2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, T.N., India. 6 - 8 May 2015. pp.165-167.

Efficient and Effective Security Model for Database Specially Designed to Avoid Internal Threats

Aditya A. Shastri[1] and **Dr. P.N. Chatur**[2]

Department of Computer Science and Engineering, Government College of Engineering, Amravati, India
Email: [1]aditya.shastri111@gmail.com, [2]chatur.prashant@gmail.com

***Abstract*— Since the information or data stored in databases are usually considered as vulnerable and also important corporate resource, security is of uttermost importance in any database management system, particularly those database that has sensitive information. There are lots of security models for commercial systems but information system security is often ignored. Information security remains a key issue in the IT industry, as shown in several surveys. Security accidents continue to increase in frequency and sophistication. As the client or user using the database wants more access to the data in this world connected by internet, the chances for security breaches are increasing. Therefore in this paper a security model specially designed for avoiding internal threats is given which already exist. But because of the performance issues of that model an amended security model is proposed. This amended security model has high performance i.e. without affecting to the security of overall model, response time of the system is reduced. The performances of both the models are compared and which model is best is decided based on the performances.**

***Keywords*— Database Security; Internal Threats; Security Enhanced Model; Safety Rule Base; Optimization etc.**

I. INTRODUCTION

A database contains data of various degree of importance and that data is shared among wide range of users which have different privileges, so it need to be managed and protected because any undesirable changes to the database can affect its integrity and also the other things related to database. Security problem of database cannot be considered as isolated problem because it is also affected by the other components of the computerized system like operating system [1]. Therefore many of the security model adopted for trusted OS can be adapted to DBMS. Security models are the basic tools to start with when developing a security system. For this purpose information security managers are tasked with various functions, including planning for security, forming the policies, risk management, selection of the security technology, threat assessment and maintenance [2]. In this paper we mainly focused on the threats which arise from within the organization and propose an efficient model that can be used to avoid such threats. These threats include the member from the organization, interns etc. As different users have different degree of accessibility i.e. different privileges, a particular user should not be able to access that part of the database that he is not allowed. For this purpose a security model is proposed.

II. SECURITY MODEL

The role of any security system is to maintain the integrity of an operational system by enforcing a security policy defined by a security model. System integrity refer to both i.e. data is correct and accurate (data integrity) and system should be operational and working (system integrity). This type of integrity can be achieved by control and management of subjects which include users and processes [3]. This control is governed by set of rules which will be called as “safety rules” of “rule base”. These rule base maintain the security requirements of the organization which specifies what security properties the system must provide and describes protocols an organization must follow to achieve security. Security models are nothing but the formal description of security policies. These can also be considered as useful and important tools for calculating and comparing security policies [4]. These models allow us to test for the security of the database system and also its completeness and consistency.

III. EXISTING SYSTEM

We all know that in any server client application we have front end and back end. Front end is generally a HTML or ASPX page and back end is any database. It could be SQL server, MySQL of even Oracle. This front end and back end is connected either by a java program or C# language if. net framework is used. That means there is no specific security measure used. Hence we introduce an extra security model

978-1-4799-9855-5/15/$31.00 ©2015 IEEE

which will ensure the security of the database system. Thus normal architecture of the database system becomes as shown in following Fig. 1.

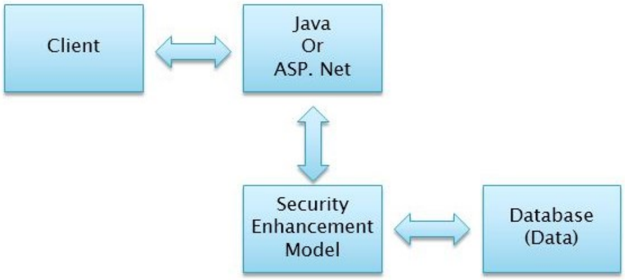

Fig. 1. Traditional System

It is the role of this security enhancement model to maintain the security of the database system. The detailed architecture of this model is as shown in the following figure.

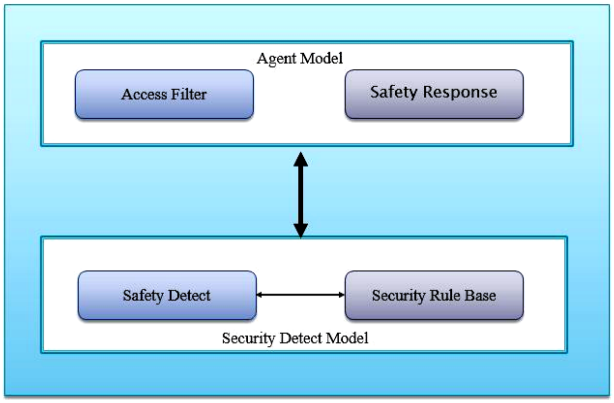

Fig. 2. Exixting System

As shown in Fig. 2 the query is first passed to the Agent Model. Access filter which is part of agent model intercept the users access request, judge the type of the request and confirms the type of request. The results of this filter is passed to the next model i.e. Security Detect Model [5]. According to the data received by this model safety detect module of this model detects whether it is safe to allow the particular user to let access the part of the database that the user wants to access.

For this, safety detect module takes help from Safety Rule Base which is another part of security detect model. This rule base is governed and maintained by Database Administrator. Thus a combined result of security detect model is once again passed to Agent Model in the form of the safety response. Then according to the safety response agent model takes the decision whether to allow or disallow the request of the user.

IV. Proposed System

An alteration of the above model is proposed which has several advantages over that model which we will discuss in next point. As we have already mentioned in abstract and introduction that this model is only for security from internal threats. So data stored in the database need to be protected from unauthorized access, malicious alteration or destruction and accidental introduction to inconsistency. The detailed architecture of this altered model is shown in Fig. 3.

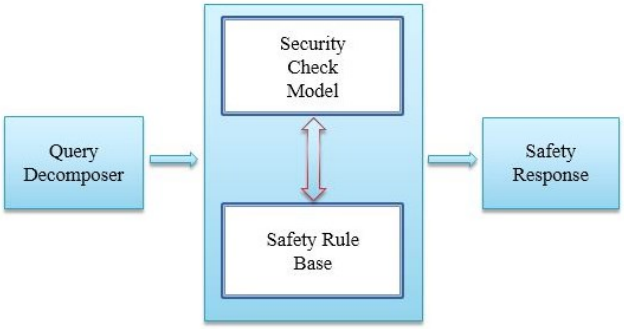

Fig. 3. Proposed System

Above architecture is liner architecture. It's not a two level architecture as shown in previous section. The first module i.e. Query Decomposer plays important role in the working of this architecture. Query Decomposer decompose the query in two sub parts, first the type of the query that user has fired and second name of the table to which user wants the access. This two parts are then combined with the user-id of the user and transported to next phase i.e. security check model.

This security check model will check whether requesting user actually has the privilege to access the part of the database that it wants to access. For this it takes the help form safety rule base. Safety rule base is strictly maintained by the DBO (Database Administrator). The result is passed on to next phase which is safety response. It performs the task of decision making i.e. whether to give that user access to the table that he is requesting. In this model we not only check that whether user has access to that part of the database but also check whether user can perform that action that it is requesting.

A. Performance Analysis of Two Models

In the existing model as discussed above, architecture is multilayer i.e. there are two different layers, one is Agent module and another is Security detect module. So the transition time between the two models adds to the overhead of the overall system. First the data is passed from agent module to security detect module and then the results of second module is passed back to the agent module. These transition of data to and from the two different module increases the execution time of the overall system.

On the other hand the proposed system is single layer. There is no transition of data from one module to another module. This transition time is saved in proposed model. Practical analysis shows that overall time of the system is reduced by 30% to 40% depending upon the type of operation that the user wants to perform on the database. This is quite a decent reduction in the overall execution time of system. Also security of the system is unchanged i.e. execution time is reduced without affecting the main thing which is security from the internal threats.

B. Salient Feature of the Proposed Model

There are several features that makes the proposed model secure and efficient to use. They are

1. No user is able to obtain the information without authorization.
2. No user is able to modify the information without authorization.
3. No mechanism exists whereby a user authorized to obtain an information can communicate that information to another user not authorized to obtain it.
4. No user is able to activate a method without authorization.

V. Conclusion and Future Work

Database security is not an isolated problem but in overall sense it is a total system problem. Security of the database not only depends on the choice of particular DBMS product or security model but also on the operating environment and people involved. Thus the method of adding an extra security enhancement module between client and the database server works for the improvement of the security of the database server. Also conversion of multilayer model into single layer architecture reduce the overall execution time of the system. Hence the security from the internal threats is achieved and even because of the addition of extra module the overhead is also reduced to improve the system performance. The concept of the encryption is not used anywhere in this model. So the data can be encrypted along with the authorization feature will provide more protection for the sensitive data. However the problem of establishment of secure model for the database is wide open particularly where the database attempts to share the common data.

References

[1] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE “Database Security—Concepts, Approaches, and Challenges” IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 1, January-March 2005

[2] Nedhal A. Al-Sayid, Dana Aldlaeen “Database Security Threats: A Survey Study” 978-1-4673-5825-5/13 ©2013 IEEE.

[3] Zhu Yangqing, Yu Hui, Li Hua “Design of A New Web Database Security Model” 978-0-7695-3643-9/09 © 2009 IEEE DOI 10.1109/ISECS.2009.180

[4] Raymond Chiong and Sandeep Dhakal “Modelling Database Security through Agent-based Simulation” 978-0-7695-3136-6/08 © 2008 IEEE DOI 10.1109/AMS.2008.164

[5] Peng Wang, Liu Xing, Xin Gu, Changming Zhu “Design and Implementation of Security Enhanced Module in Database” 978-0-7695-5118-0/13 © 2013 IEEE DOI 10.1109/ICICSE.2013.20

[6] Xueyong Zhu, J. William Atwood “A Web Database Security Model Using the Host Identity Protocol” 11th International Database Engineering and Applications Symposium (IDEAS 2007) 0-7695-2947-X/07 © 2007

[7] WANG Baohua, MA Xinqiang, LI Danning “A Formal Multilevel Database Security Model” 978-0-7695-3508-1/08 © 2008 IEEE DOI 10.1109/CIS.2008.45

[8] Yi Huang, Xinqiang Ma “A Security Model Based on Database System” 978-0-7695-4031-3/10 © 2010 IEEE DOI 10.1109/iCECE.2010.1198

[9] Premchand B. Ambhore,B.B.Meshram,V.B.Waghmare “A Implementation of Object Oriented Database Security” Fifth International Conference on Software Engineering Research, Management and Applications 0-7695-2867-8/07 © 2007 IEEE DOI 10.1109/ SERA.2007.120 359