International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

THE ANALYSIS OF USER BEHAVIOUR IN WEB APPLICATIONS AND NETWORK SECURITY

Miss.R.S.Maldhure
PG Department of Computer Science
SGBAU,Amravati, India
maldhurerohini@gmail.com

Dr . S. S. Sherekar
PG Department of Computer Science
SGBAU,Amravati , India
swatisherekar@gmail.com

Dr. V. M. Thakare
PG Department of Computer Science
SGBAU,Amravati, India
vilthakare@gmail.com

Abstract-

Nowadays, more and more online services, including web pages, as well as some client applications which are based on web services, security problems based on web applications become more serious. Most intrusion detection systems are based on every single request to find the cyber-attack instead of users' behaviors. In order to detect newly developed attacks, the system analyze web logs from web servers and define users' behaviors to divide them into normal and malicious ones. Anomaly detection method of user behavior is used to detect the internal attackers of database system. With using Discrete-time Markov Chains (DTMC), an anomaly detection system of user behavior is already proposed, which can detect the internal threats of database system. The experimental results show that this detection system can detect normal and abnormal user behavior precisely and effectively. These Previous research propose a novel method of user behavior analysis in semantic network. Using the weight value to analyze and record user behavior and then check user behavior record with the signatures which are generated by the Intrusion Detection System (IDS). Fuzzy expert system enables it to identify user behaviors and categorize suspicious behaviors with various levels of intensity. The method proposed in this paper is "Network Security Based On The Analysis Of user Behaviour For Web Applications". This proposed methodology gives an attention on Web usage mining to predict the behavior of web users based on web server log files.

Keywords— Intrusion Detection System, Fuzzy expert system, web logs, anomaly detection users' behaviors, security, network security, cyber security, SIEM, program for detecting the abnormal behavior of users.

INTRODUCTION

Nowadays, more and more online services, including web pages, as well as some client applications which are based on web services, are using HTTP protocol for development. Most intrusion detection systems are based on every single request to find the cyber-attack instead of users' behaviors, and these systems can only protect web application from known vulnerability rather than some zero-day attacks. A new way of detecting intrusion which is based on the model that analyze users' behaviors. This model is inspired by the malicious behavior detection for online rating system[1].A system for detecting the abnormal behavior of users is very important because it provides visibility and greater control for the network's security. This system allows the network administrator to observe real-time events both from the computer operating systems and from other security devices within the network[2]. The existing application layer DDoS attack detection method can achieve the purpose of detecting and defending the application layer DDoS attack to a certain extent. which takes the user's HTTP request sequence as the user behavior characteristic and uses DTMC to extract and analyze Then, by calculating the result of the threshold, the judgment is made[3]. The traditional security defense mechanisms

protect web service and prevent the on-line threats. This traditional system creates user profile for each user, build the knowledge base, and give the weight value. If the weight value is higher, the limit of authority will be low[4]. The internet banking is a new method of offering banking services. The availability of the internet to a large number of customers coupled with the expansion of electronic communications between various people and organizations has paved the way for commercial transactions and transformed customers consumption pattern[5]. Web Usage Mining becomes an important aspect in today's era because the quantity of data is continuously increasing .

The proposed paper deal with the web server logs which maintain the history of page request and Web log files are the files which contain complete information about the users browse activities on the web server, So this proposed paper gives an attention on Web usage mining to predict the behavior of web users based on web server log files.

II. BACKGROUND

As per the studies Analysis Of user Behaviour For User Applications different approaches have been develop for the Analysis Of user Behaviour in recent past years. Such approaches are:

A new way of detecting intrusion which is based on the model that analyze users' behaviors. This model is inspired by the malicious behavior detection for online rating system. The result shows that by using the feature of web resources to define users' behaviors, a higher accuracy rate and lower false alarm rate of intrusion detection can be obtained[1]. System for detecting the user behavior in a network is a tool for Security Information and Event Management (SIEM). This technology provides real-time analysis of security [2]. DDOS attack , one of the most severe threats existing in the internet, refers to using a puppet host to consume the computing resources of its target . Constructs an application layer DDoS attack detection system based on DTMC , which takes the user's HTTP request sequence as the user behavior characteristic and uses DTMC to extract and analyze[3].

The Web Service has been extended to the back-end database. This paper propose a novel method of user behavior analysis in semantic network. Use the weight value to analyze and record user behavior and then check user behavior record with the signatures which are generated by the Intrusion Detection System (IDS)[4]. An intelligent system that enables detecting the user's abnormal behavior in online banking. The system has been developed based on the fuzzy theory, This enables it to identify user behaviors and categorize suspicious behaviors with various levels of intensity[5].

This paper introduces analysis of five method for Analysis Of user Behaviour For User Applications i.e Anomaly Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs,Computer Networks Security Based on the Detection of User's Behavior, DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer, Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System, An Intelligent system for User Behavior detection in Internet Banking. The paper is organizes as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on analysis of user behaviour **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III. PREVIOUS WORK DONE

In research literature, many method for Analysis Of user Behaviour have been studied and improve the performance in terms effectiveness, software reliability, accuracy rate, lower false alarm rate.

Yang Gao et al. (2017) [1] have analyze web logs from web servers and define users' behaviors to divide them into normal and malicious ones. The result shows that by using the feature of web resources to define users' behaviors, a higher accuracy rate and lower false alarm rate of intrusion detection can be obtained.

Adrian Badea et al.(2015) [2] has proposed an system for detecting the user behavior in a network is a tool for Security Information and Event Management (SIEM). This technology provides real-time analysis of security alerts generated by applications and hardware networks**.**

Wang Andi et al. (2017) [3] has worked anomaly detection method of user behaviour is used to detect the internal attackers of database system. With using Discrete-time Markov Chains (DTMC), an anomaly detection system of user behavior is proposed, which can detect the internal threats of database system.

Yi-Tung F. Chan et al.(2009) [4] has present novel method of user behavior analysis in semantic network. Use the weight value to analyze and record user behavior and then check user behavior record with the signatures which are generated by the Intrusion Detection System (IDS).

Saeideh Alimolaei et al.(2015) [5] have proposed an intelligent system that enables detecting the user's abnormal behavior in online banking. Since the user's behavior is associated with uncertainty, the system has been developed based on the fuzzy theory, This enables it to identify user behaviors and categorize suspicious behaviors with various levels of intensity.

IV. EXISTING METHODOLOGIES

Many techniques for analysis of user behaviour have been implemented over the last several decades. There are different methodologies that are implemented for different detection of malicious user behaviour i.e Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs, Computer Networks Security Based on the Detection of User's Behavior, DDOS Attack Detection System based on Analysis of Users' Behaviors, Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System, Intelligent system for User Behavior detection in Internet Banking.

A) Anomaly Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs: Anomaly Detection of Malicious Users' Behaviors for Web Applications has proposed a new way of detecting intrusion which is based on the model that analyze users' behaviors. This model is inspired by the malicious behavior detection for online rating system. In order to detect newly developed attacks, Analyze web logs from web servers and define users' behaviors to divide them into normal and malicious ones. The result shows that by using the feature of web resources to define users' behaviors, a higher accuracy rate and lower false alarm rate of intrusion detection can be obtained [1].

To calculate its entropy which is to describe a user's behavior:

$$E_i = \sum_{j=1}^{L} - P_{ij}^{k} \log_2 P_{ij}^{k}$$

B) Computer Networks Security Based on the Detection of User's Behavior: Security Information and Event Management (SIEM) is a tool for detecting the user behavior in a network. It is a combination of two separate legacy products: Security Information Management (SIM) and Security Event Manager (SEM).This technology provides real-time analysis of security alerts generated by applications and by the network hardware

equipment. SIEM solutions can come as software, management services and are used to record data security and to generate reports for compliance purposes. SIEM is also an application for identity management and access. A main target of this product is to monitor and to help managing users and privileges of services and to provide records, analysis and incident responses [2].

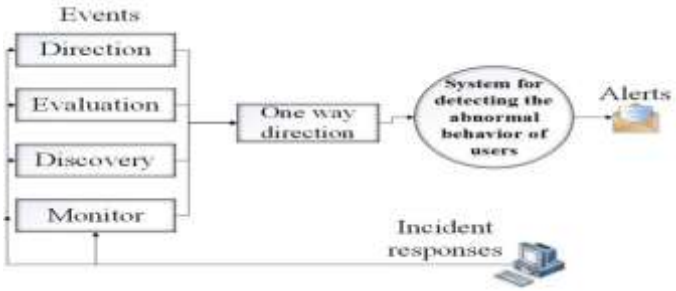

Fig. 1. Logical flow of the system for detecting the abnormal behavior of user

C) DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer: Discrete-time Markov Chains (DTMC), an anomaly detection system of user behavior is proposed, which can detect the internal threats of database system. Based on the theory of DDOS attack of the Web application layer, this paper chooses the request sequence of HTTP; and the time interval of adjacent HTTP request as the users' behavior characteristic to analyze while the server's log file records all users' access to the Web server. The experiments are used to test the feasibility of the detction system. The experimental results show that this detection system can detect normal and abnormal user behavior precisely and effectively. Two procedures are here to exist: training and testifying. (1) training: The system runs under normal conditions for a period of time, collects data during normal operation, and extracts users' characteristics behavior to set up a normal users' behavior pattern. (2) Testifying: The system runs in the actual environment, collects the behavior data of the current users and extracts the characteristics behavioral [3].

$$\text{detection rate} = \frac{\text{number of abnormal data detected}}{\text{total number of abnormal data}} \times 100\%$$

$$\text{Omission rate} = \frac{\text{number of abnormal data not detected}}{\text{total number of abnormal data}} \times 100\%$$

D) Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System: The traditional security defense mechanisms protect web service and prevent the on-line threats. In research, the author utilized the concept of the semantic network to propose ACID system. This system creates user profile for each user, build the knowledge base, and give the weight value. If the weight value is higher, the limit of authority will be lower. Moreover, user profile can compare with signature in order to filter each user. Furthermore, this proposed system can compared with previous work, the system can manage different user by using different criteria, reduce the misjudgment rate from IDS system, and record each user's behavior. The ACID does not only help the system administrator to maintain and protect the web service in order to prevent the intruders' attacking but also show the security information. it can not only successfully solve the Cross-Site Scripting (XSS) attack and SQL Injection attack but also understand user behavior [4].

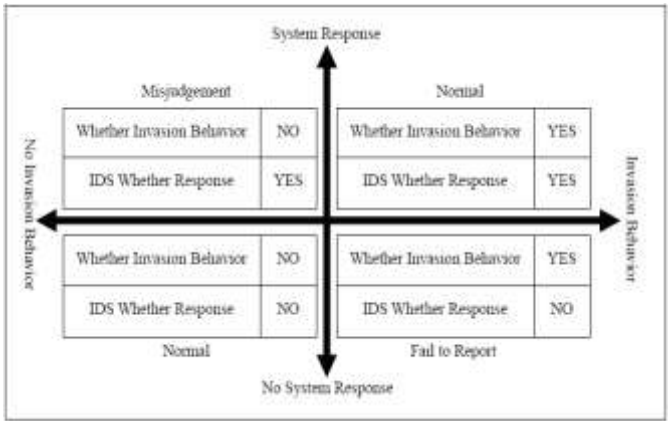

Figure 3: Schematic Diagram on Possible Detection Result

E) An Intelligent system for User Behavior detection in Internet Banking: The system has been developed based on the fuzzy theory, This enables it to identify user behaviors and categorize suspicious behaviors with various levels of intensity. The performance of the fuzzy expert system has been evaluated using an receiver operating characteristic curve, which provides the accuracy of 94%. Through the internet banking is a new method of offering banking services. The availability of the internet to a large number of customers coupled with the expansion of electronic communications between various people and organizations has paved the way for commercial transactions and transformed customers consumption pattern. Customers attitude toward the internet banking and their acceptance of this phenomenon is one concern of information technology management, especially the internet banking management[5].

ANALYSIS AND DISCUSSION

Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs uses the feature of web resources to define users' behaviors, a higher accuracy rate and lower false alarm rate of intrusion detection can be obtained [1]. Computer Networks Security Based on the Detection of User's Behavior uses Security Information and Event Management (SIEM) is a tool for detecting the user behavior in a network. This technology provides real-time analysis of security alerts generated by applications and hardware networks[2]. DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer shows that how DTMC model extract behavior features of a normal user and the detected user and make a comparison between them .This experimental results show that this detection system can detect normal and abnormal user behavior precisely and effectively. [3]. Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System shows enhanced IDS system which utilizes the concept of the semantic network to build the knowledge ontology. It can not only successfully solve the Cross-Site Scripting (XSS) attack and SQL Injection attack but also understand user behavior [4]. An Intelligent system for User Behavior detection in Internet Banking aimed at creating trust in the banking industry. Winning the trust of customers through activities such as the safe processing and transmission of highly confidential information could be a useful step toward preserving electronic customers [5].

Proposed Methods and Techniques	Characteristics	
	Advantages	*Disadvantages*
Anomaly Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs	This proposed method provide higher accuracy rate and lower false alarm rate. It provides data quality and data recovery.	In this proposed method use k-means algorithm such as the initialized center has effect on the final result and is sensitive to abnormal data.
Computer Networks Security Based on the Detection of User's Behavior	Network Security helps in protecting personal data of clients existing on network. This technology also provide long-term storage, analysis and reports for registered data, real-time monitoring.	The drawback of this method set up of a network security system can be a bit expensive. The software installed on some networks is difficult to work with.
DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer	A major advantage of using the proposed scheme this proposed detection system can detect normal and abnormal user behavior precisely and effectively.	The drawback of this proposed scheme have the problems of complex detection process.The proposed scheme has some limitations on large databases.
Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System	The proposed model is based ACID which does not only help the system administrator to maintain and protect the web service in order to prevent the intruders.	There is no guarantee that the user that gained initial authentication is still the same person.
An Intelligent system for User Behavior detection in Internet Banking	In this approach, This expert system is optimistic to be used for improving e-ban king services security and quality. It provides the trust management between data owners and the receivers.	This system is used to determine there was also the chance that the user make use of a less known browser and thus increased the error percentage.

TABLE 1: Comparison between different mobility schemes.

PROPOSED METHODOLOGY

Analysis Of user Behaviour For Web Applications is important and difficult task to analyse and discuss about various methods based on different parameters i.e. accuracy, false alarm rate, cyber security , flexibility, effectiveness, etc for different Analysis Of user Behaviour. There are still problems which trouble in this web application . New method for analysis of user behavior by using web usage mining called "Network Security Based On The Analysis Of user Behaviour For Web Applications" Web usage mining to predict the behavior of web users based on web server log files are more effective and more accurate method is propose here to overcome the problems of previous models. The proposed method gives an attention on Web usage mining to predict the behavior of web users based on web server log files. Users using web pages, a frequent access path's and frequent access pages, links are stored in web server log files. Depending upon the frequency of users visiting each page mining is performed. By finding the session of the user this paper can analyze the user behavior by the time spend on a particular page and based on the values contained in the log file, derives indicators about when, how, and by whom a web server is visited. Using frequent links, this proposed paper can predict the user behavior and identify are all the sites mostly viewed by users.

web usage mining consists of three phases as follow:

1) Data Preprocessing : In this phase, data will be transform into a format that is more easily and efficiently understand for user purposes. In this phase consists of three steps: data cleaning, user and session identification.

2) Pattern Discovery: In this phase, the result from previous phase will be used to find frequent user access pattern. In this phase will used data mining technique like association rule, classification, clustering, and sequential pattern technique to find useful information. The result that has been extracted can be represented in many ways such as graphs, chart, tables, etc

3) Pattern Analysis : Typically the results of pattern discovery phase is not in a form that suitable for analysis. Therefore, in this phase will develop a technique or tools that can help analysts understand the information that has been extracted.

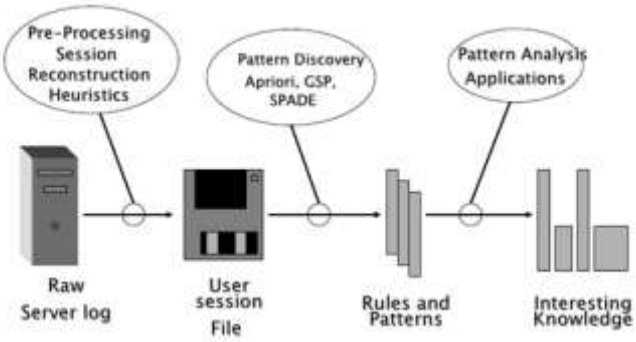

Fig 4: Phases of Web Usage Mining

ACKNOWLEDGMENT

OUTCOME AND POSSIBLE RESULT

In this way the proposed method is performed for the analysis of user behavior for web application using web usage mining . With the help of the of the web usage mining of proposed method calculate performance of system. The proposed method mainly focus on the the web log Mining technology in user behavior analysis which maintain the history of page requests, and builds the user interest model based on the user interest information, and finally draws the user's interest.

CONCLUSION

This paper focused on a the analysis of various schema i.e. Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs, Computer Networks Security Based on the Detection of User's Behavior, DDOS Attack Detection System based on Analysis of Users' Behaviors, Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System, Intelligent system for User Behavior detection in Internet Banking. But there are some problems in accuracy, false rate ,web log, So to improve this analysis of user behavior in web application using web usage mining is proposed here.

FUTURE SCOPE

From observations of the proposed method the future work will include conducting additional detection method to tackle common problems that affect the effectiveness of user behavior in web application. This paper analyzed some significant behaviors. With the development of malicious attack tools, the intrusion detection system also need to be improved.

REFERENCES

[1] Yang Gao, Yan Ma, Dandan Li "Anomaly Detection of Malicious Users' Behaviors for Web Applications Based on Web Logs", 2017 17th IEEE International Conference on Communication Technology, 2017.

[2] Adrian Badea1, Victor Croitoru2, Senior Member, IEEE, Daniel Gheorghică1 "Computer Networks Security Based on the Detection of User's Behavior",THE 9th INTERNATIONAL SYMPOSIUM ON ADVANCED TOPICS IN ELECTRICAL ENGINEERING, May 7-9, 2015.

[3]] Bi Meng1, Wang Andi , Xu Jian , Zhou Fucai, "DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer ", 2017 IEEE International Conference on Computational Science and Engineering (CSE) , 2017.

[4] Yi-Tung F. Chan, Charles A. Shoniregun, Galyna A. Akmayeva, Ali Al-Dahoud., "Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System", 2009 by the Institute of Electrical and Electronics Engineers, 2009.

[5] Saeideh Alimolaei, "An Intelligent system for User Behavior detection in Internet Banking", 2015 4th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2015.