IJIEMR Transactions, online available on 20th Oct 2021.

Link : https://ijiemr.org/downloads/Volume-10/Issue-10

Title: IIDPS based on Usage behaviour with TF-IDF

volume 10, Issue 10, Pages: 207-216

Paper Authors: **A. Ramaswami Reddy**

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IIDPS based on Usage behaviour with TF-IDF

A. Ramaswami Reddy
Professor, Computer Science Engineering, Malla Reddy Engineering College,
Maisammaguda, Hyderabad

Abstract —Presently, most computer systems use user IDs, login patterns and passwords as the login to authenticate the authorised users. But there might have chances that people may share their user IDs and passwords to their acquaintance. In organisations, many people share their login patterns with co-workers to assist or do co-tasking, thereby making the pattern as one of the weakest points for security of computer and data in it. In insider attackers, a valid user of a system who attack the system internally, are hard to be detected since most intrusion detection systems and firewalls, identify and isolate malicious behaviours launched from the outside world of the system only and therefore internal intrusions are overlooked. In addition, some studies claimed that analysing event logs, with which to accurately detect attacks, and attack patterns are the features of an attack. Therefore, in this paper, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks using Naive Bayes along with TF-IDF and some forensic techniques. The IIDPS creates users' personal profile to keep track of authorised users' behaviour patterns as their forensic features and determines whether a logged in useris the valid account holder or not by comparing his/her current system usage behaviours with the patterns collected in the account holder's personal profile. This paper, presents an intelligent learning approach,to identify the legality of a login user. The model usesNaive Bayes along with TF-IDFto increase the accuracy. The experimental results demonstrate that the IIDPS's user identification using Naive Bayes along with TF-IDF has accuracy higher than 97%, implying that it can detect any malicious behaviour launched towards system, hence protecting the system from insider attacks effectively and efficiently.

Keywords —Internal intruder, Naive Bayes, TF-IDF, Usage behaviour, Internal Intrusion Detection

I. INTRODUCTION

In the past years, computer systems have been widely employed to provide users with easier and more convenient lives. Today accessing information has become lot more easily than past. However, the security of the computer and security of data in it has become a task,when people exploit capabilities, data and processing power of computer systems, security has been one of the serious problems in the computer domain since attackers usually try to penetrate into the computer systems and behave maliciously, e.g., stealing critical data of a company or a person, making the computers out of work, inserting spyware to the system or even destroying the systems.

In general, among all well-known attacks such as pharming attack, SQL Injections, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack, insider attack is one of the most difficult ones to be detected because firewalls or other intrusion detection systems (IDSs) usually defend the system against outside attacks. Currently to authenticate users, most systems verify user ID and password as a login pattern. However, attackers may install Trojans to steal victims' login patterns or issue a large scale of trials with the assistance of a dictionary to acquire users' passwords like in dictionary attacks. Even they may take much time but the possibility of accessing to the user ID and password is high by using dictionary attacks. When successful, they may then get the access to log in to the system posing as a authorised user and access users' private files, sensitive data or modify to their favour or destroy system settings.

Fortunately, currently most of the host-based security systems and network-based Intrusion Detection Systems can discover a known intrusion in a real-time scenario. However, it is very difficult to identify who the attacker is because attack packets are often issued with forged IPs or other type of attacks, attackers may enter a system with valid login patterns.

To detect insider threats, the traditional detection systems primarily focus on the technical monitoring data derived from internal and network security audits and have been deployed to monitor and track insiders' computer and network activities. However, the majority of these approaches avert the occurrence ofmalicious insiders by policy violation checks and by anomaly detection based on the users' computer or network activities, neglecting the fact that insiders intrinsically have authorized access to organization assets and data at attack under normal behaviour profiles.

One of the main issues of internal intrusion detection is adversity of determining new attacks due to progressive nature of certainly new behaviour patterns. We need to deal with changing data in the presence of continuous data flow. Over period of time, the drastic changes on profiles may cause the recent instances to be classified incorrectly or lead the system not to recognize them at all. Therefore, the need to thoroughly update learnt profiles arises. Deviating from the normal activity or any policy violation is treated as a potential threat and typically reported to an administrator or centralized collection for further investigation and mitigation. To distinguish between the normal and abnormal user behaviour we identify user patterns and construct the user's initial behavioural normal/usual profile and the attacker profile. This profiles needs to be constantly updating as per the usage of the system, so that the behaviour patterns are up to date and can efficiently identify the potential threat and alert the admin.

In this paper, we propose a security system, named the Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviours launched toward a system. The IIDPS uses mining and forensic profiling techniques to mine log patterns defined as the longest log sequence that has repeatedly appeared several times in a user's log file for the user. The user's forensic features, defined as a log pattern frequently appearing in a user's submitted SC-sequences but rarely being used by other users, are retrieved from the user's computer usage history.

IIDPSmines log data of each action performed by user and their sequences, which a user habitually submits and follows respectively as the user's forensic features. When an unknown user logs in to a computer, the IIDPS starts monitoring the user's input and log sequence to detect whether he/she is issuing an attack by monitoring and verifying the users normal behaviour pattern those which are already collected in the user's personal profile with current generated log pattern.

The rest of this article is organized as follows. Section 2 introduces the related research. Section 3 describes the framework and details of collecting and creating user behaviour patterns and the IIDPS. Experimental results are shown in section 4. Section 5 concludes this paper and addresses our future work.

II. RELATED WORKS

In the field of information security, intrusion detection refers to the process of identifying unauthorized access to computer systems or electronic data. Various methods exist for detecting intrusions: manual inspection of a system, audit log processing, event log analysis, host-based intrusion detection, and network intrusion detection. Each method has advantages and disadvantages, either in the amount of human attention required to set up and maintain the system to detect the intrusion and the accuracy of incident detection.

Most of the intrusion detection methods focus on how to find malicious network behaviours. [3] One of the main issues of intrusion detection is adversity of determining new attacks due to progressive nature of network traffic. We need to deal with changing data in the presence of continuous data flow. Over a period of time, the drastic changes on profiles may cause the recent instances to be classified incorrectly or lead the system not to identify them at all. Therefore, the need to update learnt profiles arises. Moreover, characteristics of dynamic detection demand the update of the parameters based on the recent activities in the system. For this purpose, the system should be retrained with the recent traffic instances. [2] Machine learning (ML) based IDS can better detect new patterns or behaviours. Addition of natural language processing (NLP) can enhance the detection accuracy of these IDSs as NLP-based detection mechanisms do not rely on the attack techniques. Whenever, this module identifies a so far unseen attack, the pattern or origin of this malicious activity can be added to the database of known attacks. The main contribution of this paper is the development of an intrusion detection system that analyses natural language based network traffic using NLP techniques that detects anomalous, potentially malicious, traffic using an ensemble based machine learning scheme.

One of the technique broadly used is TF-IDF [5] our model uses Term Frequency Inverse Document Frequency (TF.IDF) to convert data types to an acceptable and efficient form for machine learning to achieve high detection performance [6] Frequency domain analysis has been found to be promising in detecting DDoS attack. Different literatures have employed the capability of the frequency based methods to analyse traffic patterns, and to discover abnormalities. Naive Bayes classifier which is fast and easy to implement, is used to classify attack and normal traffic and results are compared with a simple thresholding classifier.

These techniques and applications truly contribute to the network security. However, they cannot easily authenticate a remote-login users and detect specific types of intrusions, example - when an unauthorized user logs in to a system with a valid user ID and password. [10] We describe two feature representations of system call sequences that intrusion detection algorithms deal with. The first one is a contiguous subsequence with fixed length k from original input traces, and the second is bag of system calls, which is our approach. In our approach, we convert the input sequence to bag of system calls or bag of words. Thus, only the frequency of each system call is preserved for each input sequence. It will be shown that frequency information is effective enough to discriminate between normal sequences and abnormal sequences. [11] Anomaly detection systems are extensively used security tools to detect cyber-threats and attack activities in computer systems and networks. We discuss n-gram text categorization and focus our attention on a main contribution of method TF-IDF (Term frequency, inverse document frequency), which enhance the performance commonly term weighting schemes are used, where the weights reflect the importance of a word in a specific document of the considered collection. [12] To distinguish between the normal and abnormal user behaviour we identify user parameters and construct the user's initial behavioural normal/usual profile. This profile is not constant and may vary as per the usage of the system.

III. PROPOSED SYSTEM

In proposed system, a security system, named Internal Intrusion Detection and Protection System (IIDPS) is proposed, which detects malicious behaviours launched toward a system. The IIDPS uses mining and forensic profiling techniques by recording and analysing behavioural characteristics to mine log patterns defined as the log sequence that has repeatedly appeared several times in a user’s log file for the user. The user’s forensic features, defined as log patterns frequently appearing in a user’s submitted log sequences but rarely being used by other users, are retrieved from the user’s computer usage history.The IIDPS creates both users' personal profile to keep track of authorised users' usage habits and attacker behaviour patterns as their forensic features for the analysis of intrusion detection.

a. Creating profiles

To distinguish between the normal and abnormal user behaviour we identify user patterns and construct the user's initial behavioural normal/usual profile, these profiles will be dynamic in nature. Further to keep track of users’ usage habits, the authorised user logs and user submitted log sequences are monitored and stored.

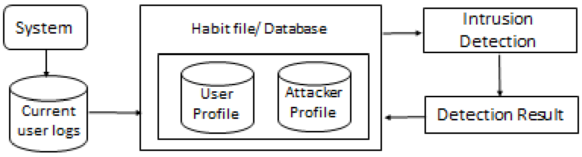

Fig 1: Framework of Creating and updating profiles

To ensure the efficiency of the attack detection these profiles keep on updating, because one of the main issues of intrusion detection is adversity of determining new attacks due to progressive nature of certainly new behaviour patterns. We need to deal with changing data in the presence of continuous data flow. With the passing time, there could be drastic changes on profiles that may cause the recent instances to be classified incorrectly or even lead the system not to recognize them at all. Therefore, the need to constantly updating learnt profiles arises.

Once current user submitted the log sequence, those would be subjected to intrusion detection by comparing current user computer usage behaviours with the patterns collected in the account holder's personal profileand with existing attacker profiles.

If the current log sequences are classified as user pattern then this log sequence is added as new user sequence in the account holder user profile. Else if, the current log sequences are classified as attacker pattern then IIDPS gives the admin chance to verify, if those potential attack patterns are being submitted by the actual account holder or those are unknown to him (i.e., submitted by unauthorised user). If admin says, those are generated and submitted by him – the new user log pattern is added to user profile else if done by unauthorised user – the new log pattern is added to attacker profile. In this manner both the user and attacker profiles keeps on updating and used as forensic features for the further analysis of intrusion detection and ensures the efficiency of the attack detection.

b. Intrusion detection

TF-IDF

Generally, a huge amount of logs are generated during the execution of a job, i.e., a task or process. Therefore, it is hard for a system to monitor and analyse all logs at the same time for intrusion detection process. As a result, we need to know which logs are more precise. To find out what logs are typical ones generated as result of the execution of an task, the statistic model of term frequency-inverse document frequency (TF-IDF) is used to analyse the importance of logs collected in a user log file.

In the information retrieval domain, the relationship between a term and a document is similar to that between anlog$t_i$and the action that caused t_i, e.g., j, which generates t_i. The term frequency (TF) employed to measure the weight of the frequency of an log produced by j is defined as

$$\mathrm{TF}^{i,j} = \frac{n_{i,j}}{\sum_{k=1}^{k=h} n_{k,j}}$$

Where$n_{i,j}$is the number of times that $t_i$is issued during the execution of j, h is the number of different log generated when j is executed, and the denominator $\sum_{k=1}^{k=h} n_{k,j}$ sums up the numbers of times that all these logs are launched. The inverse document frequency (IDF), the measure of the importance of $t_i$among all other logs generated, is defined as

$$\mathrm{IDF}^{i = \log \frac{|D|}{|\{j \, : \, t_i \, \in \, d_j\}|}}$$

Where $|D|$, is the cardinality of D. Here D is the total number of commands in concerned corpus and $\{j \, : t_i \in d_j\}$ is the set of shell commands d_j, in which each member generates $t_i$during its execution. In other words, numerator,|D| is total number of documents in the corpus and the denominator $|\{j \, : \, t_i \in d_j\}|$ number of documents where the term appears.The TF-IDF weight of $t_i$generated by j is defined as

$$(\text{TF-IDF})_{i,j} = \text{TF}_{i,j} \times \text{IDF}_i.$$

In fact, the TF-IDF weight as one of the feature weighting methods in data mining and information retrieval domains increases proportionally to the number of times alog appears in a user log file, and it can indeed show the importance of a certain log. And by using TF-IDF, each log gets a specific TF-IDF weight, where each log can be seen as a vector, making them and those weights indicates the relevance of a specific log in corpus of many.

Naive Bayes Classifier

The naïve Bayes classifier operates on a strong independence assumption, it is assumed that all features are strong (naive) independent from each other. Because naive Bayes classification can be implemented easily without any complicated iterative parameters, it is useful for very large datasets. Bayes theorem provides a way of calculating the posterior probability, P(c|x) (Posterior probability), from P(c), P(x), and P(x|c) (Likelihood). Naive Bayes classifier assumes that the effect of the value of a feature (x) on a given class (c) is totally independent of the values of other features. This assumption made is called class conditional independence.

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)}$$

$$P(c|x) = P(c) \prod_i P(x_i|c)$$

By considering the naive Bayes equation, the likelihood probability(Π_iP(x_i |c)) could be used as a score of class C. This score can be used as a verdict to classify attack from normal traffic.

System frame work:

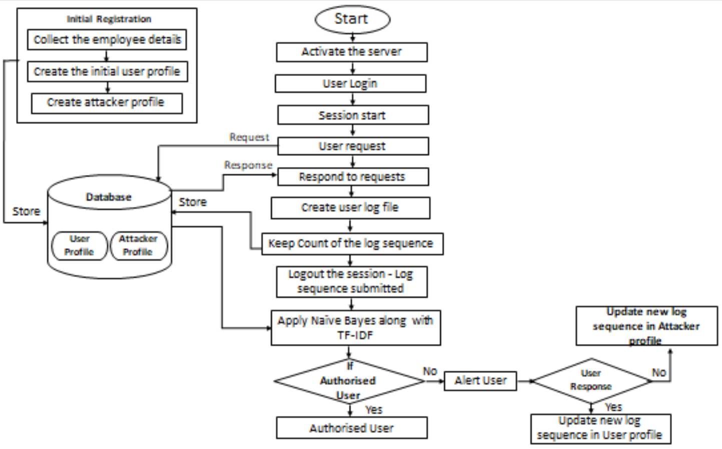

Fig 2: Internal Intrusion Detection and Protection System (IIDPS)

IV. RESULTS

In this paper, an IIDPS is developed to detect insider attacks, by using mining and forensic techniques. The experimental results shows that the IIDPS can effectively resist internal intrusions. The experimental results on proposed system demonstrate that the average detection accuracy is higher than 97%, for the approach using Naïve Bayes along with TF-IDF, confirming that data mining and forensic techniques used for intrusion detection provide effective attack detection. Generally, users' forensic features retrieved from their basic operations are helpful in detecting the users' malicious behaviours and tell us who the possible attackers would be. This also detect malicious behaviours for systems employing GUI interfaces.

V. CONCLUSION

In this paper, we have proposed an approach that employs mining and forensic techniques to identify the representative log patterns for a use, then a user's profile is established. The time that a habitual log pattern appears in the user's log file is counted, the log are given TF-IDF weight this, indicating the relevance of certain log. By identifying a user's logs patterns as his/her computer usage habits from the user's current input logs, the IIDPS detects suspected attackers. The experimental results demonstrate that the average detection accuracy is higher than 97%, indicating that the IIDPS can assist system administrators to point out an internal intruder or an attacker in a closed environment. The further study can be done by improving IIDPS's performance and investigating third-party shell commands. Further studies can also study on integrating it to cloud environment and external computing grid hence maintaining the security across the organisation covering wider area.

REFERENCES

1. F. Leu, K. Tsai, Y. Hsiao and C. Yang, "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques," in *IEEE Systems Journal*, vol. 11, no. 2, pp. 427-438, June 2017, doi: 10.1109/JSYST.2015.2418434.

2. Leu, Fang-Yie& Hu, Kai-Wei & Jiang, Fuu-Cheng. (2007). Intrusion Detection and Identification System Using Data Mining and Forensic Techniques. 137-152. 10.1007/978-3-540-75651-4_10.

3. F. Gumus, C. O. Sakar, Z. Erdem and O. Kursun, "Online Naive Bayes classification for network intrusion detection," *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, 2014, pp. 670-674, doi: 10.1109/ASONAM.2014.6921657.

4. S. Das, M. Ashrafuzzaman, F. T. Sheldon and S. Shiva, "Network Intrusion Detection using Natural Language Processing and Ensemble Machine Learning," *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2020, pp. 829-835, doi: 10.1109/SSCI47803.2020.9308268.

5. AWADH, Khaldoon& AKBAŞ, Ayhan. (2020). Intrusion Detection Model Based on TF.IDF and C4.5 Algorithms. Journal of Polytechnic. 10.2339/politeknik.693221

6. Anarim, Emin&Fouladi, Ramin&Kayatas, Cemil. (2016). Frequency Based DDoS Attack Detection Approach Using Naive Bayes Classification. 10.1109/TSP.2016.7760838

7. G. Yang, L. Cai, A. Yu, J. Ma, D. Meng and Y. Wu, "Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model," *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*, 2018, pp. 9-16, doi: 10.1109/BigDataService.2018.00011.

8. M. D. Bhat, P. A. Pandita, H. A. Chheda and J. Ramteke, "Determining User Behaviour Using System Calls To Prevent Internal Intrusions," 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020, pp. 40-45, doi: 10.1109/ICCCA49541.2020.9250880. 2020

9. Cao, Van Loi& Hoang, Van & Nguyen, Uy. (2015). A scheme for building a dataset for intrusion detection systems. 280-284. 10.1109/WICT.2013.7113149

10. Kang, D. K., Fuller, D., &Honavar, V. (2005). Learning classifiers for misuse detection using a bag of system calls representation. *Lecture Notes in Computer Science*, *3495*, 511-516. https://doi.org/10.1007/11427995_51

11. Kakavand, M., Mustapha, N., Mustapha, A., & Abdullah, M.T. (2015). A Text Mining-Based Anomaly Detection Model in Network Security. *Global journal of computer science and technology, 14*.

12. Z. S. Malek, B. Trivedi and A. Shah, "User behavior Pattern -Signature based Intrusion Detection," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 549-552, doi: 10.1109/WorldS450073.2020.9210368.