Detection and Prevention of Malicious Activities on RDBMS Relational Database Management Systems

Arafat Mohammed Rashad Al-dhaqm, Md.Asri Nagdi Associate Prof. DR. Malaysia

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 prevent the 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.

Index Terms ---**Dependency Relationship; Detection; Prevention; Malicious; Insider Attack;**

1 INTRODUCTION

Information is one of the main assets of any organization which is essential to its continuity. 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, antivirus 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 attacks. Therefore, Detection of Misuse Activities in Database Systems is considered as the last defence layer of the database security systems of any organization.
The insider attack forms the biggest threaten on the database systems due to it has authorized access to the database systems [2].

2 Problem 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 defined 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 outsider 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 insider attacks [6]. According to [2] the insider attacker's forms the biggest threat on the database security level than the outsider attacker, because two reasons, their knowledge about systems and their granted privileges. [7] Indicates that the insider attacks can forms the extremely dangerous on database systems. Furthermore, insider attacks use their rights to achieve the malicious action.

- *Arafat Mohammed Rashad Aldhaqm is currently pursuing masters degree program in computer science (Information Security) in University Technology Malaysia. E-mail: arafat_aldoqm@yahoo.com*
- *Md Asri bin Ngadi, Associate Professor Dr. is currently head of computer science & communication UTM Faculty of Computer Science & Information Technology(FSKSMn . E-mail: dr.asri@utm.my*

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 system management. The mechanism used data mining approach to determine the dependency 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 not able 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 that address by this study is difficult to capture the malicious data on authorized commands. Figure 2.2 shows the architecture of the proposed mechanism.

[12] 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 and complex 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.

3 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?

4 Project Aim

The aim of this project is to develop misuse detection mechanism using dependency relationship among items to detect and prevent the misuse activities in RDBMS relational database management systems.

5 Project Objectives

The objectives of this project are:

1- To design a database mechanism to detect and prevent the misused activities on the approved database records using dependency relationship among items.

2- To develop the proposed detection and prevention mechanism.
3- To evaluate the proposed mechanism with existing mechanism.

6 Project scope

The scope of this project is limited on:

1- The proposed mechanism limited only on the relational database management systems.
2- The dataset used is constructed by this study.
3- The platform is limited on windows environment only.
4- The proposed mechanism will be developed by oracle database, (PL/SQL) language and developer 2000 only.

7 Summary

The insider threats are considered the most dangerous threats that threaten the confidentiality, integrity and availability. The misuse activity is one of the insider threats and considers the most dangerous that focus to damage the critical and sensitive data. Many approaches have been developed to detect and prevent the malicious and anomaly activities. This project concentrates specifically on malicious activities like delete or update approved records.

8 Literature Review

8.1 Introduction

This chapter establishes a background for the study and will begin by reviewing insider attacks overview, malicious activities. After that focus more into the relational database model, dependency relationship and detection mechanisms that utilize to detect and prevent the malicious activities on database systems. Finally, it will conclude on the research gap and what is missing in this area to proceed for further research.

8.2 Overview of the insider attacks

Almost of the organization have been sufferings of the insider attacks. The insider attack formed one of the most important threats on the database security systems. Therefore, the database integrity, confidentiality and availability still more vulnerable towards the insider attacks, and this, lead to believe that the countermeasures is not enough quite.

According to [14] most insider threats on the financial organization were coming from human errors and insider attacks. Therefore, the lack of countermeasures and detection tools on database still not more efficient. Insider attacks can be classified into two types of attacks, intended attack and unintended attack. Intended attack may implement by a malicious user who have or have not authorized access on database level. On the other hand, the unintended attack may happened by authorized user who make effects on database level using SQL commands (insert, update, delete) in wrong way. Moreover, each of which of them may harm the confidentiality, integrity and availably of database. Many tools and mechanisms have been developed to detect and prevent the insider attacks on database level and application level. However, these mechanisms still under developing owing to, there are no one enough efficient security to protect the database [5].

8.2.1 Definition of Insider Attacks

There are many definitions about the insider attacks, the researchers puts these definition of their point of view and according to their knowledge. However, all these definitions have same concept (destroy the confidentiality, integrity and availability) of databases. According to [5] the insider attack is a person who can access through the insider system. [15] Said the insider attack is an individual who has the knowledge of the organizations information system structure to which entity has authorized access. The insider is a person who has privileges to access the underlying system [16]. Threats that generated from person who have been given access rights to an information system and misuse their privileges, thus violating the information system security policy of the organization [17].

8.3 Malicious Transaction

The malicious transaction is one of the insider attacks, the paragraphs below will focus on the overview of the malicious transactions, definitions and reasons of the malicious transactions. According to [5] the malicious transactions consider one of the violent insider attacks that harm the integrity and availability of the database. Many mechanisms have been developed to detect and prevent insider attacks specially detect the malicious command but still there are many weakness in these mechanism which the malicious transactions or data can pass through it, so it is so difficult to detect these kinds of attacks [7]. Malicious transaction is coming in many definitions according to authors, for instance [3] mentioned the malicious transaction is one of the biggest threaten on the database. It is corrupted data that harm the integrity of the database and spread across it. [2] Said the malicious transactions are one of the insider attacks which damage the data by find vulnerabilities in system easily. Malicious transactions are a group of authorized or unauthorized activities, which harm the integrity of database. According to [5] the bad configuration, low DBA (Database Administrator) experiences and absent of security mechanisms as well as hidden flaw and weakness in database implementation can lead malicious transaction or misuses activities. Moreover, the unauthorized and authorized users can cause the malicious transactions.

8.4 Database Modeling

According to [18] database model is the method that represents stored and processed data and their relationships. All database systems stored data in string and numeric data forms, which related together by relations. There are three models to represent the databases such as Network, Hierarchical, and Relational model. This project will utilize the relational database; therefore, the next paragraph will concentrate on the definitions, goals, and types of the relational database model. Almost of the organizations have used the relational database model to process and stored their data. [19] Has been developed this type of database modeling. The relational model is a logical data model that manages and organizes database using relations which make dealing with data is very clear, coherent and easy to work. According to [19] the relation is a group of rows (Tuples) and attributes (columns) that form the table (entity). Table is collection of rows and columns, therefore the relation equal table and the vice versa. The goal of a relational model is to prepare the data to be in consistent form and protect data from some anomaly activates like duplicating or losing, as well as, it supports operations for data manipulation such as insert, update, delete and select.

8.4.1 Types of Database Relations

The next paragraphs show three types of database relations.

I- ONE-TO-ONE RELATIONSHIPS

One-to-one relationship is a relation that has two direction relationships, which means that there is one value in both directions [19].

II- ONE-TO-MANY RELATIONSHIPS

One-to-Many relationship defines as one entity has many value relationships with another entity [19].

III- MANY-TO-MANY RELATIONSHIPS

Many-to-Many relationship is a relationship that is more than one value in both directions [19].

8.5 Dependency Relationship

The information above has given a clear meaning about relationships among data items and kinds of these relations. According to [19] dependency relationship represent as pointers of the resources. The pointer denotes to that resource only. The dependency concept in database represent data stored in same table as uniquely form. These data denote to other data in same table or in other table. The dependency can define as a relationship among the attributes that determine the groups of attributes values by one attribute value. For example, the passport number, refer to other information (name, family, nationality, issue date, and other information in passport), so all these information dependent on the passport number. By other words, the dependency relationship is like a tree family, son dependent father, father dependent grandfather and thus. Therefore, this study use this concept to protect database from misuse activities by know the dependent data in whole database tables.

8.6 Evolution Parameters

The measures that will be used in this study to evaluate the accuracy of the proposed mechanism are: detection rate, false positive rate and false negative rate. Detection rate refers to the percentage of detected intrusion events, namely detection rate is equal to the product of the quotient of dividing the number of detected intrusion events by the total of intrusion events and 100%. The false positive 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%. 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%.

8.7 Existing Mechanisms to Detect and Prevent Malicious Activities

Many mechanisms have been developed to prevent and detect the malicious activities in database systems. However, a lot of them based on a predefined data profile generated from database log file and a few used a dependency relationship among the data items. So, this part will explained these mechanisms.

[8] Stated that the mechanisms based on auditing only detect the malicious commands, and if legitimate commands contain malicious data, it will not be detected. [8] Proposed mechanism to detect and prevent the malicious activities in database management systems based on data dependency among items. The mechanism use data mining approach to extract data dependency among data items through classification rules. The classification rules represent three sets (pre-written, read, and post-written set). These rules working as control unit to detect the malicious modification, for instance: what data item must be read (pre-write) before this data item is updated and what data item must be updated after one data item updated (post-write). So if there is any activity does not matching with these rules will define as malicious activity. The limitation of this mechanism is limited to user transactions that conform to the read-write patterns assumed by the authors. Also, the system is not able 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 attributes and there is no concept of attribute sensitivity, [9], [3] ,[6].

[9] Has solved the attributes sensitivity problem in [8]. The proposed mechanism to detect malicious activities in the da-

tabase management system add more rules to compare the sensitive attributes than the rules in approach presented in [8]. The sensitive attributes become more sensitive to malicious modification than other attributes, for instance the important attributes like the verification attributes (columns) must given more sensitive than other attributes. So if there is any modification on these attributes the alarm raise notification. Therefore, if there are any transaction does not follow these dependency rules will identified as malicious transaction. The limitation of this approach is limited to detect the malicious modification data only; it does not include the others command like inserting or deleting data as well as the identification of suitable support and confidence values, [6], [11].

[6] try to address the problem of [8]. Also Part of the limitation [9] approach already has been solved by [6]. This approach use to detect the malicious behavior based on RBAC (Role Based Access Control). The technique has 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 working on role based access control mechanism. The limitation of this approach is inability to detect transaction level dependency; so some of the database attacks may be undetected [12], [10].

[12] Addressed the detection of malicious activities in DBMS by developed a mechanism called Database Malicious Transaction Detection (DBMTD). This mechanism tries to solve the problems of [8]. The mechanism based on two different phases called transactions profile phase and detection phase. The authors assumed authorized transactions were known already in advance. The DBA (Database Administrator) is responsible for prepared it manually to the detection mechanism, then the detect phase check the user activities with the profile phase, if there is any transaction does not match with the commands in the profile, then the detect phase will raise notification. 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 and complex database installations,[10],[13]. Figure8.1 displays the mechanism that used in this graph.

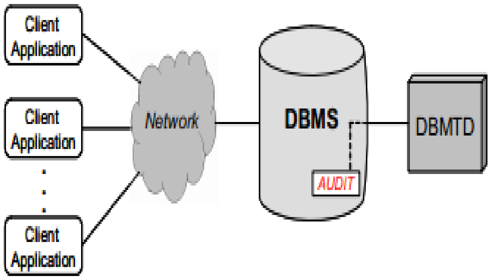

Figure 8.1: DB system using the DBMTD Mechanism.

The problem of the [12] has been solved by [10]. 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. So when the users send queries to database system, the query will pass through the database intrusion detection system (DIDS) and the checks the transaction is authorized for that user or not. If the transaction is authorized then DIDS allows the transaction to commit into the DBMS unless, capture it as malicious activities. The limitation of this approach that address by this study is difficult to capture the malicious data on authorized commands.

8.8 Discussion

Through the existing mechanisms, almost of the authors have been used the auditing log file to prepare the profile of the authorized transaction automatically or manually. Therefore, the mechanisms starting to verification previous command (predefined command) with user activities. Therefore, what about authorized commands like delete or update on the approved records. The idea of this project will address this situation, through add detection and prevention layer between the end user and the original database to add more verification on data as well as protect the data from malicious activities before it go to original database. The authors will use the concept of the dependency relationship among items detect and prevent the misuse activities. Chapter 4 will explain more about this idea.

8.9 Summary

In conclusion, as a result of the lack of providing good mechanism to detect and prevent the misuse activities on relational database systems, the authors will used the dependency relationship among items. The dependency relationship among items will detect and prevent the missus activities among items.

9 Methodologies

9.1 Overview

This chapter discusses the methodology used to design and develop the detection and prevention mechanism to detect the malicious activities that harm the integrity of database. Scientific research 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 researchers 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].

9.2 Research Framework

A methodology is required to guide the activities conducted by the project, in order to make sure that all project activities are well-organized. However, to gather all the information 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 9.1 shows the project research framework.

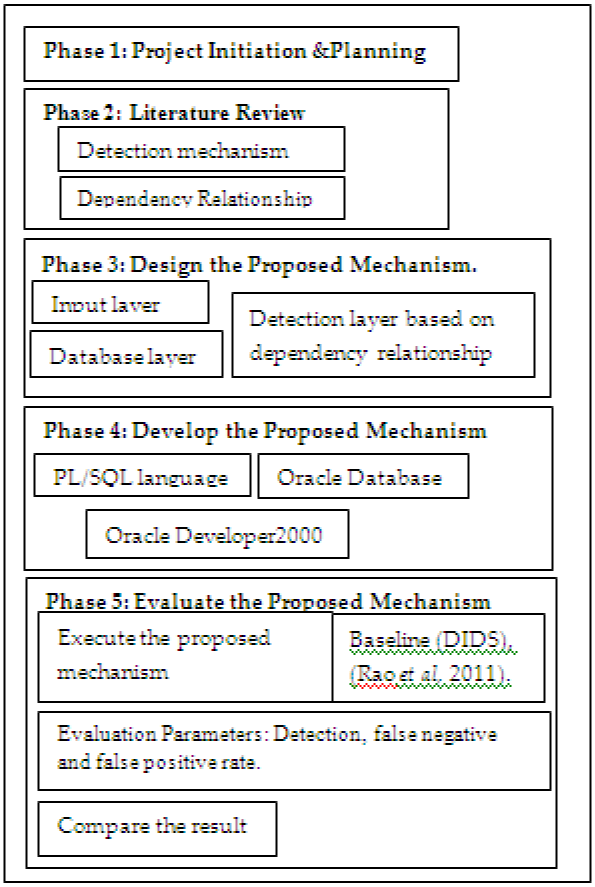
Phase 1: Project Initiation &Planning
Phase 2: Literature Review
Detection mechanism
Dependency Relationship
Phase 3: Design the Proposed Mechanism.
Input layer
Database layer
Detection layer based on dependency relationship
Phase 4: Develop the Proposed Mechanism
PL/SQL language
Oracle Database
Oracle 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 9.1: Research Framework

9.2.1 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 research on the problem background of the project was done in order to decide on the methodology of the project.

9.2.2 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 review focused on the components influencing on information security, such as insider attack, malicious transaction. 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.

9.2.3 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:

a- 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 explain more about it.

b- 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.

3-Events Table

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

iii 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.

9.2.4 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 interfaces of the mechanism (input layer).

9.2.5 Evaluation 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 compare 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%.

iv Compare the Results

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

9.3 Environment Used

This project needs the hardware and software requirements to achieve the mission.

3.3.1 Hardware Requirement

1- One PC with this descriptions:-
- At least (2000) megahertz (MHZ) Pentium processor.
- At least 250 megabytes (MB).
- At least 5 GB available on hard disk.

9.3.2 Software Requirement

2- Windows XP with SP2 or windows Vista.

3- Oracle10G or 9i

4- Oracle developer 2000

5- 9.4 Summary

Scientific research is that type of research which applies a set of principles and rules which ensure the validity of result obtained by the researcher. In this chapter, the different phases of this project, misuse activities problem identification, literature review, mechanism design, development and testing are discussed. Each phase plays an important role in accomplishing the aim of this project. The next chapters will cover the remaining phases of this project, which are mechanism design, development and evolution mechanism.

10 Initial Finding

10.1 Overview

In this chapter, the initial finding of the study will be discussed. The content of this chapter will give a general view of the future results of this project.

10.2 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 10-1: show the architecture design for the mechanism and the relations among the components of mechanism. Figure 10-2 shows the mechanism flow processes of the mechanism.

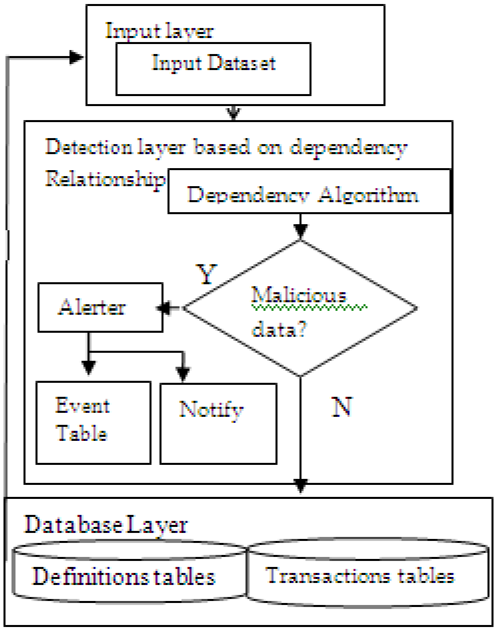

Figure 10.1: Dependency Relationship Mechanism

The Figure 10-2 below show more details of the mechanism working.

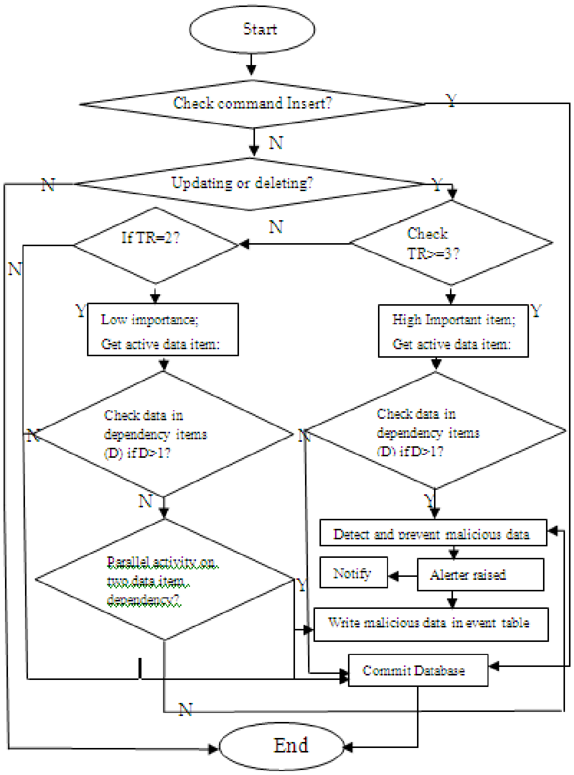
Start
Check command Insert?
Y
N
Updating or deleting?
N
Y
If TR=2?
N
Check TR>=3?
N
Y
Low importance; Get active data item:
High Important item; Get active data item:
Y
Check data in dependency items (D) if D>1?
N
Check data in dependency items (D) if D>1?
N
N
Y
Parallel activity on two data item dependency?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

Figure 10.2: Mechanism Flow processes

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, if the total relations among items equal 2 (low important), and the two data items have been used already. So, if there is updated or deleted command on 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 the 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 events table. On the other hand, if the TR equal two relations then check the 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, then detect as malicious activity and prevent it, and also notify the DBA and write the event in events table. Algorithm 10.3 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 data;
        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 10.3: Dependency Algorithm

REFERENCE

[1] Ren Hui, G., M. Zulkernine, et al. (2005). A software implementation of a genetic algorithm based approach to network intrusion detection. Software Engineering, Artificial intelligence, Networking and Parallel/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 international Multi 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 Conference on 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 transactions 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.

[14] Chickowski.E(2011).Insider Attacks and Human Error. Is Your Database Safe?.http://www.channelinsider.com/c/a/Security/Insider-Attacks-and-Human-Error-Is- Your-Database-Safe-293745.

[15] Althebyan, Q.(2008). Design and analysis of knowledge-base centric insider threat models. University of Arkansas.

[16] Nguyen, N., P. Reiher, et al. (2003). Detecting insider threats by monitoring system call activity. Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics society.

[17] Theoharidou, M., S. Kokolakis, et al. (2005). "The insider threat to information systems and the effectiveness of ISO17799." Computers &amp; Security 24(6): 472-484.

[18] DIETZE, et al.(1994). Network Model Database of Eukaryotic Transcription Regulating sequences and Proteins, 1994.

[19] Codd, E.F.(1070). A relational model of data for large shared data banks. Comm. ACM 13, 6 (June 1970), 377-387.detection system'. Tech. rep., LA-SUB{93-219, Los Alamos National

[20] Marczyk. C(2005). Essential of research design and methodology.