International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 2 080 - 084

Multilevel Hashing based Access Control for Authentication and Security in Relational Database Management System

Mr. Surya Pratap Singh*
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009
spsingh8161@htomail.com

Dr. Upendra Nath Tripathi
Department of Computer Science
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009
untripathi@gmail.com

Dr. Manish Mishra
Department of Electronics
DDU Gorakhpur University
Gorakhpur (U.P.) – 273009
manish.ddu1976@gmail.com

***Abstract*—**The relational database is very widely used in these days and so as the relational database security is very vital to protect from different kinds of threats and attacks. The security of relational database is very important because now these days all data and information are stored in database by some form of database objects including user's personal information like credit/debit card details, username, passwords etc. as well as confidential data of business organization and companies. Many researches are done in order to protect the relational database from these vulnerabilities but the methodologies of relational database security are not able to protect the relational database from all security issues. Authentication of users is an important issue in the database that is needed to be addressed most because it can give full access to the database objects.

In this paper we present various security issues that can cause degradation in relational database security and we also identify various problems in the current database security policies. In this paper we propose the use of Multilevel Hashing based Access control mechanism for authentication and security in Relational database.

Keywords —*Relational Database Management System, Database Security, Multilevel Hashing based Access Control, Database Authentication, Access Control*

*****

I. INTRODUCTION

The use of computer is growing very fast now days most of the organizations are computerized and those not till date are seeking computerization. The use of database is necessary at the places where the process is computerized .the Relational Database Management system is world most widely used database management system software. With this grate level of popularity the Relational Database is most vulnerable of security problems. The Relational Database security is the prime concern of research these days. Security policies available for the Relational Database differ in various aspects because all security policies focus on different features of the database security problem and they also establish different assumptions on secure database. This discrepancy leads to difficulty to construct different security requirement.

One of the most severe problems arises the Relational Database is Access control. The current Relational Database management systems are based on discretionary access control which control access of data. The common control policies are based on central control, with this approach only some authorized person can grant and revoke authorization. This approach leads to problems because it give one person full control of the database.

In this paper we first show the major security issues in Relational database management system followed by the work done by the researchers to counterfeit from the security issues. We also identify the problems which incurred in the current Relational database system and we propose the use of Multilevel Hashing based Access control mechanism for authentication and security in Relational database.

II. SECURITY ISSUES IN RELATIONAL DATABASE

The Relational Database Management system is most vulnerable to the security problems. Mainly the security of the database revolves around the three primary issues explained bellow –

A. Confidentiality – confidentiality is the process of limiting the access and disclosure of information contained in the database in such a manner that only authorized users can access the database. The confidentiality is equivalent to the privacy of the information. The methods used to enforce confidentiality are designed in such a manner that it is able to prevent sensitive data from reaching to unauthorized users while ensure the authorized users can access it.

B. Integrity – integrity is the process of ensuring trustworthiness of information. The basic concept behind the integrity is "the data have not been changed inappropriately, either intentionally or accidently. The integrity involves enforcing and maintaining consistency and accuracy of the data over the entire life cycle. It states that the data must not be changed in transition and steps must be followed to ensure that the data can't be modified by unauthorized people. The integrity also involved source integrity i.e., it ensures that data came from the user or database object which supposed to. The integrity to the database can be established by file permissions, user access control, version controls etc.

C. Availability – the availability refers to the ability of the database system is that the data is available all the time if it is required by authorized users. It based on the concept that the database system that is not available when needed is the worst situation. The major threat to the availability of data is DOS Denial of Service attack in which hacker tries to deny the authorized users to access the database.

These three aspects of the database security can be better understood by the following fig 1.

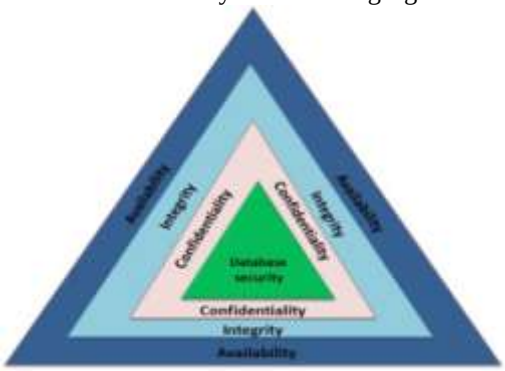

Fig 1. Security Issues in Relational Database

From Fig-1, It can be understood that the database security is based on the CIA (Confidentiality Integrity and Availability) concept. If there is loss of confidentiality, Integrity and Availability in Relational Database then the system is said to be unsecured. So it is the prime responsibility of Database Administrator and Database Designers to ensure these concepts.

III. VULNERABILITIES IN RELATIONAL DATABASE

The Relational Database system is with us from a very long period of time and it is in active use in modern time too. The Relational database seems to posses some vulnerability which may arise because of the following issues –

A. **Architectural Flaws –** the Architectural flaws can arise because of inadequate design of the database or the application which uses the database, it can leads to various security problems. These vulnerabilities are very hard to counterfeit because major rework by the development team.

B. **Vendor Flaws –** vendor flaws are faults that refer to buffer overflows and other errors related to programming that depredate the security of database. In such case the user can execute those commands in database they are not allowed to.

C. **Inappropriate use of Tools –** this flaw in the database security can be caused by usages of inappropriate tools for building applications utilizing developer tools in such a manner that it can be used to break the security of the database. Example of such kind of problem is SQL Injection attack where the hacker tries to break the security of database by injecting some code in the normal query.

D. **Incorrect Configuration –** incorrect configuration of the database can leads to various security breaks this problem is also based on architectural or design flaws.

E. **Installation and Compatibility flaws** – if we use default installation and configuration throughout the uses of the database which is known by public users. For example while using the database if the default username and password is used that is supplied by vendor or manufacturer of the database, in such a case the database security cannot be assured.

F. **Hidden flaws in Database** – the hidden flaws in database can be result from humanistic and un-awareness of certain problems. These problems can be exploited by the hackers.

G. **Privilege Abuse –** this class of vulnerability arise when an authorized user intentionally or accidently misuse his privilege to cause harm to the content of database. It can be result from poor privilege allocation by the database administrator or can be a design fault.

H. **Irresponsible use by Database Administrator –** the database administrator is the person or group of persons who are responsible for managing and maintaining the followings-

   a. Access control of database
   b. Ensuring database integrity
   c. Ensuring confidentiality
   d. Ensuring availability of data
   e. Controlling security of data
   f. Defining privacy levels

   If the DBA's not obey the standard practices and process, it can result a serious database security threat.

I. **User Mistakes**- sometimes the users of the database make mistakes which can result in serious database security flaws. This situation may arise because of unawareness of bad authentication process, not having adequate technical skill. For example the authentic user of database accidentally deletes some contents of the database, change the privilege, etc.

The table given bellow shows the comparison of different types of security vulnerabilities to the database contents

SN.	Vulnerabilities	Criticality	Cost to apply Fix
1	**Architectural Flaws**	***	***
2	**Vendor Flaws**	*	**
3	**Inappropriate use of Tools**	**	***
4	**Incorrect Configuration**	***	*
5	**Installation and Compatibility flaws**	**	**
6	**Hidden flaws in Database**	***	***
7	**Privilege Abuse**	***	**
8	**Irresponsible use by Database Administrator**	***	*
9	**User Mistakes**	*	*

Table 1. Comparison of Vulnerabilities

In table 1. We use * for low ** medium and *** for high values. From the above table it is clear that vulnerability 1, 4, 6, 7, 8 are very critical and must be handled in order to secure the database from various problem. At the same time vulnerabilities 1, 3, 6 are very costly to fix so for these vulnerabilities we need to take early steps such that these vulnerabilities does not turn into actual problems.

IV. LITERATURE REVIEW

Marco Vieira. [1]: explained typical database security mechanisms are not able to detect and handle many data security attacks. More importantly malicious transactions executed by unauthorized users that may gain access to the database by exploring system vulnerabilities and unauthorized database transactions executed by authorized users cannot be detected and stopped by typical security mechanisms. They proposed a new mechanism by which detection of malicious transactions in DBMS is done. They presented a practical example of the implementation of the proposed mechanism in the Oracle 10g DBMS and evaluates the mechanism using the TPC-C benchmark.

M.B. Thuraisingham,, [2]: discuss the notion of multilevel security and the difficulties encountered in designing an implementation scheme for a security policy for a multilevel secure database management system (MLS/DBMS). They will then describe how these difficulties may be overcome in augmenting a database with an inference engine so that it functions like a knowledge based system.

Elisa Bertino. [3]: descries over the years the database security community has developed a number of different techniques and approaches to assure data confidentiality, integrity, and availability. They survey the most relevant concepts underlying the notion of database security and summarize the most well-known techniques. They focus on access control systems, on the basis of which a large body of research has been devoted, and describe the key access control models, namely, the discretionary and mandatory access control models, and the role-based access control (RBAC) model. They also discuss security for advanced data base management systems, and it covers various topics such as access control for XML. They then discuss current challenges for database security and some preliminary approaches that address some of these challenges.

R. R. Schell [4]: describes basic view concepts for a multilevel-secure relational database model that addresses different issues. All data entering the database are labeled according to views called classification constraints, which specify access classes for related data. In addition, views called aggregation constraints restrict access to aggregates of information. All data accesses are confined to a third set of views called access views.

Andriy Furmanyuk [5]: described modern techniques to protection of databases, classical threats and ways of their elimination. The special attention is given to vulnerability assessment and intrusion detection systems. Are defined the simple and structured approaches to a safety of a DBMS.

V. PROBLEMS IN EXISTING RELATIONAL DATABASE SYSTEM

The relational Database security is very important in the modern environment because of its excessive use by different kinds of application and services. Various researches are done in order to develop standard methodologies my which the security of relational database can be ensured but all approaches available till date is not sufficient in a way to cover all different types of security problems that may arise day by day because of the dynamicity. In the modern environment various Hackers, Spammers etc. are trying and developing different methods to bypass the security of the Relational Database so the need of protection is very prominent issue.

The security policies available till date are very rich and resourceful but at the same time it also possess some problems which we present bellow –

A. **Problem in Username and password based Access control –** All available application software and websites uses only username and password validation for the purpose of authentication of user to enable login to the database. In this approach when user wants to login to the database, the application first ask for the username followed by password, once the user enter these details it is passed to the application server as an HTTP request. This approach can be better understood by the following fig 2.

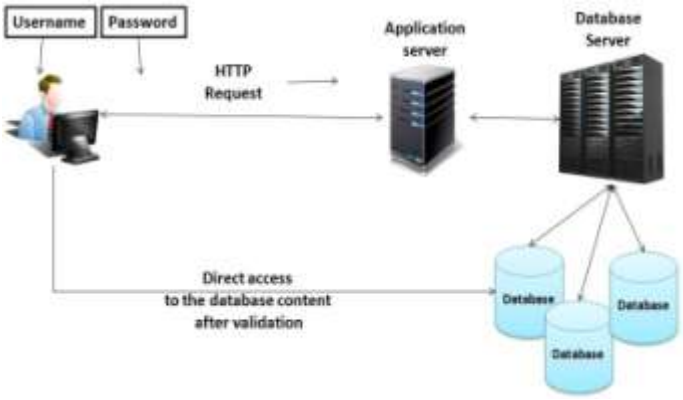

Fig 2. Problem in Username and Password based Access control

From the above fig it is clear that the user pass the username and password, which is passed to the application server which is passed to database server which matches username and password supplied by the user to stored one, the match will allow the user to login to the database server.

The major problem with this approach is that there is many ways by which hackers can bypass such login and password credentials like which occurs in the case of SQL Injection attack. so to enhance the security additional security credentials have to be implemented.

B. **Problem in access management policies –**Another problem with the current approach of access control is the access management policies. Once the user is login to the database then he/she can perform any activities because most of the database access control policies available till date is based on all or nothing method of protection. If the some intruder somehow gains the login

credentials of some user then he can perform malicious activities without any resistance.

C.

Another instance of problem in this type of access management is the person performing malicious activity can be insider of the organization too, accessing those portions of the database he/she not privileged to.

VI. PROPOSED METHODOLOGY

The relational database system is most vulnerable to different kinds of attacks because different hackers are trying to exploit the vulnerability of the database to break the security. To overcome from the problems in the existing database system we identified above, we propose following methodology –

Use of Multilevel Hashing Based Access control - In this approach the traditional username and password authentication is modified with the use of Multilevel Hashing. The use of Multilevel hashing is divided into the following levels –

Level 1 – For the purpose of login to the database system the user needs to enter the username and password just like the traditional system but here we use two additive variables to store the one to store hash value for username and one to store hash value of password. The hash value is calculated by the use of predefined hash function. The hash value of the username hash variables is assigned at the time of creation of user account, where as the hash value of password hash variable is also assigned at the time of creation of user account but additionally, this value is updated at times when the password is changed by standard process. This process is shown in the following fig.

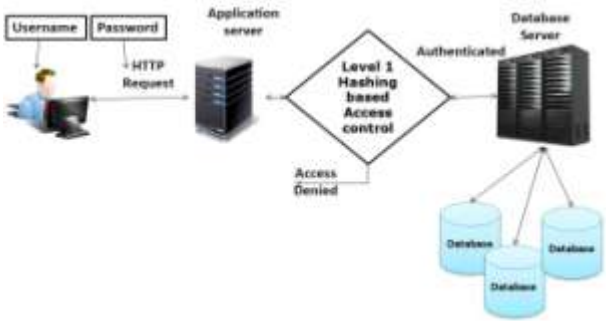

Fig 3. Level 1 Hashing based Access Control

From the fig 3. It is clear that when the user wants to login to the database he/she provides username and password, after it the hash value for the username and password is automatically created and it is passed to the application server along with the username and password, in turn the application server pass it to the database server where first the stored username, password and hash value is fetched from the database, the username and password is matched with the user's supplied one if the match is found then the fetched hash value is matched with the user supplied one if again match is found then the user is allowed to login, but if mismatch is found in any of the steps then the login denied. The validation process is explained in the following fig.

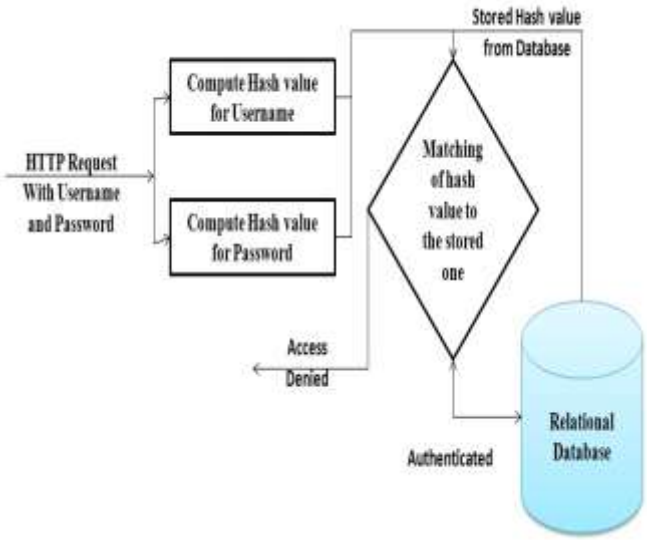

Fig 5. Architecture of Level 1 Hashing

Level 2 – once the level1 validation is done and the user signed in to the database then normal processing is continued but when the user wants to perform any critical process then the user have to supply the transaction password for committing a transaction, creating a new session or trying to use a new service, at this time we propose the use of hash value which is stored along with transaction password. The user supplied transaction password and hash value is matched with the stored one to validate the transaction. The use of level 2 hashing is shown in the fig

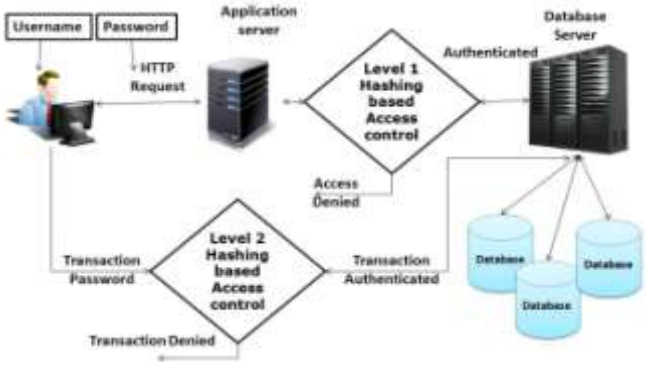

Fig 5. Level 2 Hashing based Access Control

From the fig it is clear that to commit a transaction or perform any critical process the hash value must be matched. In this manner the database is ensured to be protected from those security issues we addressed in the preceding sections.

VII. CONCLUSION

The Relational Database system is most favorable database system these days and is most vulnerable to security breaks. One of the main problem in Relational Database security can be weak access control. If the access control policies are not followed properly the hackers as well as the valid users of the

database can exploit these vulnerabilities to cause harm to the content of the database by performing malicious activities. So protecting the contents of Relational database is very important.

In this paper we discussed various security issues that can cause harm to the database. We also explained and compared different types of security vulnerabilities. We also tries to exploit some problems associated with the existing access control policies of the Relational Database system. In this paper we proposed the use of Multilevel Hashing based access control to secure the contents of Relational Database.

REFERENCES

[1] Marco Vieira, Henrique Madeira , "Detection of Malicious Transactions in DBMS", 11th Pacific Rim International Symposium on Dependable Computing.
[2] M.B. Thuraisingham, "Security Checking in Relational Database Management Systems Augmented with Inference Engines", International conference on Computer technology at University of Taxas at Dallas
[3] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE, "Database Security—Concepts, Approaches and Challenges" in IEEE transactions on dependable and secure computing, vol. 2, no. 1, january-march 2005
[4] R. R. Schell, M. Heckman, "Views for multilevel database security", IEEE Trans, on Software Engineering, 1987.
[5] Andriy Furmanyuk , Mykola Karpinskyy, Bohdan Borowik, "Modern Approaches to the Database Protection" in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
[6] Lars E Olson, Carl A Gunter, and P Madhusudan. A formal framework for reective database access control policies. CCS, 2008.
[7] Raghu Ramakrishnan and Johannes Gehrke. Database Management Systems. McGraw-Hill, Inc., New York,NY, USA, 3 edition, 2003.
[8] Shariq Rizvi, Alberto Mendelzon, Sundararajarao Sudarshan, and Prasan Roy. Extending query rewriting techniques for _ne-grained access control.SIGMOD, 2004.
[9] Jerome H Saltzer and Michael D Schroeder. The protection of information in computer systems. Proceedings of the IEEE, 63(9):1278{1308, 1975.
[10] Fred B Schneider, Kevin Walsh, and Emin G□un Sirer. Nexus authorization logic (nal): Design rationale and applications. TISSEC, 14(1), 2011.
[11] Guoliang Zou, Jing Wang, Dongmei Huang, LiangJun Jiang, "Model Design of Role-Based Access Control and Methods of Data Security", 2010 International Conference on Web Information Systems and Mining.
[12] Advanced SQL Injection in SQL Server Applications An NGSSoftware Insight Security Research (NISR) Publication ©2002 Next Generation Security Software Ltd
[13] W. G. Halfond and A. Orso. Combining Static Analysis and RuntimeMonitoring to Counter SQL-Injection Attacks.2005
[14] Vulnerability Management in Web Applications R. Thenmozhi, M. Priyadharshini, V. VidhyaLakshmi, K. Abirami http://www.ciitresearch.org/dl/index.php/dmke/article/view/DMKE042013007
[15] Melchor, C.A., Gaborit, P. A fast private information retrieval protocol In ISIT 2008. pp. 1848 – 1852. IEEE (2008)
[16] Ostrovsky, R., Skeith, W.E.: A Survey of Single-Database Private Information Retrieval: Techniques and Applications In Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 393–411. Springer (2007)
[17] Park, B., Moon, D., Chung, Y., Park, J.W.: Impact of embedding scenarios on the smart cardbased fingerprint verification. In Lee, J.K., Yi, O., Yung, M., (eds.) WISA 2006. LNCS, vol. 4298, pp. 110–120. Springer (2006)
[18] Shmueli, Erez, Vaisenberg, Ronen, Elovici, Yuval and Glezer, Chanan(2009)Database Encryption- An Overview of Contemporary Challenges and Design Considerations SIGMOD Record vol38, No 3.
[19] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, "Review of Attacks on Databases and Database Security Techniques", international Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

AUTHOR'S PROFILE

``**Mr. Surya Pratap Singh** is MCA and UGC-NET qualified, He is pursuing Ph.D In the department of Computer Science Deen Dayal Upadhyay Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Database Security and Networking. Mr. Surya Pratap Singh has published 19 **papers** in different national and international conferences/ Journals.

Dr. Upendra Nath Tripathi is Assistant professor in Department of computer science Deen Dayal Upadhyay Gorakhpur University, Gorakhpur (U.P. India). He has 14 years of teaching and research experience. He has published **50 papers** in various National and International Journals/conferences. His area of research interest is database systems and networking.

Dr. Manish Mishra is Assistant professor in Department of Electronics DDU Gorakhpur University, Gorakhpur (U.P. India). He has 14 years of teaching and research experience. He has published 55 papers in various National and International Journals/conferences. His area of research interest is Computer Technology, fast processor design.