ISSN:0975-9646

A Review of Security Mechanisms for Detection of Malicious Transactions in Database

Varada Bharat Srinivas[#], Dr.Syed Umar[*]

[#]*Student, ECM dept., KL University, Vaddeswaram, Guntur.*
**Assc.Professor, ECM dept., KL University, Vaddeswaram, Guntur*

***Abstract*— Insider attacks formed the biggest threaten against database management systems. There are many mechanisms have been developed to detect and prevent the insider attacks called Detection of Malicious Activities in Database Systems DEMIDS. The DEMIDS consider as one of the last defenses mechanism of the database security system. There are many mechanisms that have been developed to detect and preventthe misuse activities like delete, and update data on the database systems. These mechanisms utilize auditing and profiling methods to detect and prevent the malicious activities. However these mechanisms still have problems to detect the misuse activities such as limit to detect the malicious data on authorized commands. This study will address these problems by propose a mechanism that utilizes dependency relationship among items to detect and prevent the malicious data by calculate a number of relations among data items. If the number of relations among items is not allowed any modification or deletion then the mechanism will detect activity as malicious activity. The evaluation parameters such as detect, false positive and false negative rate use to evaluate the accuracy of proposed mechanism**.

***Keywords*—Dependency Relationship; Detection; Prevention; Malicious; Insider Attack.**

I. Introduction

Information is one of the main assets of any organization which is essential to itscontinuity. Therefore, information security is very important to protect the confidentiality, integrity and availability of the information. Many systems and tools are used to achieve the requirements of the information security and to prevent information systems from any possible incident. Access control systems, authentication systems, anti-virus software and firewalls are examples of such systems.According to [1] despite different protection mechanism, it is nearly impossible to have a completely secured system. Although sophisticated security systems can be used to achieve the information security requirements, those systems may be under threat due to vulnerabilities or misconfiguration of those systems. As a result, those vulnerabilities or misconfiguration may be exploited by intruders or implement their at-tacks. Therefore, Detection of Misuse Activities in Database Systems is considered as the last defense layer of the database security systems of any organization.The insider attack forms thebiggest threaten on the database systems due to it has authorized access to the database systems.

II. Background

There are many types of insider attack that try to abuse the access rights and do malicious activities for example, employees, masquerading and the malicious activities such as updated and deleted approved records.A malicious activity is de-fined as a group of actions that attempts to harm the Integrity, confidentiality of database system, [3]. DEMIDS is a mechanism designed to detect and prevent the malicious activities such as malicious transactions on the database systems [4].

There are many insider attacks that may hurt the confidentiality, integrity and availability of database systems. According to [5]the database security attacks classified into two types of attack such as: outsider attacks and insider attacks. The out-sider attack can defined as malicious actions that cause many problems such as delay or bugs. However, the insider attacks categorized into legitimate and illegitimate access. Legitimate access can abuse his privilege to do malicious actions, and on the other hand, the illegitimate accesses try to exploit the vulnerabilities of the system to do malicious actions.

Many researchers have been conducted to investigate the in-sider attacks [6]. According to [2]the insider attacker's forms the biggest threat on the database security level than the out-sider attacker, because two reasons, theirknowledgeabout systems andtheir granted privileges. [7]Indicates that the in-sider attacks can forms the extremelydangerous on database systems. Furthermore, insider attacks use their rights to achieve the malicious action.

Malicious transaction is one of the inside attacks which harm the integrity and availability of the database [5]. There are many causes of malicious activities [5] such as bad configuration, low experiences of the Database administrator (DBA), hidden flaw and weakness of database implementation. [8]Stated that the mechanisms based on auditing log file only detect the malicious commands, and if legitimate commands contain malicious data, it will not be detected. [8]Proposed mechanism to detect the malicious activities in database sys-tem management. The mechanism used data mining approach to determine thedependency among data items. The data dependency indicates to the access relations among data items. These data dependency are generated in a set of rules (pre-written, read, and post-written sets). Therefore, the activities that don't follow any of rules are signed as malicious activity. The limitation of this mechanism is limited to user transactions that conform to the read-write patterns assumed by [8]. Also, the system is notable to detect malicious behavior in individual read-write commands and the false alarm rate is may be more as well as the same sensitive are given to the each items and there is no concept of attribute sensitivity [6],[3].

[9]Addressed the problem of [8]. The approach adds more rules to some attributes to become more sensitive to detect malicious modification. The limitation of this approach is identification of suitable support and confidence values, also is not suitable for the role based database access control, as well as it is not support other manipulation commands like insert and delete [11],[6].

[6]Try to address the problem of [8]. This approach use to detect the malicious behavior based on RBAC (Role Based Access Control). The technique used in this approach working as control unit on the user role profile. If the technique discover that the user use different role than the normal role of user, then the mechanism will raise notification. The approach is suitable for databases that employ role based access control mechanism. The problem of [9] also addressed in this approach. The limitation of this approach is inability to detect transaction level dependency; so some of the database attacks may be undetected [10].

[10] Addressed the problem of [6] by extracts the correlation among queries of the transaction. The proposed mechanisms called DIDS (Database Intrusion Detection System) generate the transaction profiles mechanism automatically. This mechanism has two phases: learning phase and intrusion detection phase. The learning phase generates authorized transactions profile automatically. The detection phase will check the behavior of executable transactions by compare it with authorized transaction profile. The limitation of this approach thataddress by this study is difficult to capture the malicious data on authorized commands. Developed mechanism to detect the malicious transaction based on predefined profile transactions called Database Malicious Transaction Detection (DBMTD). Therefore, if the enter transaction is not matching with predefined transaction in the profile will detect as misuse or malicious transaction. The limitation of this approach is limited transactions and manual generating of the predefined profile transactions and this cause consuming time as well as difficult to achieve in real andcomplex database installations [13],[10].

The problem of the [12] has been solved by [10] which generate the transaction profiles mechanism automatically. This approach used detection mechanism to detect the misuse activities. The limitation of this approach is inability to detect the authorized malicious activities like delete or update on approved records will address in this study by the author. The previous studies try to solve the problems of malicious activities on the relation database management system. However, the malicious data on the authorized commands can pass to the database. This study tries to address this kind of problems.

Problem Statement

One of the database security problems is inside malicious activities. Among them are: updating of approved records with malicious data, and deleting approved records. This study hypothesize that dependency relationship among items can be used to detect and prevent the aforementioned malicious activities. To test this hypothesis, the following questions needs to be answered:

i. How to represent the dependency relationship to detect and prevent malicious activities?

ii. How to use the dependency relationship to detect and prevent the malicious activities?

III. Methodologies

This chapter discusses the methodologyused to design and develop the detection and prevention mechanism to detect the malicious activities that harm the integrity of database.Scientificresearch is the research which relies on the application of scientific method. So, scientific method can be defined as a set of research principles and methods that helps re-searchers obtain valid results from their research studies by providing a set of clear guidelines for gathering, evaluating, and reporting information in the context of research study [20].

Research Framework

A methodology is required to guide the activities conduct-ed by the project, in order to make sure that all project ac-tivities are well-organized. However, to gather all the in-formation related to the study, the researcher have to build a methodology or research framework to make sure that all the tasks of the project have been done clearly. Figure 1 shows the project research framework.

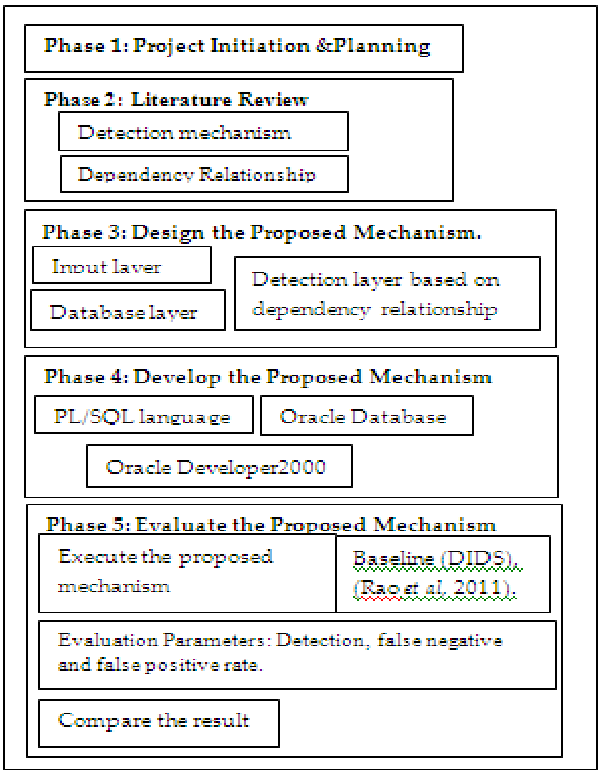

Phase 1: Project Initiation &Planning
Phase 2: Literature Review
Detection mechanism
Dependency Relationship
Phase 3: Design the Proposed Mechanism.
Input layer
Database layer
Detection layer based on dependency relationship
Phase 4: Develop the Proposed Mechanism
PL/SQL language
Oracle Database
Oracle Developer2000
Phase 5: Evaluate the Proposed Mechanism
Execute the proposed mechanism
Baseline (DIDS). (Rao et al. 2011).
Evaluation Parameters: Detection, false negative and false positive rate.
Compare the result

Figure 1:Research Framework

Phase 1: Initial Planning Phase

The first step in achieving this project was the initial planning phase. First of all, the title of the project was discussed with the supervisor. The objective of the project development reviewed and defined according to the problem statement. Besides that, the scope of the project identified to draw the boundary for this project. After that, some re-search on the problem background of the project was done in order to decide on the methodology of the project.

Phase 2: Literature Review

The literature review should give a theoretical base for the research and help to resolve the nature of the research. The purpose from writing the literature review is to reveal to the reader what knowledge and ideas have been established on a topic by previous studies and how similar are they to this project topic. Thus, the literature review for this study started with overview on information security in general term. Then the literature re-view focused on the components influencing on information security, such as insider attack, malicious trans-action. Moreover, continue the study by talking about importance of dependency relationship in the relational database systems. Finally, the discussion goes through related works on how to detect and prevent the misuses activities on the relational database systems. It has two parts:

i. Dependency Relationship:

This part focus about dependency relationship concept, including the purpose of dependency relationship and how the dependency relationship among items can use to detect and prevent the malicious activities.

ii. Detection mechanisms:

Some of the mechanisms that used to detect and prevent the malicious activities have been mentioned in this part. Also the methods used in these mechanisms such as auditing log files, profiling, data mining, and dependency relationship.

Phase 3: Design the proposed mechanism

In this phase, the design of the mechanism will be developed which will contain specification on the mechanism components. The components of the mechanism are three layers: Input layer, detection and prevention layer and database layer as follow:

i. Input Layer

This layer will used to input data to the mechanism. The source of input data is a dataset that constructed by this study. The dataset contains more than 20,000 records that include malicious and none malicious records.

ii. Detection Layer Based on Dependency Relationship

It considers the most important layer in the mechanism. It will receive the data from the input layer and check if there is malicious or not. It is collection of objects such dependency algorithm, alerter and events table. The components of this layer are:

Dependency Algorithm.

The DA dependency algorithm is a set of instructions that used to calculate the total dependency relationship among date items and calculate the data items that related with, to mining the malicious data among items. Chapter 4 will ex-plain more about it.

Alerter

During the process, the malicious activities like updating or deleting commands will be detected by the mechanism. Therefore, an alert needed to be raised by the alerter and notify the DBA.

Events Table

This table used to store the misuse activities events when happened.

Database Layer

The database layer is the original database tables (schema), which store the clean data that coming from the detection and prevention layer. The database layer includes the definition and transaction tables.

1- Definition Tables: These tables store the primary and fix data of the system.

2- Transaction Table: The tables which have the transaction data those changes continuously, for example salaries tables, check tables and so on.

Phase 4: Develop the Proposed Mechanism

Three software products will used to develop the proposed mechanism:

i. PL/SQL Language

Procedural language/ structured query language is the best language to develop the logic of the mechanism. It has a good feature such as: flexibility, easy to use, control statement and so on. Pl/SQL will used to connect all components of the mechanism.

ii. Oracle Database

The oracle database will used to create target database schema such as: tables, views, triggers, procedures and functions of the mechanism.

iii. Oracle Developer2000

Oracle developer is one of the oracle corporation products. The oracle developer2000 will be used to build the inter-faces of the mechanism (input layer).

Evaluation of the Proposed Mechanism

This phase will evaluate the mechanism to verify it meet the project objectives or not. To evaluate the mechanism there are some steps should be executed such as execute the proposed mechanism, baseline, and evaluation measures and compare the result.

i. Execute the Proposed Mechanism

Execute the proposed mechanism to get the results and com-pare it with existing mechanism. The exiting mechanism is DIDS (Database Intrusion Detection system), [10]**.**

ii. Baseline

The baseline of this project is used DIDS (Database Intrusion Detection System), [10].The DIDS is one of the mechanisms that used to detect and prevent the malicious activities in database.

iii. Evaluation Parameters

The measures that will be used in this study to evaluation the accuracy of the proposed mechanism are: detection rate, false negative and false positive rates measures.

1. Detection Rate

Detection rate refers to the percentage of detected malicious events, namely detection rate is equal to the product of the quotient of dividing the number of detected intrusion events by the total of malicious events and 100%.

2. False positive Rate

Rate of false negative refers to the probability that correct events are falsely detected as abnormal events, namely rate of false positive is equal to the product of the quotient of dividing the number of events which are falsely detected as abnormal events by the total of events and 100%.

3. False Negative Rate

Rate of the false negative represent the abnormal or harmful activities which are classified wrongly by detection mechanism as normal activities, namely Rate of false negative is equal to the product of the quotient of dividing the number of events which are falsely detected as normal events by the total of events and 100%.

4. Compare the Results

The results that have gotten will be compared with the results in the existing mechanism. These results will compare the ac-curacy of the proposed mechanism with accuracy in the existing mechanism.

IV. CONCLUSION

Entail Design of the mechanism

The initial results that have gets from this study are initial design of the mechanism, and the flowchart of the mechanism working. Figure 2: show the architecture design for the mechanism and the relations among the components of mechanism. Figure 3shows the mechanism flow processes of the mechanism.

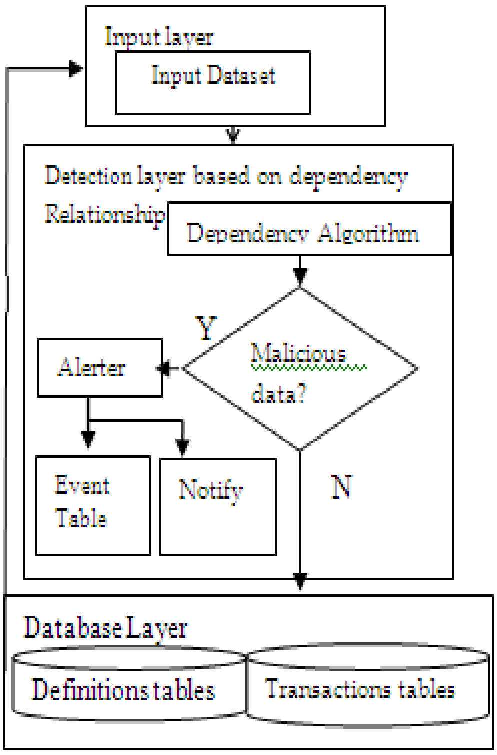


Figure 2: Dependency Relationship Mechanism

According to the proposed dependency algorithm among items the calculate relations among items and data items that related with these relations will be accrue. For example, if the total number of relationship among items is greater than or equal three relations then the attribute is more used and high important. After, that checks the data in the items. If the data has been written already in more than one item, then this item is used in other places by other users and the update or delete is prohibited and classified as malicious. On the other hand,

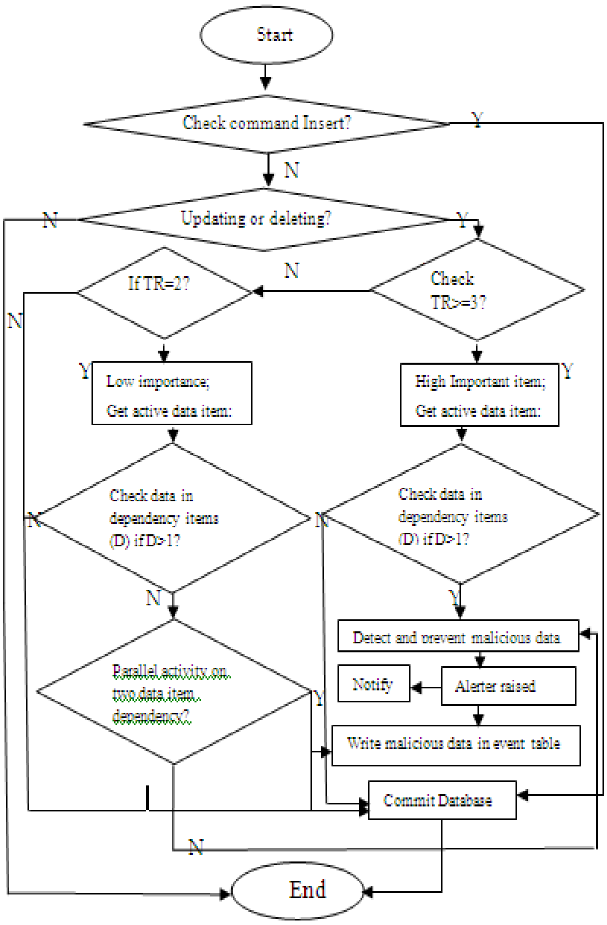
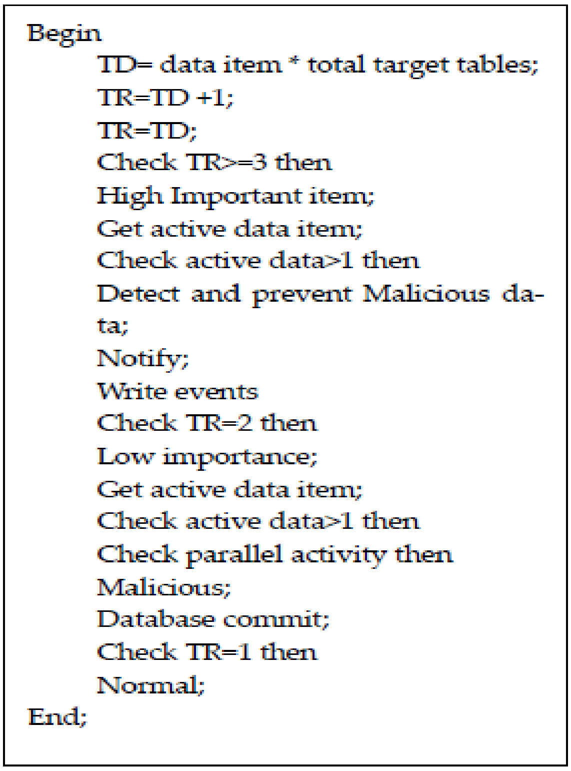

Start
Check command Insert?
Y
N
Updating or deleting?
N
Y
If TR=2?
N
Check TR>=3?
N
Y
Low importance; Get active data item:
High Important item; Get active data item:
Y
Check data in dependency items (D) if D>1?
N
Check data in dependency items (D) if D>1?
N
N
Y
Detect and prevent malicious data
Parallel activity on two data item dependency?
Y
Notify
Alerter raised
Write malicious data in event table
Commit Database
N
End

Figure 3: Mechanism Flow processes

if the total relations among items equal 2 (low important), and the two data items have been used already. So, if there is up-dated or deleted commandon only one data item without other item, it will determine as malicious command. However, if there is updating or deleting in parallel on these two data items, it will be determine as malicious but it will be pass and committed in database. The proposed dependency algorithm working as:

When the authorized user send a command to the database, the algorithm checks the command type, if insert then will move directly to database. However, if the command update or delete then, the algorithm will check first the total number of the dependency relationship among items(TR) and then check the total number of data items(TD) that related by the relation dependency. Therefore, if the TR greater than or equal three relations, then check the relevant data items if data has been written already to more than one item , then the mechanism will detect the activity as malicious and prevent it and notify the DBA as well as write the events to the eventstable. On the other hand, if the TR equal two relations then checkthe TD if written in more than one item, then check the activity on two data items, if parallel activity then detect as malicious but can pass to the database, owing to the data may be correct or not, but if the activity is only on the one data item, thendetect as malicious activity and prevent it, and also notify the DBA and write the event in events table.Algorithm in figure 4 will explain the proposed dependency algorithm among items.



```
Begin
    TD= data item * total target tables;
    TR=TD +1;
    TR=TD;
    Check TR>=3 then
    High Important item;
    Get active data item;
    Check active data>1 then
    Detect and prevent Malicious da-
    ta;
    Notify;
    Write events
    Check TR=2 then
    Low importance;
    Get active data item;
    Check active data>1 then
    Check parallel activity then
    Malicious;
    Database commit;
    Check TR=1 then
    Normal;
End;
```

Figure 4: Dependency Algorithm

REFERENCE

[1] Ren Hui, G., M. Zulkernine, et al. (2005). A software implementation of a genetic algorithm based approach to net-work intrusion detection. Software Engineering, Artificialintelligence,Networking unparallel/Distributed Computing, 2005 and First ACIS international Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth international Conference on.

[2] Nahla Shatnawi, Q. A., and Wail Mardini (2011). "Detection of Insiders Misuse in database Systems proceedings of the internationalMulti Conference of Engineers and computer Science 2011 Vol I, IMECS 2011, March 16 -18, 2011, Hong Kong.

[3] Heady, R. et al. (1990). The architecture of a network level intrusion Javidi, M. M., M.

[4] C. Y. Chung, M. Gertz, and K. Levitt. Demids:A misuse detection system for database systems. In *14th IFIP WG11.3 Working Conferenceon Database and Application Security*, 2000.

[5]Yushi, A. S., Reena Bansal. (2010). "Detection of Malicious Transactions in DBMS." international Journal of Information Technology and Knowledge Management, July-december 2010, Volume 2, No. 2, pp. 675-677.

[6] Bertino, E., E. Terzi, et al. (2005). Intrusion detection in RBAC-administered databases. Computer Security Applications Conference, 21st Annual.

[7] Asmawi,A., Z. M. Sidek, et al. (2008). System architecture for SQL injection and insider misuse detection system for DBMS. Information Technology, 2008. IT Sim 2008. International Symposium on.

[8]Yi, H. and B. Panda (2003). Identification of malicious trans-actions in database systems. Database Engineering and Applications Symposium, 2003. Proceedings. Seventh international.

[9] Srivastava, A., S. Sural, et al. (2006). Weighted intra-transactional rule mining for database intrusion detection. Proceedings of the 10th Pacific-Asia conference on Advances in knowledge Discovery and Data Mining. Singapore, Springer-Verlag: 611-620.States). Dept of Computer Science.

[10]Rao,U., D. R. P. (2011). "Design and Implementation of Database Intrusion Detection system for Security in Database." International Journal of Computer Applications (0975–8887) Volume 35–No.9, December 2011.

[11] Patel, U. P. R. D. R. (2011). "Design and Implementation of Database Intrusion detection system for Security in Database." International Journal of Computer Applications (0975 –8887) Volume 35–No.9, December 2011.Proceedings of the 2008 ACM symposium on applied computing. Fortaleza, Ceara, Brazil, ACM: 1013-1020.

[12]Vieira, M. and H. Madeira (2005). Detection of malicious transactions in DBMS. Dependable computing, 2005. Proceedings. 11th Pacific Rim International Symposium on.

[13] Jos, et al. (2008). Online detection of malicious data access using DBMS auditing. Lab., NM (United States); New Mexico Univ.