RESEARCH ARTICLE OPEN ACCESS

A Survey on Log Mining: A Data Mining Approach for Intrusion Detection

Smita P. Bhapkar[1], Shubhangi S. Dhamane[2], Yogita S. Kandekar[3], Khushbu S. Lodha[4]

[1,2,3,4](Student of BE computer Chhatrapati College of Engineering,Nepti, Ahmednagar, SavitribaiPhule, Pune University)

--************************--

Abstract:

There are many approaches present in today's world to protect data as well as network. One of the way is an Intrusion Detection System (IDS) to make data more secure. Many researches are done in the field of intrusion detection, but the main concentration of these researches is on the networks and operating system. The unauthorized access may lead to break the integrity of the system as it may be in the form of execution of malicious transaction. E-commerce is one of the sectors suffers from million dollar losses only because of these unauthorized activities and malicious transactions. So, it is today's demand to detect malicious transactions and also to provide some protection. In this paper, we provided the detection system for intrusion detection in the e-commerce system and we are also trying to avoid different types of attack by applying different preventive measures. For detecting malicious transactions, we are going to use one of the data mining algorithm weighted data dependency rule minerfor our eCommerce database IDS. Which, extracts the read-write dependency rules to check whether the transactions are malicious or not. This system finds the malicious transactions as well as identify the transactions that performs read write operations without permission.

Keywords **— *Data mining , Database security , Intrusion detection***

--************************--

I. INTRODUCTION

Every organization is associated with more valuable information. Data is important and so it should be consistent and correct. Intrusion Detection System (IDS) is one of the ways to make data more secure. The Intrusion detection technique is a technology used to observe computer activities for finding security violations. When an intrusion takes place computer system is compromised. Intrusion detection is the process of identifying and responding to malicious activity in the various transactions on the internet.

In many systems, firewalls are used for intrusion detection, but they sometimes fail in detecting attacks that take place. To overcome this drawback of firewalls, different data mining techniques are used that handle intrusions occurring from many transactions in databases.

Different data mining techniques like classification, clustering and association rule can be used for monitoring and analyzing the network traffic and thereby detecting intrusions. [4]

In today's online world, we use the online eCommerce websites for many purposes. So, different E-commerce applications are becoming targets for criminal attacks. Malicious activities are identified from the huge amount of data sets which is generated widely for each transaction in eCommerce system such as logging data and user behavior. The data collected through logs and user behavior, can be a great advantage for intrusion detection to learn from the previous attacks [7]

When making purchases online, consumers should have a general sense of security. Even though there is no way to completely secure consumer information, businesses should take as many precautions as possible, while still allowing for usability. Technology is constantly changing, criminals are constantly finding new methods of attack, and it is the responsibility of users and administrators to use it in a way that is ethical and complies with all laws and regulations. Businesses need to ensure their e-commerce infrastructures are up-to-date with the latest updates and security necessities [5].

In recent years, data mining has lots of attention in the industry due to the wide availability of the huge volume of unstructured data. Data mining, commonly refers to the process of determining patterns or extracting useful models from large observed data. Recently, researchers have started to use data mining techniques in the system security and especially in intrusion detection systems [8].

Many researchers use different techniques of data mining for detection of intrusion. In this paper, for intrusion detection we are making use of the weighted data dependency rule mining. The read-write dependency rules are used to check whether the coming transaction is malicious or not. This approach mine the dependency among various attributes in a database. The transactions that do not follow these dependencies are called as malicious transactions. After detection of intrusion the appropriate action can be taken.

II. LITERATURE SURVEY

Different approaches have been proposed by researchers to address the problem of identifying malicious database transactions.

[1] Ms. Apashabi Chandkhan Pathan, Mrs. Madhuri A. Potey "Detection of malicious transaction in database using log mining approach "2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies. In this paper they use log mining approach for detecting anomalous transaction. They define some rules such as data item dependency rules, data sequence rules, domain dependency rules, and domain sequence rules. Database transaction that does not comply these rules are called as malicious transaction.

[2] Ashish Kamra, Elisa Bertino, "Guy mechanisms for Database Intrusion Detection and Response", Proceedings of the Second SIGMOD PhD Workshop on Innovative Database Research, ACM 2008. The main focus of this paper is to develop higher security solutions for

Protecting data reside in database management system (DBMS).The strategy used for detecting intrusion is developing an intrusion detection system within server which is capable of identifying anomalous user request to a DBMS. The idea behind this system is learning profiles of user and application interacting with the database and when the database request deviates from these profiles called as anomalous.

[3] Srivastava A, Sural S, and Majumdar A. K, "Database intrusion detection using weighted sequence mining", Journal of Computers, IEEE 2006.In this paper intrusion detection system (IDS) is used for detecting potential violations in database security. They propose an algorithm to find the dependency among various data items in a relational database system and the transaction which does not follow this dependency rule is termed as malicious transaction. As every database has some sensitive attribute for malicious modification. The algorithm novel weighted data dependency rule mining is used to detect modification of sensitive attribute. Sensitivity levels of attributes can be captured syntactically while data modeling by using a simple extension of the E-R diagram notations.

[4] Ms. Radhika S. Landge, Mr. Avinash P. Wadhe "Review of Various Intrusion Detection Techniques based on Data mining approach", International Journal of Engineering Research and Applications (IJERA). Recently data mining techniques are emerging trends in detection of intrusion. In this paper they give various data mining techniques for detecting intrusion such as classification, clustering, association rule mining. These techniques identify intrusion by analyzing network data.

[5] Syed (Shawon) M. Rahman, Ph.D. and Robert Lackey "E-COMMERCE SYSTEMS SECURITY FOR SMALL BUSINESSES" International Journal of Network Security & Its Applications (IJNSA) March 2013. In this paper they discuss how the attacks are carried out and how to secure the network from these attacks with minimum cost. They discuss various protection methods such as biometrics, smart cards, wireless security for

protecting eCommerce system for various types of attacks.

III. PROPOSED SYSTEM

A. Working flow of the system

The fig. is the working flow of the intrusion detection on data mining using log mining approach. The user can be an administrator, an auditor or a third party user (employee). The user will authenticate giving his legal identity. Depending on the type of user the access to the data will be granted. If the user is an administrator, the access to the original database is granted. If the user is an auditor or an employee, a copy of the database is accessed not the original one. All the modifications and updating by the auditor and employee are done only on the copy of the database.

For every change or access to the data, whether on original or on the copy, a default log file is created, which will have all the details of what changes were done, at what time and by whom. Only administrator has the access to the log files.

Using the Log Mining algorithm, the administrator can extract the specific log files, which will help to compare the original database and the modified copy of the database.

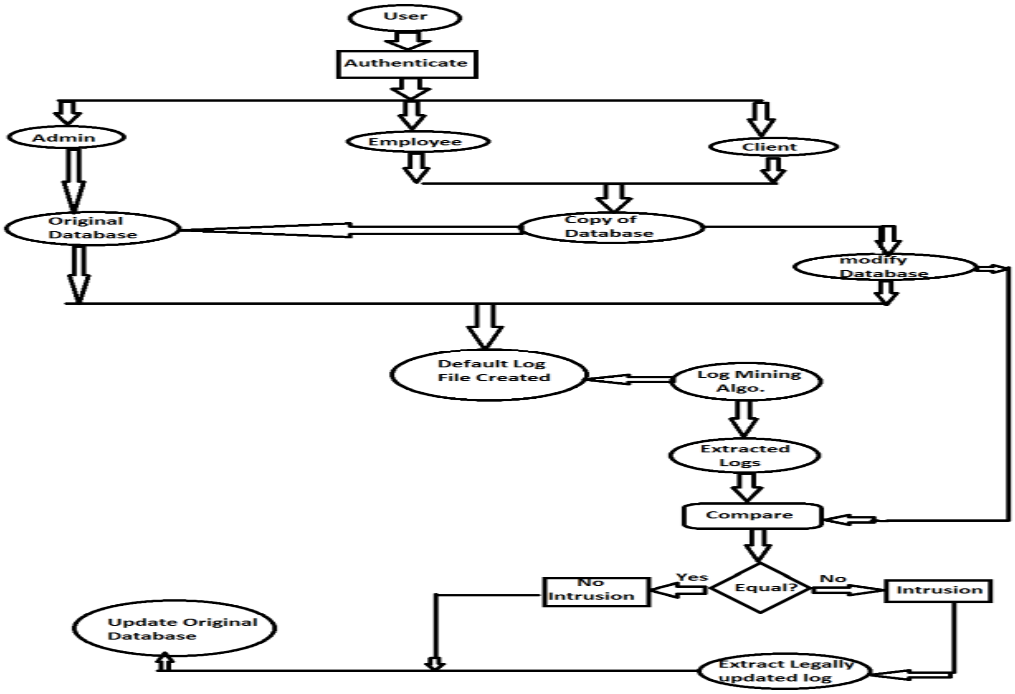

Fig. 1. Schematic representation - Working flow of IDS

If the changes made are legal or the same as expected, then there's no intrusion in the database. If the changes are made illegal, then intrusion is detected and action can be taken.

For detecting malicious transactions, the data mining algorithm weighted data dependency rule miner is used for our eCommerce database IDS. Which, extracts the read-write dependency rules to check whether the transactions are malicious or not. The transactions which will not follow these dependencies are considered to be a malicious transaction. After detection of intrusion the appropriate action can be taken.

IV. CONCLUSION

Malicious attacks in e-commerce websites can be easily identified using our proposed system. Our system provided the detection system for the intrusion detection in the e-commerce system. To detect malicious transactions, we are going to use data mining algorithm which uses read-write dependency rules for detecting malicious transactions. If any malicious transaction is detected by our IDS it will be rollback the tampered data with the original. We will use logs files to rollback the data.

This system can be used in various sectors such as Banking, Business, Medical systems for securing the valuable information.

V. REFERENCES

[1] Ms. Apashabi Chandkhan Pathan, Mrs. Madhuri A. Potey "Detection of malicious transaction in database using log mining approach "2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[2] Ashish Kamra, Elisa Bertino, "Guy mechanisms for database intrusion detection and response", Proceedings of the Second SIGMOD PhD Workshop on Innovative Database Research, ACM 2008.

[3] Srivastava A, Sural S, and Majumdar A. K, "Database intrusion detection using weighted sequence mining", Journal of Computers, IEEE 2006.

[4] Ms. Radhika S. Landge, Mr. Avinash P. Wadhe "Review of Various Intrusion Detection Techniques based on Data mining approach" International Journal of Engineering Research and Applications (IJERA) June 2013.

[5] Syed (Shawon) M. Rahman, Ph.D. and Robert Lackey "E-COMMERCE SYSTEMS SECURITY FOR SMALL BUSINESSES" International Journal of Network Security & Its Applications (IJNSA) March 2013.

[6] Ho, SweeYenn (George) "Intrusion Detection - Systems for today and tomorrow"
Version 1.2e, SANS Institute

[7] Daniel Massa& Raul Valverde, "A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications" Computer and Information Science; Vol. 7, No. 2; 2014Published by Canadian Center of Science and Education

[8] Abhinav Srivastava1, Shamik Sural, and A.K. Majumdar,"Weighted Intra-transactional Rule Mining for Database Intrusion Detection", 2006

[9] William A. R. Weiss, "An Introduction to Set Theory", October 2, 2008.

[10] Morten Blomhoj, Thomas Hojgaard Jensen, "Developing Mathematical Modelling Competence: Conceptual Clarification and Educational Planning", July 2003.

VI. BIOGRAPHIES

R. Tambe is currently working as Asst. Professor in Computer Engineering Department, Chhatrapati College of Engineering, Nepti, Ahmednagar and Maharashtra India. His research interest includes data mining, network security.

Bhapkar Smita is pursuing B.E Computer Engg. in SCSMCOE, Nepti, Ahmednagar. Her areas of research interests include Database Security and Data mining.

Dhamane Shubhangi is pursuing B.E Computer Engg. in SCSMCOE, Nepti, Ahmednagar. Her areas of research interests include Database Security and Data mining.

Kandekar Yogita is pursuing B.E Computer Engg. SCSMCOE, Nepti, Ahmednagar. Her areas of research interests include Database Security and Data mining.

Lodha Khushbu is pursuing B.E Computer Engg. in SCSMCOE, Nepti, Ahmednagar. Her areas of research interests include Database Security and Data mining.