Trust Based Infererence Violation Detection Scheme Using Acut Model

Mr. K. Karthikeyan[1], Dr. T. Ravichandran[2]

[1] Research Scholar, Department of Computer Science, Karpagam University, Coimbatore, Tamilnadu-641021, India,

[2] Principal, Hindusthan Institute of Technology, Coimbatore, Tamilnadu-641032, India

Abstract

The inference problem is the major problem in securing the sensitive data in the secured database. In the inference problem the user tries to access the sensitive data from the secured database by giving series of queries with the non-sensitive fields. Inference problems affect the securities in the database and peculiarly in the Multilevel secure databases in which the data and users are differentiated into different levels. Our approach provides the control over the inference problems in the single as well as multi level database. We are provided with a trust based system which results in more efficiency when compare to the other techniques.

Keywords: *Inference Problem, Secured Database, Multilevel database, Trusted Servers*

1. Introduction

From early 80s, the inference problem in the multilevel database had been put forward for the research. It can be described that if the information is secured with the higher level security then user can retrieve the secured data with the data with lower security level, this phenomenon which we are calling as "inference problem". For example, consider an enterprise is maintaining the project details of every staff in a higher level security, but the meeting held and the persons who were attending the meeting is placed in a lower security levels. Then a user can retrieve the projects and the company associated by giving the query with the persons attended the meetings.

The inferred result from the secured database may produce some harmful results if the inferred user knowledge is not authorized to use the secured database, later only the database manager came to know that some inference problem occur in the secured database.

The response taken for the inference problem can be made easy by finding the computation between the accessing feasibility and response time. But there are some complications that we have to identify. In the secured databases there occurs a conflict while

granting a query result for a user, if multi users are allowed to responds for a

particular query then we should made the security alerts for the servers and the queries are analyzed before responding to the queries. This phenomenon is called collision resistance. This process identifies the inference problem but it requires a scheme for inference detection system among the users and their queries.

We are focusing only in the inference problem occurring in the multilevel secured database. In such database the data and users are differentiated with different security levels. Our system authenticates every user before accessing the database, if the users are not authorized means they cannot access the database. This is the first level of security in our approach.

The following approaches are needed to prevent the inference problems, the first approach is to control the unwanted authentications of the users in the secured database, the second approach is to design the database so that with the inference control. The third process is to create a "Trust Model" which acts as the advisor for the secured database. Since the inference problem is very complex and a single layered control does not provide more security effectively, hence we go for this integrated approach to overcome the inference problem.

2. Related Works

The former works posted many researches related to the Inference problems, one of the proposal were key based schema [3]. In this process, the initial process was to generate set of key pairs; the key generation process can be done by using any of the key generation algorithms.

Each key was associated with the objects. The number of key pairs depended on the length of the inference channels. The key pairs are denoted by the letter 'Ks', in this approach two types of key sets are represented in which the first approach is used by the database systems in which the user did not need to hold the keys. In the other approach, every user needs to have the secret key. In the initial phase, all objects in the inference channel are linked with the key or key sets.

If a key is accessed for an object by a query algorithm, other queries have to use the same key to access the object, this process can be achieved by rejecting the associations between the objects and keys. To do so, this process provides the easy access and fast query processing. But different keys cannot be utilized to access the same objects.

Another approach is proposed in the database security technology [5]. A knowledge based inference control machine had been proposed to detect the inference strategies. Users can use this inference controller to monitor for the unauthorized inferences and simultaneously secure the database from violations. To make the inference controller more efficient, it should have knowledge about the various inference strategies. A controller should determine the sensitive data or objects. Finally a controller should detect or prevent the security violation of inference attacks.

A knowledge based inference violation detector is proposed named XINCON (eXpert INference CONtroller) which has the capability to detect unauthorized access of the users. It uses some logical detection and analogical reasoning concepts to find out the inference attacks. The major advantage of XINCON is the user interface components, knowledge management, and truth maintenance system. XINCON uses security constraints to find out the sensitive levels of the data and objects.

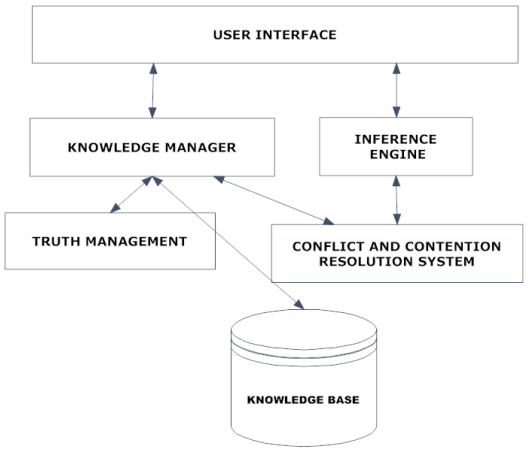

Fig. 1 Represents the XINCON framework

Data and knowledge are distinguished into different security levels. Security constrains plays vital role in assigning the security levels for data and knowledge. We describe the various constrains in the followings;

• Constrains that separate the database, relation or attribute.

• Constrains that separate the part of the database based on the value of some data. These processes are called as content-based constraints.

• Constrains which splits any part of the database based on the real world events. These processes are called as value-based constraints.

• Constrains that classify based on the information based on already processed. These are called aggregate constraints.

In this paper [3] a system with a modern intrusion-tolerant technique had been proposed in distributed database system security model. In the former secured distributed database systems lie on the precautions are limited to the malicious attacks, but there is no action taken for the intrusion tolerance mechanism, isolate access and recovery from the intrusion in the secured database. Our proposed approach maintains the integrity and availability of the data even when the intrusion attacks may occur. In this system a threshold secret share schema is used to ensure the data from the servers with intrusion on it.

Distributed database are vastly used in many industrial applications and research applications, but the security concerns in the distributed database is longer milestones to achieve it. More researches have been put forward for the information security. DDBS have been integrated with many attack overcome techniques like secure audit, message tracing, firewalls and IDS systems. But some

time the preventive actions fail to find the malicious attacks in attack methods and frequently attack occurs. So a new approach with Intrusion tolerance has been proposed to find even a single rare intrusion attacks in the database.

This system uses some triggers tolerance mechanism which secures the intrusion and provides the normal service to the users. The intrusion tolerance mechanism is presented with the distributed database security model to provide the distributed database applications with integrity and data availability.

A distributed database is written of databases put in physically classified schemes, co-ordinated by communicating networks, and dealt by disseminated database management system. While conventional database security techniques frequently go wrong to conduct with vicious attacks or intrusions an intrusion-tolerant database system can discover invasions, isolate attacks, assess and repair the damage cause by attacks or intrusions, and keep confidential data safe. The ITDDB model is designed for these goals and has four main subsystems:

• The Proxy Sever subsystem, which will receive and filter users' requests and communicate with other sites in DDBS;

• The Intrusion Detection subsystem, which acts as an intrusion tolerance trigger to the whole system;

• The Assessment and Repair subsystem, which will assess and repair the damage caused by attacks or intrusions in a timely manner;

• The Isolation subsystem, which will isolate suspicious users (transactions) when the intrusion detection subsystem gives an alert.

Knowledge management [4] improves the values by finding the possessions and resources for the management efficiency. But we are lacking in the security for the knowledge management. Every management should protect their important possessions. So authenticated individuals only will be granted to perform operations in the organizations. In this paper the security of the knowledge management will be done based on the confidentiality and trust. But mainly the access control will be made based on the trust management and higher level of privacy will be achieved.

Knowledge management is the combination of many technologies like data mining, multimedia and www. So the knowledge management's manager cannot be thinking about the security. The possessions they are having higher security risks. Trade secrets are high confidential one, so that the competitors should not access it. So we need an access control mechanism, credential mechanism to secure the intellectual possessions. We have introduced a process which is having higher secured operations. The security of the knowledge management architecture will be build around the intranet. Trust management is the key role in the secure knowledge and it increases the additional security features of the security.

This process states that the trust of the individual will be taken into the account and based on the trust knowledge sharing will be allotted. In our process we are focusing on corporate, so every corporate needs to posses their trust values and based on the trust values knowledge will be shared otherwise negotiation process will be carrying on. In our trust negotiation models enough knowledge management tools will be used efficiently. Trust management is a vital role in the secured technique for knowledge management.

Many recent researches [5] in the multi secure database management system focus on the centralized security systems in the distributed database. Due to the demand of the higher performance and higher availability, database systems are migrated from the centralized approach to the distributed approach. Since there occurs lot of problems in the distributed architectures, like concurrency, security causes major problems in the distributed architectures of the database. So concurrency control has to be integrated with the distributed architecture of the databases. In this approach we propose several concurrency algorithms for the centralized multilevel secure database management systems. To make the distributed architecture more secure we present a virtual model and we analyze the performance of them with concurrency control in a distributed database systems.

In this paper, we propose two security levels: high and low. A main pertain in multilevel surety is information leakage. Leakage can occur in two ways: directly through intelligence such as interpretation an information item or circuitously through a cover channel. Cover channels are ways not normally meant for data flow. In multilevel secure information low security level deal can be retarded or discharged by a high security level deal due to partook data access. Direct leakage can be controlled by the required control schemes but for the covert channels is requiring more modification in the former concurrency technology with two phase locking and time stamp ordering.

Experimental result shows that the result obtains from our system shows the effective result when compare with the former method.

The distributed database architecture [6] is having many successful designs on it, the designs help to improve many criteria like scalability, accessibility and flexibility for

many data. Developing such a efficient distributed database requires security issues which is to be solved for the integrity and access control of the systems. Distributed database has some security issues, from the former techniques have proposed many technologies but it is still under research only. These databases are majorly affected by the denial of service and information modifications, etc., some important security requirements for the database management system such as access control, reliability, integrity and recovery should be achieved.

In our process, we provide a user interface has been built for the user request which will be under the control of the distributed Transaction Manager. A customized user interface provides the entry for the user requests and gives the query results to the users. The parameters that we have mentioned as the issues for the security will be providing solutions in the user interface for the query submissions. The transaction manager structures the view of the data before giving to the users and also it validates the output of the query submitted.

We propose a method [7] which is based on the different stages of security process and access control rights to the users. In the process a stages of security for the database have been proposed and different types of security tags also proposed for the objects and data. The major concept behind this is the creation of rules for the tags and tag tables. Access control can be obtained by changing the user's query by the security tag table in distributed database. Different stage security refers that the objects are splited into different groups with the specified security level, every groups has its own security levels and the objects in the similar groups have the same security levels, the data across the objects with multi security levels must meet the security access control policies. In the concept we have proposed Bell-LaPadula model shows the considerable way for the information security system and redefines the system requirements for the data security for the data. This concept forms the basis for every different stage of database security systems.

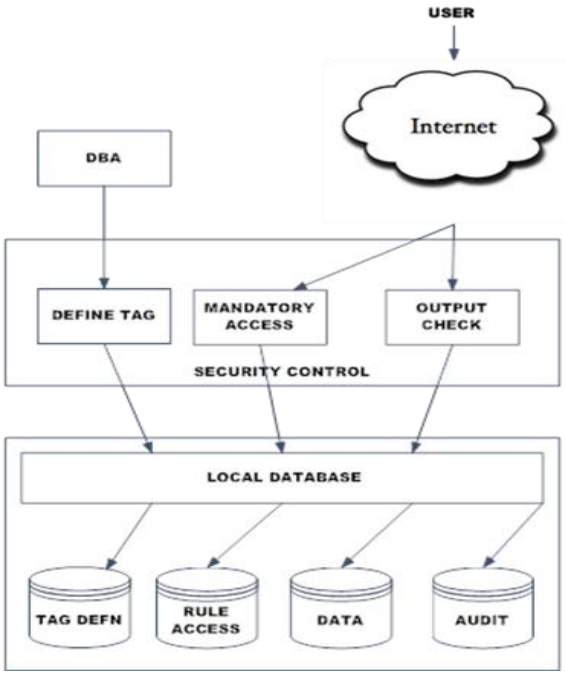

Fig. 2 represents the framework for the multilevel database security

Define Tag: In this module the complete security tag definition and object definition for the database administration, in this process additionally the integrity and consistency checks have been processed.

Access Control: In this module, the security access of the query statements given by the users has been achieved. The process of this module is for confirming the security tags then according to the system security policies it gives the privilege to the users submitted queries from the local and global.

Output Validation: In this module, the query results for the user submitted queries will be validated before giving the result to the users.

3. Proposed System

3.1 ACUT Model

In this model we propose a Access Control Model named **ACUT (ACCESS CONTROL USING TRUST)** which grants the access for accessing the data using trust value calculated from the user logs or history or behavior. In the previous paper we have seen that how a user behavior can be analyzed with additionally we state that based on the behavior we are calculating the trust value. The trust value is the one which decides whether the user will be given access to use the database or their request will be declined initially. The overall diagrammatic flow has been stated as follow;

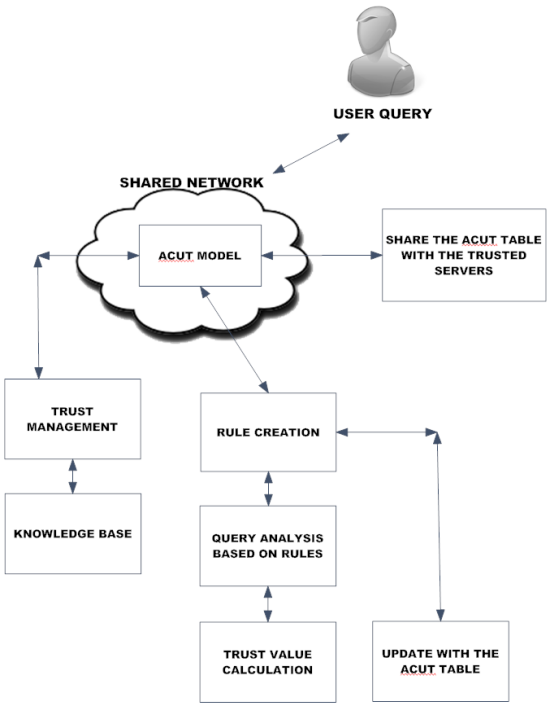

Fig. 3 represents the working procedure of ACUT model

In this model we use ACUT model process, so that we use shared network to update the behavior and trust value of the users to share the knowledge with the trusted servers. In the shared network we are having our ACUT model framework; it is having three processes in it.

- Trust Management
- Rule Creation
- Share the ACUT Table.

3.1.1 Trust Management

In the Trust Management process, we are going to manage the Trust based model with it. The trust based model is having the back end data as the knowledge base data. In the previous paper we have done based on IVDS which has the working procedure based on the prior knowledge threshold limitations.

In our Trust Management process we use the prior history of the user's behavior and previous query access and results. These backlogs help us to manage the trust for every user. The Trust Management block helps the ACUT model to grant the access for every user in the access control policy.

3.1.2 Rule Creation

In the Rule Creation process we have the query analysis phase. The query submitted by the users will be analyzed here. The rules for the data or objects which is to be posed as the query result will be determined here.

The sensitive data will not be posted for the user submitted query but how we are going to achieve that, for that we need to create rules. These rules are having the results as binary values and if the sensitive data are requested from the query means the rules result the '0' value and the query will be denied if the rule result will be '0'.

3.1.3 Share the ACUT Table

In our process we maintain an ACUT table which acts as the backlog for every user. In the ACUT table the user details and their respective trust values. The trust values will be given to the ACUT process for the access provisions.

In the access provision based on the ACUT value of the users, he will be given result for the query, so both the knowledge base and the behavior based will be carrying on in our process.

4. Experimental Result

We made experiments with the number of users and their queries submitted. Based on the query analysis we have analyzed what type of data they try to access from their queries. Based on the query they have submitted we will be assigning the trust value for them.

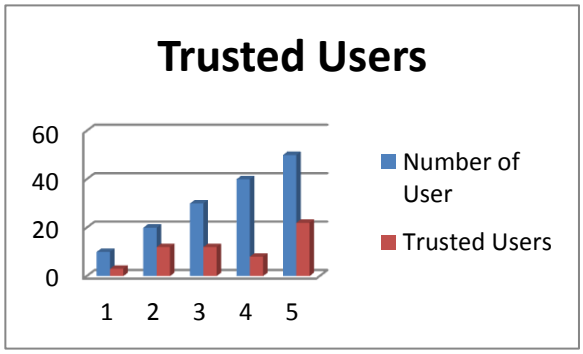

Fig. 4 represents the graph between the number of users and trusted users.

In the graph depicts that we are having the trust management and the trust management analyzes every user based on the prior knowledge and based on the knowledge we come to a conclusion that the trusted users from the whole users who had submitted the queries.

In the second experiment we have analyze the queries submitted by the users. Our query analysis process analyzes the query for inidiviudal users and based on the data they have obtain from their queries we have calculate the query analysis value and their result will be displayed.

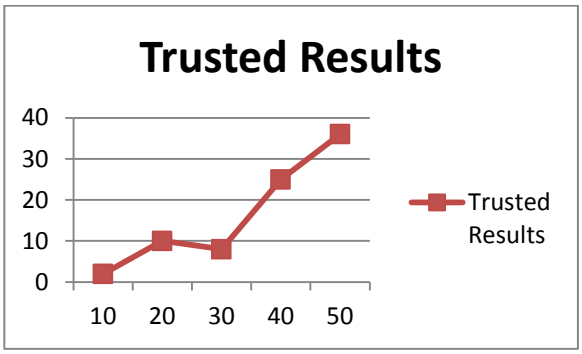

Fig. 5 represents the Trusted result for the queries given by the queries.

The above graph shows how the trust query results are depicted. In the graph we calucate number of queries have been submitted to the query analysis phase and based on the query analysis phase we have calculated the trust values from the query analysis phase.

5. Conclusion

The inference problem is the major problem in securing the sensitive data in the secured database. In the inference problem the user tries to access the sensitive data from the secured database by giving series of queries with the non-sensitive fields. To overcome that we have introduced a process namely ACUT model which analyses the query as well as the user who is giving the queries. Based on the trust values obtain from the backlogs as well as the behaviors we can avoid the inference problems and also the experimental results show that our approach works well for knowledge base as well as behavior based using trust values.

6. Reference

[1] Gu-Ping Zheng and Lu-Feng Xu, "Distributed Database System Security Model of Power Enterprise Based on Intrusion Tolerance Technology" 2006 International Conference on Power System Technology.

[2] K. Pradeep and Z. Mohammad, "DIDMA: A Distributed Intrusion Detection System Using Mobile Agents," in Proc. Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks, SNPDISAWN 2005, Sixth International Conf., pp. 238-245.

[3] "Distributed Database System Security Model of Power Enterprise Based on Intrusion Tolerance Technology " by Gu-Ping Zheng and Lu-Feng Xu 1-4244-0111-9/06/$20.00c02006 IEEE.

[4] "Secure Knowledge Management: Confidentiality, Trust, and Privacy" by Elisa Bertino, Fellow, IEEE, Latifur R. Khan, Ravi Sandhu, Fellow, IEEE, and Bhavani Thuraisingham, Fellow, IEEE 1083-4427 © 2006 IEEE.

[5] "Performance Evaluation of Secure Concurrency Control Algorithm for Multilevel Secure Distributed Database Systems" by Navdeep Kaur, Rajwinder Singh, A.K.Sarje, Manoj Misra 0-7695-2315-3/07 IEEE.

[6] "On Distributed Database Security Aspects" by Zakaria Suliman Zubi 978-1-4244-3757-3/09/ ©2009 IEEE

[7] "Access Control Method Based on Multi-level Security Tag for Distributed Database System" by Ying-Guang Sun 978-l-61284-088-8/ll ©2011 IEEE

[8] Jiang Wen-bin,Zhang Ren-jin,Zhang Fang-xia.Analysis of Security Strategy on DDBS[J].Computer Knowledge and Technology.2009, vol.5,no.4, pp.769-776.

First Author: MR.K.KARTHIKEAYAN is pursuing Ph.D in Database Security. He received the B.Sc degree from Kamaraj University, Tamilnadu, India in 1994, and M.C.A degree from Bharathidasan University, Tamilnadu, India in 1998 and M.Phil from Manonmaniam Sundaranar University, Tamilnadu, India in 2004. He is currently working as Assistant Professor in Department of Computer Application, Anna university of Technology, Madurai. Before Anna University of Technology he was working as a Lecturer in Sengunthar Arts & Science College, Tiruchengodu, Tamilnadu, India.

Second Author: Professor **Dr.T.Ravichandran** received the BE degree from Bharathiar University, Tamilnadu, India and ME degrees from Madurai Kamaraj Universtiy, Tamilnadu, India in 1994 and 1997 respectively, and PhD degree from the Periyar University, Salem, India in 2007. He is currently the **Principal** of Hindustan Institute of Technology, Professor Ravichandran has been a professor and Vice Principal in Vellalar College of Engineering and Technology, Erode, Tamilnadu, India. His research interest includes theory and practical issues of building distributed systems, internet computing and security, mobile computing, performance evaluation, and fault tolerant computing, Professor Ravichandrann is a member of the IEEE, CSI and ISTE. Professor Ravichandran has published more than 80 papers in referred International journals and refereed international conferences proceedings.