International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

"Internal Intrusion Detection System Using Machine Learning"

Prof.Vaibhav Dhage[1] , Prof. Minal Chaudhari[2] , Shinde Nikhil Sunil[3],
Khopade Nagesh Bapurao[4] , Mankar Gitesh Gangaram[5],
[1,2] Asst. Prof. of Department of Computer Engineering, & [3,4,5] PG Students
Indala College Of Engineering, Bapsai , Kalyan .

Abstract*—With billions of users connected to the internet today, ensuring cybersecurity has become increasingly critical. Intrusion Detection and Protection Systems (IDPS) represent a new wave of security solutions designed to monitor and respond to harmful activities within a network. This research focuses on a call-level Intrusion Detection and Protection System that employs neighborhood-based procedural grids to observe and analyze user behavior over time, particularly identifying patterns associated with malicious intent. The system builds user profiles to detect deviations from typical usage, enhancing the ability to detect internal threats. The proposed approach is evaluated using forensic techniques and established intrusion detection methodologies. This paper also provides a comprehensive review of existing literature on both general Intrusion Detection Systems (IDS) and Internal Intrusion Detection Systems (IIDS), which utilize real-time data processing and algorithmic analysis to detect threats. Emphasizing the role of cyber analytics, the research presents the development of an IIDS that leverages predefined algorithms to effectively differentiate between legitimate user activity and potential security breaches.

Keywords: Intrusion Detection, Cybersecurity, Internal Threats, Malicious Behavior, System Call Monitoring.

I. INTRODUCTION

In recent decades, the widespread use of portable computer systems has provided users with enhanced convenience and seamless access to digital resources. However, as the reliance on these systems grows, so do concerns about their security. Cyber attackers increasingly target portable systems to carry out malicious actions such as data theft, disrupting operations, or rendering entire systems inoperable. Among various cyberattacks—like spear phishing, eavesdropping, and distributed denial-of-service (DDoS) attacks—the so-called "insider" or business executive attacks are often the hardest to detect, especially when perimeter defenses like firewalls are in place.

Intrusion Detection Systems (IDS) are commonly used to protect against external threats. These systems typically rely on user credentials, such as a username and password, for access control. However, attackers may deploy Trojan horses to capture login credentials or employ dictionary attacks to guess passwords by generating numerous combinations. If successful, these intrusions can lead to unauthorized access, allowing the attacker to read or manipulate personal data, change system settings, or even take full control of a device.

Many current host-based security systems pair basic intrusion detection mechanisms with network-based IDS. However, detecting sophisticated attacks—especially those leveraging seemingly legitimate login credentials and reliable IP addresses—remains a significant challenge. Attackers who acquire valid credentials can bypass traditional security measures and gain unauthorized access, making these threats harder to trace and neutralize.

Computer forensics plays a critical role in identifying, preserving, analyzing, and interpreting data related to security incidents. It treats digital environments as crime scenes, carefully investigating actions taken within the system. By applying forensic techniques alongside robust intrusion detection mechanisms, it becomes possible to strengthen system defenses and respond more effectively to emerging threats.

II. METHODOLOGY

The IIDPS framework is particularly effective in identifying and mitigating insider threats. It proactively blocks attacks by recognizing suspicious behaviors that could potentially harm the protected system. The core components of the IIDPS include:

- A local computational grid
- Three main data repositories:
  - User log files
  - User profiles
  - Attacker profiles
- A mining server
- A detection server
- A system call monitor
- A filter module

In the secured environment, the SC monitor and filter are embedded into the operating system kernel as loadable modules.

These logs are then analyzed by the mining server, which employs data mining techniques to extract patterns and behavioral trends associated with each user. The extracted information is stored in the corresponding user profile.

The detection server plays a crucial role in identifying intrusions. It compares the real-time behavior of users (based on SC patterns) against two sources: user profiles and known attacker profiles. When abnormal or unauthorized activity is detected, the detection server triggers an alert and communicates with the SC monitor and filter to immediately block the user from continuing interaction with the system, preventing further harm.

To support continuous and real-time detection, both the mining and detection servers operate on a local grid of computers. This distributed design enhances the IIDPS's ability to perform real-time analysis and detection without affecting the overall performance of the system.

Moreover, the IIDPS includes a feature that identifies users attempting to log in with credentials that do not match their usual behavioral profile. It does so by comparing the incoming SC patterns with existing user profiles. If discrepancies arise, the system flags the session as potentially compromised.

The SC monitor and filter also enforce class-based restrictions by referencing a *class-limited system call list*. This list defines which system calls are restricted based on user roles. For example, a user classified as a secretary may not be allowed to execute privileged system calls intended only for administrators. This enforcement helps prevent users from performing unauthorized actions, even if they manage to gain access to elevated credentials.

In summary, the methodology of IIDPS integrates system call monitoring, user behavior analysis, and real-time pattern comparison to effectively detect and prevent both external and internal security threats.

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

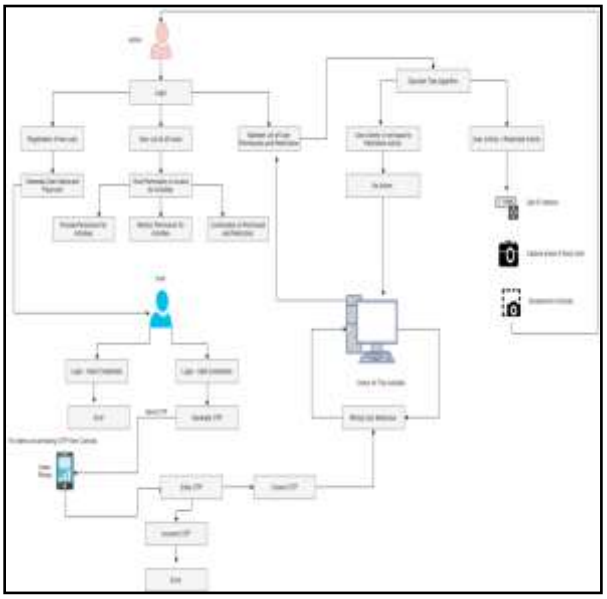
Description: In big data systems, the infrastructure is such that large amounts of data are hosted away from the users. . From a customer perspective, one of the big risks in adopting big data systems is in trusting the provider who designs and owns the infrastructure from accessing user data

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.

IV. SYSTEM ARCHITECTURE



V. RESULT

VII .CONCLUSION

This project highlights the critical need to safeguard systems against internal threats, which are often overlooked in favor of defending against external attacks. Traditional security measures tend to prioritize external intrusion, leaving systems vulnerable to malicious activities from authorized users. The Internal Intrusion Detection and Protection System (IIDPS) addresses this vulnerability by integrating forensic analysis with real-time behavioral monitoring to detect and respond to insider threats effectively. By continuously analyzing user activity, IIDPS can swiftly identify and block suspicious behavior, offering an enhanced level of system security. Its rapid response capabilities significantly reduce the risk posed by insiders. Looking ahead, further advancements can enhance the precision and adaptability of the system, making it more effective across a broader range of computing environments.

VIII. REFERENCES

[1] DTITD: An Intelligent Insider Threat Detection Framework Based on Digital Twin and Self-Attention Based Deep Learning Models.
[2] Hunt for Unseen Intrusion: Multi-Head Self-Attention Neural Detector.
[3] Network Intrusion Detection Method Based on CNN-BiLSTM-Attention Model.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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
[9] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," Internet Things.