Shanthi A.V.K " A survey on Privacy Preserving Homomorphic in Collaborative Data Publishing" Proc. International Journal of Engineering and Computer Science, volume 3-no.3, march-2014.