International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-2, Issue-6, March, 2015

A Proficient Way to Avert Malicious Transactions in Database Management System

Abhishek Mukherjee
Department of Computer Science and Engineering
Dr.B.C.Roy Engineering College
email: abhishekmukherjeee009@gmail.com

Abstract— **In recent years database security has become one of the major issues in computer security. Database security is concerned with preventing unauthorized and malicious access into a database. A number of mechanisms needed to defend information, such as verification, user privileges, data encryption, and auditing, are available in DBMS. In reality, malicious access of databases by unauthorized users by detecting system vulnerabilities and unauthorized database transactions done by authorized users cannot be handled by a simple database security mechanism. So, Database Intrusion detection systems have turn out to be a crucial matter for computer systems security infrastructures. This paper raised a proficient mechanism to avert malicious transaction in the database indemnity system.**

Keyword — **Database, Malicious, Intrusion, Benign, Transaction.**

I. INTRODUCTION

Information is a core asset of any institute to maintain its permanence. So, information security is necessary to protect the reliability, discretion and accessibility of information. The primary objective of database security research is protecting the database from unwanted activities. Unwanted activities can be authenticated misuse, malicious actions or involuntary mistakes made by authorized individuals or processes. This unauthorized access of database can be in form of malicious transaction perforating the security of database. The protection against data corruption is one of the main problems faced by system administrators. Due to the growth of networked data, security attacks have become a dominant problem in practically all information infrastructures. Many refined security systems are used to meet the security requirements but they may have security vulnerabilities or miss configuration of those systems. A successful security attack lies on the vulnerabilities of the system.

In an organizations, massive no of employees use their database from their individual departments where each user has their own userID. So by identifying their userID, the system detects the person as authorized or unauthorized person also known as external attack detection. But if an authorized person doing activities that are not integral for their task and unsafe for the organization, then the system cannot detect those activities as suspicious activities with simple security system. This type of attack is known as an internal attack. Usual database security attacks can be premeditated illegal attempts to access private data or malicious actions executed by authorized users to corrupt critical data or exterior interferences intended to cause undue delays in accessing data. To protect the database from this type of intrusions the researchers develop intrusion detection system.

Typically, Intrusion Detection Systems (IDS) are used to identify any unauthorized activities, threats, attacks on any type of resources available. Intrusion detection systems are categorized based on their source of data collection and on the strategy employed in detecting intrusions. Based on the source of audit data, IDS are either host based or network based. While from the strategy perspective, IDS are either misuse based or anomaly based [1]. Most IDSs detect those activities at the transaction level. Such attacks are identified by analyzing the transaction logs. A transaction log records all the transactions of the database. By analyzing these logs most wicked activities can be identified. This paper proposed an intrusion detection system to protect database against malicious activities. The system mainly works in two segments: the transaction modeling and intrusion detection. In the transaction modeling segment, collected data are used to create models which are stored in a data warehouse. In the detection segment, the current event is compared with those models in the data warehouse to detect if it is normal or malicious.

II. RELATED WORK

Many research works has been going since many years in the field of database security. Wenhui et al. [2] proposed a multi-layer mechanism to sense intrusions against a web-based database services. A real-time database intrusion detection system is proposed by Lee et al. [3] using time signatures by observing the database performance at the point of sensor transaction. Whenever a transaction attempts to update a pre updated temporal data in that period, an alarm is raised. Hu et al. [4] suggested an intrusion detection mechanism based on data dependency, generated in the form of association rules. Transactions that do not pursue data dependency rules are identified as malicious transactions. Some attributes are measured as more responsive to malicious adaptation compared to others. Srivastava et al. [5] proposed a weighted data mining algorithm to find dependencies among those sensitive attributes. Transactions that do not follow dependency rules are marked as malicious. Kamra et al. [6] have proposed a role based access control mechanism to detect malicious actions in databases. By classification technique role profiles of authorized user behaviour are designed. When role profiles for given user is different than the original role of a user an alarm is raised. The approach presented by Rao et al. [7] based on transaction level dependency. In [8], Vieira et al. addressed the detection of malicious DBMS transactions with the assumption with manually generated transactions profile. In[9] Rao et al. proposed the database IDS which incorporates to generate authorised transactions profile automatically instated of manually and detection phase is also automated to ensure the performance of the system. In [10], Lee et al. discussed about a structure for continuously adapting the intrusion detection system for a computer environment as it is upgraded. The paper shows a number of data mining approaches to solve this problem.

III. APRIORI ALGORITHM

“Apriori” [11] is an algorithm for frequent item set mining over transactional databases. It identifies the regular individual items in the database and extends them to larger item sets as long as those item sets appear sufficiently often in the database. Apriori is considered to work on databases containing transactions, like collections of items bought by customers, or details of a website frequentation. Here, frequent subsets are extended one item at a time and groups of candidates are tested against the data. When no more successful extensions are found, the algorithm terminates. Apriori uses bfs and a Hash tree structure to count candidate item sets efficiently. It generates candidate item sets of length k from item sets of length $k-1$. Then it prunes the candidates which have an infrequent sub pattern. The candidate set contains all frequent k-length item sets. After that, it scans the transaction database to determine frequent item sets among the candidates.
Main steps of iteration are:

1. Find frequent set *Lk-1*
2. Join step: *Ck* is generated by joining *Lk-1* with itself (Cartesian product *Lk-1* × *Lk-1*)
3. Prune step (Apriori property): Any (*k–1*) Size item sets that is not frequent cannot be a subset of a frequent *k* size item sets, hence should be removed.
4. Frequent set *Lk* has been achieved

Where, *Ck* as a candidate item set of size *k*
Lk as a frequent item set of size *k*

This algorithm uses breadth first search and a hash tree structure to make candidate item sets efficient, and then the frequency occurrence for each candidate item sets will be counted. Those candidate item sets that have higher frequency than minimum support threshold are qualified to be frequent item sets. The support value is simply the number of transactions that include all items in the antecedent and consequent parts of the association rule. The support is sometimes expressed as a percentage of the total number of records in the database. Apriori algorithm is better than using association rules. The most important advantage of this algorithm is that incremental updating of the rule set is easy. Apriori algorithm was used in the proposed method to improve the detection systems.

IV. PROPOSED APPROACH

Any activity in database leaves evidence in transaction log table. This transaction log data can be easily formatted into a database table and program executions and user behaviour have common connection among system features. Transaction dataset of user behaviour is too large, so it is important to use a mining algorithm. In this paper a well known algorithm, Apriori algorithm is used to handle the transaction data and calculate the support value. Apriori algorithm is efficient in handling large datasets.
The audit log contains the data about previous transactions executed by the authorized users. These audit information are used to create models with help of Apriori algorithm. Therefore, any user who wants to perform any transaction in DBMS also generates a current transaction log. Now, to detect the transaction is valid or not, the current transaction information is compared with transactions models. If the current information about the transaction fulfils all requirements then this transaction will be marked as valid or benign transaction. The figure below illustrated the scenario of method.

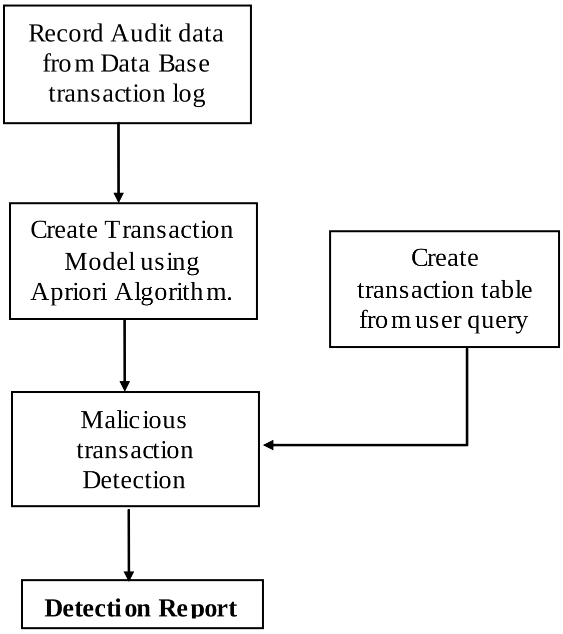
Record Audit data from Data Base transaction log
Create Transaction Model using Apriori Algorithm.
Create transaction table from user query
Malicious transaction Detection
Detection Report

Figure1: Scenario of the Model

The auditing mechanism collects all the information about the instructions executed by users from the log file. Username, user session ids, sequence number, command type, name of the target object, owner of the target object, transaction ids etc. are example of some information logged for each action by the database user. These audit information are used to create models with help of Apriori algorithm and stored at the system for future use. When any user performs any transaction in DBMS also generates a current transaction log. Required information like session id, transaction id, command type, target object for that particular user are submitted and stored in the log table. Now, in malicious transaction detection phase of the method an algorithm is developed to detect the type of the transaction. The proposed algorithm of this phase is given below;

```
Input: A set of transactions 'T' contain session_id, transaction_id, target_obj,command_type.
Output: Transaction is malicious or benign

Begin
    Read the values from T ordered by session_id ;
    Let count =null ;
    While T contain values ;
    increment the count by 1 ;
    For each session_id of T ;
    Read the values of Transaction model ;
    If session_id and transaction_id for T and Transaction model matches ;
    Read the support value for the corresponding session_id of transaction model
    if support value > min support threshold
    compare command_type and target_obj for current session_id ;
    if command_type and target_obj for current session_ID matches;
    Transaction is Benign
    else Malicious Transaction
    increment the value of session_id by 1
End
```

In this algorithm the current transaction information are compared with transactions models according to their session and transaction ids. If the current transaction information like command type and target object for a particular session id and transaction id, matches with transaction models, whose occurrences exceed a predefined minimum support threshold for that session id, then the particular transaction is allowed to commit into the DBMS and detected as valid or benign transaction. If it does not match the transaction is never allowed to commit into the DBMS and marked as a malicious.

TABLE I
SUPPORT VALUES FOR CORRESPONDING SESSION IDS.

Row	*session_id*	*Support*
1	*23*	*0.667*
2	*24*	*0.89343*
3	*25*	*0.46465*
4	*29*	*0.29642*

For example, in row 1 in the table, Apriori algorithm creates a model which contains that, for session id '23', support is 0.667. It means 66.7% of the time the user does authentic and benign activity for this session id.

TABLE II
A PARTIAL VIEW OF LOG TABLE

User Name	*session_id*	*transaction_id*	*command_type*	*target_obj*
A1	*23*	*1*	*Select*	*Order*
A1	*23*	*1*	*Select*	*Order*
A1	*22*	*2*	*Insert*	*Sale*
A2	*24*	*5*	*Update*	*Stock*
A2	*24*	*5*	*Update*	*Stock*
A3	*25*	*7*	*Delete*	*Order*
A3	*26*	*8*	*Select*	*Order*
A4	*28*	*11*	*Delete*	*Sale*
A4	*28*	*11*	*Delete*	*Sale*
A4	*29*	*14*	*Update*	*Stock*

In this algorithm the system compares the support value for the particular session id. If a user having session id “26”, transaction id “8” performs a “select” operation where the target object is “order”, then the intrusion detection algorithm mark the transaction as malicious though the information for current audit log and transaction model matches, as the occurrences of session id does not exceed the predefined minimum support threshold value 50%, set by administrator

Again, in the database, user having session id “26”, transaction id “8” performs a “select” operation on “Sale” then the intrusion detection algorithm mark the transaction as malicious as the target object for both data does not matches, even if it satisfies the minimum support value.

A transaction will be considered as valid or benign transaction only when it satisfies the minimum support value and all the information available in authorized transaction model. For example, a user having session id “23”, transaction id “1” performs a “select” operation where the target object is “order” satisfies the minimum support threshold value, is detected as benign or valid transaction.

A false positive occurs when an intrusion detector erroneously detects an intrusion in a non-infected transaction. As the filtration process of this system is strict, the number of false positive rate will be very less.

V. CONCLUSION

Intrusion detection plays a very crucial role in database security system. This paper proposed an approach for the detection of malicious transactions in database. In this approach, models of valid transactions are generated to detect unauthorized transactions. It consists of two different segments: transaction modelling and intrusion detection. Intrusion detection consists in the detection of all the activities executing sequences of instructions that potentially represent intrusion attempts.

ACKNOWLEDGMENT

I wish to express my appreciation to all the faculty members of department of CSE & IT, Dr. B. C. Roy Engineering College. Thanks to all of them for giving me valuable advice. Particularly, I would express my gratitude to my project guide Mr. Saindhab Chattaraj, Asstt.Prof. Dept. of CSE, Dr. B. C. Roy Engineering College, for his patience, understanding, excellent guidance, encouragement and inspiration through-out the project work. Without his patient guidance, this work would never have been a successful one. I would also like to thank all my classmates for their valuable suggestions and helpful discussions.

REFERENCES

[1] Ajayi Adebowale, Idowu S.A, Otusile Oluwabukola, “ An Overview of Database Centred Intrusion Detection Systems”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-2, December 2013

[2] Wenhui S., Tan T., “A novel intrusion detection system model for securing web based database systems”, In Proceedings of the 25th annual international computer software and application conference (COMPSAC), pp. 249-254, 2001

[3] V. C. S. Lee, J.A. Stankovic, S. H. Son, “intrusion detection in real-time database system Via time signatures”, real time technology and application symposium, PP. 124, 2000.

[4] Y. Hu, B. Prasad, “A data mining approach for database intrusion detection”, In Proceedings of the ACM Symposium on applied computing, pp. 711-716, 2004.

[5] Srivastava, A., Sural, S., Majumdar, A. K., “Weighted intra-transactions rule mining for database intrusion detection”, In Proceedings of the Pacific-Asia knowledge discovery and data mining (PAKDD), lecture notes in artificial intelligence, Springer. Pp. 611-620, 2006.

[6] Bertino E., Terzi E., Kamra A., Vakali A., “Intrusion Detection in RBAC-Administered Database”, In Proceeding of the 21st annual computer security application conference (ACSAC), pp. 170-182, 2005.

[7] Udai Pratap Rao, G. J. Sahani, Dhiren R. Patel, "Detection of Malicious Activity in Role Based Access Control (RBAC) Enabled Databases", International Journal of Information Assurance and Security, pp. 611-617, Volume 5, Issue 6, USA, ISSN 1554-1010,2010.

[8] Marco Vieira, Henrique Madeira, "Detection of Malicious Transactions in DBMS", Dependable Computing, 2005. Proceedings. 11th Pacific Rim International Symposium on 12-14 Dec. 2005.

[9] Udai Pratap Rao, Dhiren R. Patel, "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*

[10] W. Lee, SJ Stolfo, KW Mok, "Data mining approaches for intrusion detection", *Proceedings of the 7th USENIX Security Symposium*, 1998.

[11] Rakesh Agrawal and Ramakrishnan Srikant, "Fast algorithms for mining association rules in large databases".Proceedings of the 20th International Conference on Very Large Data Bases, VLDB, pages 487-499, Santiago, Chile, September 1994.

[12] http://www.wikipedia.org