Survey Paper On "Internal Intrusion Detection and Protection by Self-Monitoring via Forensic Techniques and help of Data Mining"

Prof. Dr.Taware.G.G[1], Prof. Shah.S.N[2], Bhandwalkar Shreyash Sunil[3], Ghadge Vaishnavi Balasaheb[4] ,
Papal Komal Maruti[5]
[1,2]Asst. Prof. of Department of Computer Engineering
[3,4,5] PG Students
Sharadchandra Pawar College of Engineering and Technology, Someshwarnagar, Pune

Abstract— Today, the global internet user base numbers in the billions. Intrusion detection technology could be new. a generation of security technologies that monitors the system to prevent harmful activities. A neighbourhood procedure grid is used by the IDPS to monitor the actions of malevolent users over time. The Intrusion Detection and Protection System at call level, which creates user profiles to track usage actions, is the security system that the system recommends during this project due to the rhetorical alternatives. Using forensic methods and intrusion detection systems, the suggested work is assessed. An overview of the literature on intrusion detection systems (IDS) and internal intrusion detection systems (IIDS). They function in real time using various algorithms for rhetoric and data processing. Methods of data processing are expected for cyber analytics intrusion detection. This research led to the construction of the Internal Intrusion Detection System (IIDS), which uses preset algorithms or techniques to discern between unauthorized user activity and network attacks.

Keywords: Intrusion System, Networking, Internal attacks, malicious activity, System calls.

I. INTRODUCTION

In the last few decades, portable computer systems have been used extensively to provide users with more easy and straightforward access to their life. But as we start to capitalize on the powerful features and methodological strength of portable computer systems, security has become one of the most prominent problems with the field. This is because attackers frequently try to get access to portable computer systems and carry out malicious activities, like stealing a company, making labor-intensive processes obsolete, or even completely eliminating them. The business executive attack is generally the hardest to detect due to firewalls and other security measures out of all the well-known assaults like spear-phishing, eavesdropping, distributed denial-of-service (DDoS). Intrusion detection systems (IDSs) often provide defense against outside threats. Most systems currently employ the user ID and password as a pattern for login verification. However, hackers may install Trojan horses to obtain victims' login information or use a dictionary to generate an excessive number of password trials in an attempt to obtain as many as possible. Once If they are successful, they will then have access to users' personal files, be able to modify or erase system preferences, and be able to log in. By coincidence, the bulk of host-based security solutions currently in use combine an acknowledged incursion in a basic manner with degreed network-based intrusion detection systems. However, The United International Organization is quite difficult to identify due of the assault packages that are typically supplied. When using strong IPs, the attacker is A system might be accessed by an attacker who knew the correct login pattern. check the password and user ID as a login pattern. However, hackers may install Trojan horses to obtain victims' login information or use a dictionary to generate an excessive number of password trials in an attempt to obtain as many as possible. Once If they are successful, they will then have access to users' private files, have the ability to add or alter system settings, and be able to log in. By coincidence, the majority of host-based security solutions in use today link an acknowledged incursion in a basic manner with degreed network-based intrusion detection systems. However, it can be challenging to identify a United Nations entity. An attacker with a valid login pattern could get access to a system due to assault packets, which are typically supplied with reliable IPs. Identification, preservation, recovery, evaluation, and provision of facts and views on information obtained for a security event are the objectives of computer forensics science. It treats computer networks as though they were crime scenes. It looks at the activities.

II. METHODOLOGY

The IIDPS frame is introduced at the start of this section. function as well as a thorough explanation of every IIDPS component. Through analysis of the corresponding SCs, it can ascertain a user's forensic traits and raise the accuracy of attack identification. It can transfer the IIDPS to a parallel system in order to further lower its detection reaction time. It effectively thwarts insider threats. The IIDPS can prevent an assault on the protected system by determining the detrimental behaviors they cause. The IIDPS is made up of a local computational grid, three repositories including user log files, user profiles, and an attacker profile, a mining server, a detection server, a SC monitor, and a filter. In the protected system, the SC monitor and filter functions as a loadable module embedded in the system kernel under consideration. It collects the SCs submitted to the kernel and stores them in the format (uid,pid,SC), where uid, pid, and SC stand for the user ID, process ID, and SC c, respectively, that the underlying user submitted, or c SCs. The user's log file, which is a file that contains the order in which the user submitted their SCs, also keeps the inputs the user makes. The mining server looks through the log data using data mining techniques to find patterns and behaviors in the user's computer activity. The person's user profile then contains documentation of these. The detection server compares user behavior patterns with the SC-patterns collected in the attacker profile—also known as attack patterns—and those in user profiles to identify harmful behaviors and the attacker in real time. The detection server alerts the SC monitor and filter to any incursion, at which time the user is kicked out of the secured system. The goal is to prevent him/her from continuously attacking the system. Enhancing the IIDPS's online mining and detection capabilities; both the mining and the detection servers are run on local computers grid. The IIDPS compares the similarity scores of the user's current inputs, or SCs, with the behavior patterns that are documented in the user profiles of different users to identify the identity of the underlying user when a user logs in to the system using someone else's login pattern. The SCs collected in the class-limited-SC list are those that aren't permitted to be used by specific user classes or groups in the underlying system, and they are a crucial component of the SC monitor and filter in the IIDPS; For instance, a secretary isn't permitted to turn in some privileged SCs. Consequently, no secretaries will be permitted to use the instructions that generate these SCs.

III. LITERATURE SURVEY

1) An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

Author: Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao- Tung Yang

Description**:** Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. How- ever, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system inter- nally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only.

2) A System Architecture for the Detection of Insider Attacks in Big Data Systems.

Author: Santosh Aditham Nagarajan Ranganathan

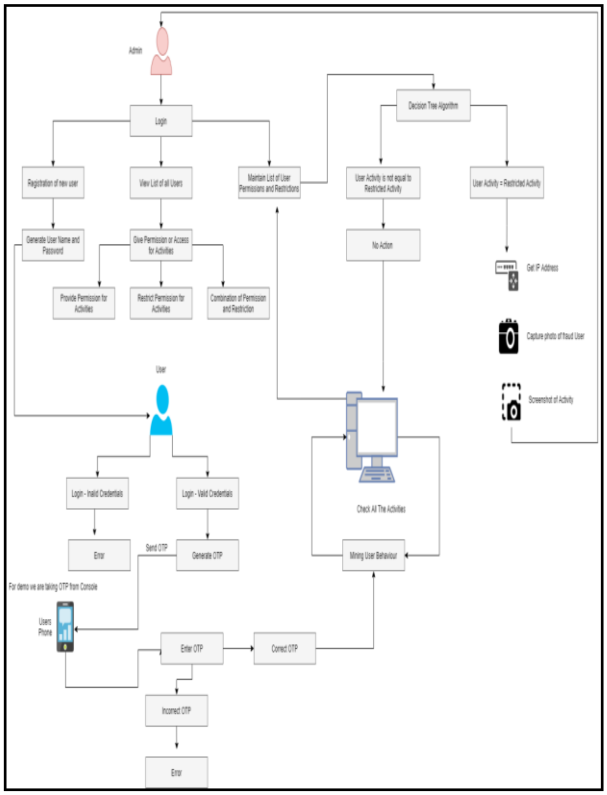
Description: In big data systems, the infrastructure is such that large amounts of data are hosted away from the users. In such a system information security is considered as a major challenge. From a customer perspective, one of the big risks in adopting big data systems is in trusting the provider who designs and owns the infrastructure from accessing user data. Yet there does not exist much in the literature on detection of insider attacks.

3) Detecting Collaborative Insider Attacks in Information Systems.

Author: Khanh Viet, Brajendra Panda Yi Hu

Description: The overall goals of information security are to ensure the confidentiality, integrity, and availability of the data in the systems. In addition to the common outsider attacks, insider attacks are often inadequately checked by the security mechanisms. This paper addresses the problem of collaborative insider attacks where two or more insiders work together to compromise critical data in the information systems. It first discusses the relations among the system components and the illegal information flow diagram.

IV. SYSTEM ARCHITECTURE


Admin
Login
Registration of new user
View List of all Users
Maintain List of User Permissions and Restrictions
Decision Tree Algorithm
User Activity is not equal to Restricted Activity
User Activity = Restricted Activity
Generate User Name and Password
Give Permission or Access for Activities
No Action
Get IP Address
Provide Permission for Activities
Restrict Permission for Activities
Combination of Permission and Restriction
Capture photo of fraud User
User
Screenshot of Activity
Login - Invalid Credentials
Login - Valid Credentials
Check All The Activities
Error
Send OTP
Generate OTP
Mining User Behaviour
For demo we are taking OTP from Console
Users Phone
Enter OTP
Correct OTP
Incorrect OTP
Error

V. CONCLUSION

This survey shows the importance of protecting systems from threats that come from within, not just from outside attacks. Most current security systems focus on stopping external threats, leaving insider attacks less protected. The Internal Intrusion Detection and Protection System (IIDPS) helps close this gap by combining forensic and data analysis to monitor user behavior in real time. By tracking unusual activities, IIDPS quickly detects and prevents harmful actions by insiders. This system offers a faster response to insider threats, making systems safer. Future improvements can help make detection even more accurate and effective for different types of systems.

REFERENCE

[1] A Self-Attention-Based Deep Convolutional Neural Networks for IIoT Networks Intrusion Detection.

[2] DTITD: An Intelligent Insider Threat Detection Framework Based on Digital Twin and Self-Attention Based Deep Learning Models.

[3] Hunt for Unseen Intrusion: Multi-Head Self-Attention Neural Detector.

[4] Network Intrusion Detection Method Based on CNN-BiLSTM-Attention Model.

[5] S. Li, G. Chai, Y. Wang, G. Zhou, Z. Li, D. Yu, and R. Gao, "CRSF: An intrusion detection framework for industrial Internet of Things based on pretrained CNN2D-RNN and SVM," IEEE Access, vol. 11, pp. 92041–92054.

[6] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial Internet-of-Things based on reconstructed graph neural networks," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2894–2905.

[7] M.Mohy-eddine, A.Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," J. Comput. Virol. Hacking Technology.

[8] M.Nuaimi,L.C.Fourati, and B.B.Hamed,"Intelligent approaches toward intrusion detection systems for industrial Internet of Things: A systematic comprehensive review," J. Netw. Comput. Appl.

[9] M. Tanveer and S. Shabala, "Entangling the interaction between essential and nonessential nutrients: Implications for global food security," in Plant Nutrition and Food Security in the Era of Climate Change. Amsterdam, The Netherlands: Elsevier

[10] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," Internet Things.