WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

INTRANET ATTACKS DETECTION BASED ON BEHAVIOUR BY MACHINE LEARNING

B Meenakshi [1] , H Lasya [2] , B Hanumanth [3]

[2-3] Depa,tment of information Technology, Mahatma Gandhi Institute of Technology, Hyderabad-7, India.
bmeenakshi_it@mgit.ac.in[1],
hlasya_it211230@mgit.ac.in[2],
bhanumanth_it2112l f@mgit.ac.in[3]

ABSTRACT :

Thereabn of cybersecurity is becoming increasingly challenging for the detection of intranet attacks since malicious behaviors change with time. This paper attempts to present a sophisticated method to detect behavior-based intranet attacks by the use of machine learning techniques. The proposed method uses the machine learning algorithms so that intranet attacks based on their behavior can be easily identified and thus mitigated effectively. Through traffic netwoix analysis and bg system analysis, the model learned what is normal or anomalous, lt is for such proactive threat detection and response mechanisms, enabling it The proposed method promises a rich opportunity to augment the security of in tranet environments with a real-time capacity for detection capabilities and adaptive mechanisms for defense. Empirical evaluations and comparative analyses prove the effectiveness of the proposed framework in augmenting the existing cybersecurity frameworks to fortify the intranet against emerging threats

Keywords: Cybersecurity, Machine Learning, Intranet Attacks, Behavioural-based Detection, Anomaly Detection.

1. INTRODUCTION :

Intranet enviromnents are an essential component of modern organizations, enabling secure communication, seamless collaboration, and efficient resource sharing among empbyees. However, as these netwoixs become more interconnected and handle increasingly sensitive data, they are being targeted by sophisticated cyber threats that exploit internal access, mimic legitimate behaviors, and subtly manipulate system operations to evade detection. Unlike traditional cybersecurity threats that originate externally, intranet attacks often leverage insider access or compromised credentials, making them particularly difficult to detect with conventional security mechanisms. Traditional intrusion detection systems (IDS) and rule-based security tool more advanced techniques to infiltrate networks, organizations must adopt proactive and intelligent security solutions to safeguard their intranet environments. This paper proposes a machine learning-based approach to detecting intranet at1acks by analyzing behavioral patterns in network traffic and system log;, offering a dynamic and adaptive alternative to traditional security measures.

The proposed model is designed to identify deviations from normal activity by continuous1y monitoring user behaviors, system interactions, and network traffic patterns. Machine learning algorithms, particularly those based on anomaly detection and behavioral analytics, provide a powerful mechanism for detecting unauthorized access, malicious intent, or subtle alterations to system operations that may indicate a security breach. Unlike signature-based systems that require prior knowledge of attack patterns, this approach learns from historical data and real-time activity, allowing it to detect emerging threats before they escalate into full-scale cyber incidents. One of the major advan1ages of this method is its ability to recognize previously unknown attack vectors by analyzing hidden patterns in large datasets. As organizations generate vast amounts ofnetwoix and system log data, machine learning techniques can effectively sift througp this infonnation, identifying anomalies that traditional security tools might overlook. Furthermore, empirical evaluation of the system demonstrates higp accuracy in detecting intranet anomalies while minimizing false positives, ensuring that security teams receive meaningful alerts without being overwhelmed by irrelevant warnings.

A key challenge in cybersecurity is the trade-off between detection accuracy and false positive rates. Many traditional IDS and rule-based mechanisms produce excessive false alarms, leading to alert fatig.ie among security analysts. The machine learning-based approach described in this paper addresses this issue by refining detection models over time, improving their ability to distinguish between legitimate and malicious activities. By integrating supervised and unsupervised learning techniques, the system can detect both known and unknown threats without relying on manually curated rule sets. Additionally, real-time monitoring ensures that potential security incidents are identified and mitigated promptly, reducing the risk of prolonged exposure to malicious actors. Adaptive defense mechanisms, such as automated response systems and threat intelligence integration, further enhance the system's effectiveness in countering cyber threats.

Another sih'Tlificant advantage of a machine learning-driven security framework is its scalability and adaptability. As organizations grow and their intranet environments become more complex, traditional security tools often struggle to keep pace with increasing volumes of network traffic and user activity. Machine learning models, however, can continuously evolve by learning from new data, allowing them to stay effective against emerging attack techniques. By leveraging advanced analytics, behavioral profiling, and predictive modeling, the proposed system strengthens the overall cybersecurity posture of intranet environments. Moreover, incorporating federated learning and decentralized intelligence-sharing mechanisms can enhance the robustness of threat detection models, enabling organizations to collaborate on cybersecurity without exposing sensitive data.

2. LITERATURE SURVEY :

This explores machine learning for detecting behaviour-based intranet attacks. By analysing network traffic and system logs, the model identifies anomalies, enabling proactive threat detection. It enhances security with real-time detection and adaptive defence mechanisms. Empirical evaluations demonstrate its effectiveness in strengthening cybersecurity frameworks and mitigating emerging threats. [I]

This paper presents a hybrid network intrusion detection method using improved residual network blocks and Bi-GRUs. It improves feature extraction and captures temporal dependencies for accurate anomaly detection. The model outperforms traditional techniques, demonstrating effectiveness in strengthening network security and adapting to evolving cyber threats. [2]

This research introduces an Al-driven network intrusion detection system based on Generative Adversarial Networks (GANs). The model improves anomaly detection by generating synthetic attack data to enhance classification accuracy. By learning complex attack patterns, it strengthens intrusion detection capabilities. Empirical evaluations demonstrate its effectiveness in improving cybersecurity and adapting to evolving threats. [3]

The infonner-based intrusion detection technique for network attacks on integrated energy systems utilizes attention mechanisms to analyse time-series data efficiently for real-time monitoring of network threats. This method also increases the efficiency of the system, and detection accuracy. However, it requires immense computational resources, both for training and real-time processing, and may pose a problem to detect new types of attacks. [4]

Network intrusion detection has greatly benefited from deep learning techniques, which enhance accuracy and adaptability to evolving cyber threats. Models such as CNNs, RNNs, and transformers improve feature extraction and anomaly detection in network traffic. Despite their effectiveness, challenges like high computational costs, data imbalance, and real-time processing limitations persist. [5]

EXISTING SYSTEM :

Existing techniques for behavior-based intrusion detection in enterprise network traffic usually deploy different alg,rithms within an analysis paradigm to identify significant deviation from the established baseline behavior. Examples of such techniques often include D:!cision Trees, which classify network dumps based on a series of if-else decision rules, and Random Forest, further an ensemble learning technique that combines various decision trees to improve accuracy and robustness. Furthennore, Ensemble methods provide using a mixture of multiple weak learners leading to proper classification performance. These algorithms combine to create an advanced intrusion detection system that would be capable of detecting and mitigating behavior- based attacks on enterprise networks.

PROPOSED SYSTEM :

In the proposed system, we aim to develop a robust and efficient framewmk for detecting intranet attacks based on user behaviour identification using machine learning techniques. The system will incorporate a combination of supervised learning algirithms, including &ipport Vector Machine (SVM), Logistic Regression, K-Nearest Neigribours (KNN), Gradient Boosting, and Naive Bayes. These algorithms will analyse network traffic data to identify suspicious pat1ems that may indicate intranet attacks. The first phase of the project focuses on pre-processing the network data 10 handle missing values and encode categirical features. Once the data is prepared, various machine learning models will be trained on labelled data to learn the typical behaviour of the intranet network.

CONCLUSIONS :

The advanced approach presented for detecting behavior-based intranet attacks by machine learning shows promising results and implications for cybersecurity. By using sophisticated machine learning algorithms, the system shows remarkable improvements in the accuracy and efficiency of detecting intranet attacks based on behavioral pat1ems. The extensive evaluation and experin1entation underscore the effectiveness of the approach in identifying and mitigating various types of intranet threats. Moreover, the adaptability and scalability of the system ensure that it remains relevant and applicable in dynamic network environments. Overa!L the fmding, indicate that leveraging machine learning for behavior-based detection can si ificantly enhance the security posture of intranet systems and provide organizations with robust defense mechanisms against evolving cyber threats. As such, this research contributes valuable insights and methodologies 10 the field of cybersecurity, therefore building a foundation for further advancements in proactive threat detection and network defense strategies.

FUTURE SCOPE :

This advanced approach for detecting behavior-based intranet attacks by machine learning may be further in1proved in the future. For example, incorporating more complex machine learning techniques, such as deep learning models, would improve the detection of intricate patterns and anomalies in the system. Incorporating real-time monitoring capabilities will enable the system 10 respond rapidly 10 emerging threats, thereby in1proving the overall security posture of the intranet. Improving the scalability and adaptability of the system to diverse network environments and configuations will also make it applicable to a wider range of organizational infrastructures. Additionally, using techniques from the area of explainable artificial intelligence (XAI) would make the system's decisions more interpretable, and hence, cybersecurity professionals would be able to understand and trust its recommendations. Lastly, continued research into new features and data sources for intrusion detection could further hone the system's detection capabilities and resilience against evolving cyber threats.

ABBREVIATIONS AND ACRONYMS :

1. **Al** - Artificial Intelligence
2. **IDS-** Intrusion Detection System
3. **SVM-** Support Vector Machine
4. **KNN** - K-Nearest Neighbours
5. GAN-Generative Adversarial Network
6. **CNN** - Convolutional Neural Network
7. **RNN** - Recurrent Neural Network
8. **XAI-** Explainable Artificial Intelligence
9. **Bi-GRU** - Bidirectional Gated Recurrent Unit
10. **NIDS-** Network Intrusion Detection System

REFERENCES :

1. [l] M Jang and K. Lee, "An Advanced Approach for Detecting Behavior-Based h1tranet Attacks by Machine Learning," in IEEE Access, vol. 12, pp. 52480-52495, 2024, doi: 10.l 109/ACCESS.2024.3387016.
2. Yu, Hongchen, et al. "Network intrusion detection method based on hybrid improved residual network blocks and bidirectional gated recurrent units." *IEEE Access* 11 (2023): 68961-68971..
3. Park, Cheolhee, et al. "An enhanced NIDS -based network intrusion detection system using generative adversarial networks." *IEEE Internet of Things Journal* 10.3 (2022): 2330-2345.
4. Sun, Yuzhen, et al. "lnfom,er-based intrusion detection method for network attack of inte ated energy system." *IEEE Joumal of Radio Frequency Identification* 6 (2022): 748-752.
5. Sinagra, Jayden. *Deep learning techniques for network intrusion detection.* MS thesis. University of Malta, 2024.