Data-Base Security Using Different Techniques: A Survey

Abhijeet Sartape [#1], Prof. Vasgi B. P[*2]

[#*]Department of Information Technology, Sinhgad College of Engineering
Pune-41, India

***Abstract*— In many organizations, Database Security plays an important issue for their safe & secure environment. Performance of the organization or any enterprise should depend on Database Security, i.e. Insider attack detection. In this paper, mainly three insider attack detection techniques introduced are as follows Log examining, Query clustering & Policy-based mechanism. In Log examining approach given transaction of each user should be examined or tested for insider attack. In Query clustering approach external query (outlier) i.e. other than a cluster of query, should be detected. In policy-based mechanism, each user having its own policy data & if any policy violated, then it should be detected as an insider attack. These three approaches should perform database correlations for identifying malicious database transactions.**

***Keywords*— Database Security, Log Examining, Query Clustering, policy Based Mechanism.**

I. INTRODUCTION

In today's world, many organizations or enterprises have a huge amount of databases to store its data. However, this data storage, maintenance and access are very hard and important issues for organizations. In these organizations, there are huge no of employees wants to use their database from their respective departments. In this case, each user has their own identity proof as like their userID. So by identifying their userID we detect as a person is authorized person or unauthorized person. But this detection is like identify from user name and password so that known as external attack detection. But if in case legitimate or authorized person or employee doing activities that are not fitted for their role & it will be harmful for their organization, then how we decide that those employee activities is suspicious activity & how we detect that, this is known as an inner attack. So data should be stored and accessed by only authorized or legitimate users otherwise this work will be acts as an attack on database. So databases should maintain its own security policies for their safe and secure environment [1]. Gartner research presented that Database transaction's activities and behaviors are examined for to detection of data leaks as well as for detection of malicious insider attacks done by legitimate user or authorized user [2],[3] SQL injection and Data exfiltration attacks are database-related attacks this is not issuing regarding operating system or the network [11]. In database security, inner attacks are done by a trusted people within that organization, so each and every organization should have their own security policy solutions or approaches to fix that problem. Inner attack is mainly detected and resolved by using three techniques, that is Log examining, Query clustering & Policy-based mechanism. These three techniques are performed as like anomaly detection technique in the intrusion-detection system. i.e firstly, observe behavior of each user during training phase, and collect some data and recorded as a benchmark for testing phase. By comparing the training phase with testing phase, If a result of training phase is match with the result of testing phase, then and then only, current activity of that user should be considered as normal activity.

II. RELATED WORK

Database Intrusion Detection Systems:

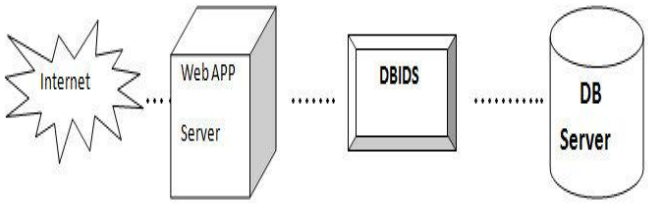

Fig.1: Database intrusion Detection System

Fig. 1 illustates the database intrusion detection System. Intrusion is nothing but the unauthorized access of data it is known as intrusion. And system which detects that system is known as the intrusion-detection system. This system is works on which domain, i.e. database or network domain then corresponds to that domain its name is database intrusion detection system or network intrusion detection system But above Database intrusion detection, system simply acts as a database firewall. It detects only external attacks as per, we provide the signature to the firewall database. But problem is that how to detect an attack when it is done by an authorized or legitimate users. So this can be the major issue for to detect an insider attack among the all legitimate user. To solve this problem or to overcome these limitations some techniques or approaches are studied from references. There are mainly three approaches listed here as follows,

A. Log Examining for DBIDS

Yi Hu, Alina Campan, James Walden, Irina Vorobyeva, Justin Shelton [4] used data mining approach for database

security. This approach determines the data dependencies among the data items in the database system. Data dependency is nothing but the access correlation between data items. From that, those transactions which are not complied with rules generated from read and write operations are identified as malicious transactions. Srivastava et al.used a weighted sequence mining approach [5] for detection of database attack. The classification rules reflecting the data dependencies are generated from the database log. Compared to other approaches of detection malicious transactions this approach is less sensitive to the user behavior changes. Data item is nothing but the piece of information i.e. Read & Write like operations, and Domain is nothing but the collection of some data items.

Flow of log examining technique:

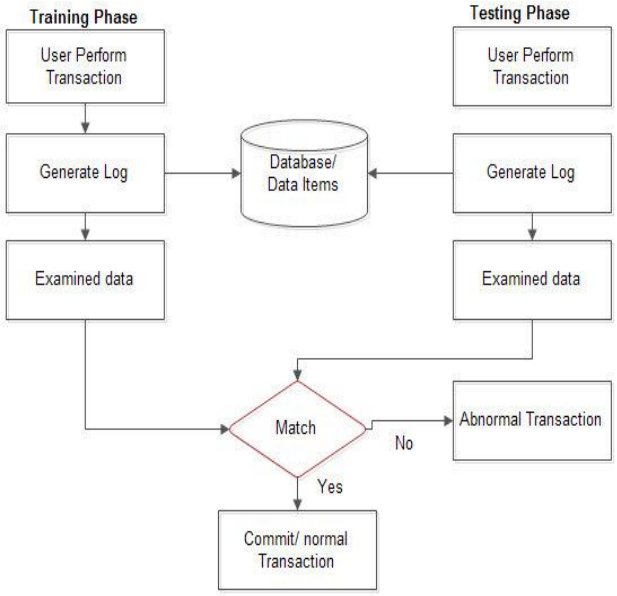

Fig..2: Log Examining Technique

Working of Log examining approach :

Fig. 2 illustrates the working of log examining technique. In Log examining a technique during training phase, each transaction should be examined i.e. transaction details are collected from log of given database. Then after that sort out some result data items which are already participated in details of log. By using some strategies like threshold or by applying algorithms like apriori algorithms on that data items and also some correlation between them that generate some rules, which are used for to collect some result data during training phase. This result data of the training phase it acts as a benchmark or sample data for testing phase. Then this training phase sample data will be examined in the future with testing phase data, if that is matches with each other, then and then only this transaction will be considered as normal transaction and that transaction will be committed [4].

In Log examining technique input is nothing but the user performed data, i.e. Log details, and then on that Log data operations are performed in three states that are frequent data items discovery phase, correlated data items generation phase and data dependency rules generation phase. From that, the output of the system will be either considered as normal transaction or abnormal transaction.

B. Query clustering for DBIDS

Sunu Mathew, Michalis Petropoulos, Hung Q. Ngo, and Shambhu Upadhyaya [7] are used semantics of the query for database security, which is more powerful than query syntax. In Query clustering, technique for each user, application can be interacted with the database by firing queries. For each query compute a statistical summary of the query result tuple. Then a summary of the query is represented by a vector of fixed dimension unlike of how a large query results.

Flow of query clustering for DBIDS:

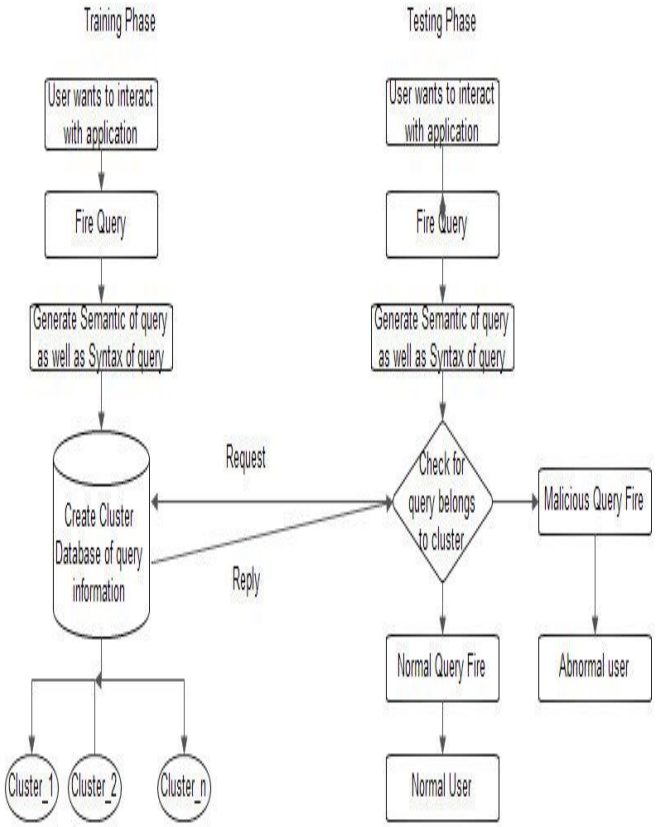

Fig.3: Query Clustering Technique

Working of query clustering approach:

Fig. 3 illustrates the working of query clustering technique. In training phase user wants to interact with application, i.e. database, so they fire query, which is regarding a database results. From that, system will generate query information, which is use full for making of cluster database of queries. Then that cluster database will be used as sample data or benchmark for testing phase. So by checking with training phase cluster data with testing phase query and decide that, either current query will be belonged to that cluster database

or either considered as an outlier, then result of that will be classified as normal user or abnormal user.

C. Policy Based Mechanism for DBIDS

Ashish Kamra and Elisa Bertino [11] used policy-based mechanism for database security. In this system, firstly, it checks for abnormal transactions and after that once an anomaly is detected, then it takes some actions against that an anomaly. In this system, actions are based on their severities that are low severity, medium severity action, and high severity action. Three types of an action are taken against any abnormal transactions or any malicious modifications. This system is based on profile based approach.

Flow of policy based Approach:

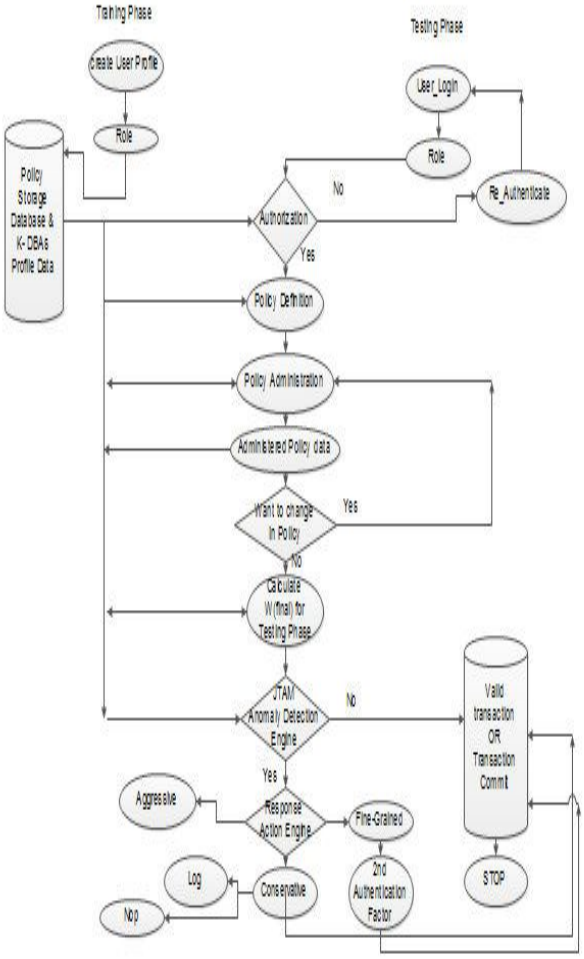

Fig.4: Policy Based Mechanism

Working of policy based approach:

In policy-based mechanism, each user has its own policy data. It is based on separation of duty's principle, i.e. fine grained data access control for different DBAs. Here each DBAs have its own policy data, then by using secret key with respective DBAs generate hash of that policy. Then by combining all the number of DBAs hash it will generate the final valid signature. Then take this final valid signature as a sample benchmark in training phase. By comparing with final valid signature in training phase with final valid signature of testing phase if both are match then and then only considered as, given transaction is done by normal DBAs. Otherwise, it should have been abnormal in nature.

III. Conclusion

In this paper, we have studied different database intrusion detection techniques These techniques provide protection of database security from a legitimate users, who has done suspicious activities. It also provides secured, fine – grained data access control based mechanism. So these techniques are useful for inner attack detection.

References

[1] A.Conry-Murray," The Threat from within. Network Computing (AUG. 2005)," , July 2009.

[2] R. Mogull, "Top Five Steps to Prevent Data Loss and Information Leaks. Gartner Research (July 2006)," 2010.

[3] M. Nicolett and J. Wheatman, "Dam Technology Provides Monitoring and Analytics with Less Overhead. Gartner Research (Nov. 2007)," http://www.gartner.com, 2010.

[4] Yi Ru, Alina Campan, James Walden, Irina Vorobyeva, Justin Shelton, "An Effective Log Mining Approach For Database intrusion Detection *", 978-1-4244-6588-0/10 IEEE, 2010.

[5] Srivastava, A, Sural S., and Majumdar, AK.: Database Intrusion Detection Using Weighted Sequence Mining, Journal of Computers, vol. 1, no. 4 (2006)

[6] Agrawal, R., Imieliilski, T., Swami, A: Mining association rules between sets of items in large databases, In Proceedings of the 1993 ACM SIGMOD international conference on Management of data (1993)

[7] Sunu Mathew, Michalis Petropoulos, Hung Q. Ngo, and Shambhu Upadhyaya, "A Data- Centric Approach to Insider Attack Detection in Database Systems", S. Jha, R. Sommer, and C. Kreibich (Eds.): RAID 2010, LNCS 6307, pp. 382–401, 2010. Springer-Verlag Berlin Heidelberg 2010.

[8] Babcock, B., Chaudhuri, S., Das, G.: Dynamic sample selection for approximate query processing. In: SIGMOD Conference, pp. 539–550 (2003).

[9] Chung, C.Y., Gertz, M., Levitt, K.: Demids: a misuse detection system for database systems. In: Integrity and Internal Control Information Systems: Strategic Views on the Need for Control, pp. 159–178. Kluwer Academic Publishers, Norwell (2000).

[10] Fonseca, J., Vieira, M., Madeira, H.: Online detection of malicious data access using dbms auditing. In: Proc. of the 2008 ACM Symposium on Applied Computing (SAC 2008), pp. 1013–1020 (2008).

[11] Ashish Kamra and Elisa Bertino," Design and Implementation of an Intrusion Response System for Relational Databases", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, vol. 23, no. 6, June 2011.

[12] A. Kamra, E. Terzi, and E. Bertino, "Detecting Anomalous Access Patterns in Relational Databases," J. Very Large DataBases (VLDB),vol. 17, no. 5, pp. 1063-1077, 2008.

[13] A. Kamra, E. Bertino, and R.V. Nehme, "Responding to Anomalous Database Requests," Secure Data Management, pp. 50-66, Springer, 2008.

[14] "Oracle Database Concepts 11g Release 1 (11.1)",download.oracle.com/docs/cd/B28359_01/server.111/b28318/datadict.htm, July 2009.

[15] R. Gennaro, T. Rabin, S. Jarecki, and H. Krawczyk, "Robust and Efficient Sharing of RSA Functions," J. Cryptology, vol. 20, no. 3, pp. 393-400, 2007.