International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Detection and Prevention of Insider Threats Using Artificial Neural Networks

[1]B Harish Kumar Reddy,[2]Besat Pavankalyan, [3]Karee Lingamurthy, [4]S. Andhraiah

[1] Assistant Professor, Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology

[2,3,4] B. Tech Students, Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology

ABSTRACT

Insider threats represent one of the most critical challenges in modern cybersecurity environments, as they originate from individuals who already possess authorized access to organizational systems and data. These threats may be intentional, such as malicious data theft, or unintentional, such as accidental data exposure. Traditional security mechanisms, including firewalls and rule-based monitoring systems, are often ineffective in detecting insider threats because they rely on predefined signatures and lack adaptive learning capabilities. This project proposes a neural network-based approach to detect insider threats by analyzing user behavior patterns, access logs, and system activity. The neural network model is trained to identify abnormal activities that deviate from normal behavioral patterns. The system continuously monitors user actions and classifies them as normal or suspicious in real time. By leveraging deep learning capabilities, the proposed approach improves detection accuracy, reduces false positives, and enhances organizational security. This intelligent and adaptive solution provides an effective mechanism to prevent data breaches, financial loss, and reputational damage caused by insider threats.

Keywords: Insider Threat Detection, Neural Networks, Cybersecurity, Deep Learning, Behavioral Analysis, Anomaly Detection, Artificial Intelligence, Security Monitoring.

I. INTRODUCTION

With the increasing reliance on digital systems and cloud infrastructure, organizations face growing cybersecurity risks. Among these risks, insider threats are particularly dangerous because insiders have legitimate access to sensitive data and systems. Insider threats may include employees, contractors, or partners who misuse their access privileges for malicious purposes or unintentionally compromise security.

Traditional security systems such as firewalls, antivirus software, and intrusion detection systems primarily focus on external threats. However, these systems are less effective in detecting insider threats because insiders operate within authorized access boundaries. Therefore, there is a need for intelligent systems that can analyze user behavior and identify anomalies.

Artificial Intelligence and Neural Networks have emerged as powerful tools for pattern recognition and anomaly detection. Neural networks can learn complex behavioral patterns from large datasets and detect deviations that indicate suspicious activity. This project uses a neural network-based model to monitor user activities and detect insider threats efficiently and accurately.

II. LITERATURE SURVEY

1.Title: Insider Threat Detection Using Machine Learning Techniques

Authors: Salem, M., Hershkop, S., and Stolfo, S.

Description:

This study focuses on detecting insider threats using machine learning algorithms by analyzing user behavioral patterns. The authors proposed a system that monitors user activities such as login time, file access, and network usage. Machine learning models were trained to distinguish between normal and abnormal behaviors. The results showed that machine learning techniques significantly improve the detection of insider threats compared to traditional rule-based systems. This work highlights

the importance of behavioral analysis in cybersecurity.

2. Title: Anomaly Detection in Cybersecurity Using Neural Networks

Authors: Javaid, A., Niyaz, Q., Sun, W., and Alam, M.

Description:

This paper presents a neural network-based anomaly detection system designed to identify suspicious activities in computer networks. The authors used deep learning models to analyze system logs and network traffic. The neural network was able to learn complex patterns and detect abnormal behavior effectively. The results demonstrated improved accuracy and reduced false positives, showing that neural networks are highly suitable for cybersecurity applications.

3. Title: Insider Threat Detection Through User Behavior Analytics

Authors: Eberle, W., and Holder, L.

Description:

This research focuses on using user behavior analytics to detect insider threats. The authors analyzed user activity data and applied data mining techniques to identify abnormal patterns. Their approach helped in detecting malicious insiders by comparing current user behavior with historical patterns. The study proved that behavioral monitoring is an effective method for insider threat detection.

4. Title: Deep Learning for Cybersecurity: A Comprehensive Review

Authors: Yin, C., Zhu, Y., Fei, J., and He, X.

Description:

This paper provides a detailed review of deep learning techniques used in cybersecurity. The authors discussed various neural network models such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN). The study explains how deep learning models can detect cyber threats, including insider attacks, with high accuracy. The review highlights the advantages of deep learning in analyzing large and complex datasets.

5. Title: Detecting Insider Threats Using Artificial Intelligence Techniques

Authors: Parveen, P., McDaniel, P., and Thuraisingham, B.

Description:

This research explores the use of artificial intelligence techniques to detect insider threats. The authors used machine learning algorithms to analyze user behavior and detect suspicious activities. The system was able to identify abnormal access patterns and prevent security breaches. The study demonstrated that AI-based approaches provide better threat detection compared to traditional methods.

III. EXISTING SYSTEM

The existing systems for insider threat detection primarily rely on traditional security mechanisms such as rule-based monitoring, signature-based intrusion detection systems, access control policies, and manual log analysis. These systems monitor user activities including login attempts, file access, and network usage, and compare them against predefined rules or known threat signatures. If any activity matches the predefined malicious patterns, the system generates an alert. However, these approaches are limited because they depend on previously identified attack patterns and cannot effectively detect new, unknown, or sophisticated insider threats. Since insiders use valid credentials and authorized access, their malicious activities often appear legitimate, making detection difficult for conventional systems. Additionally, traditional systems lack adaptive learning capabilities and cannot analyze complex user behavior patterns over time. This results in high false positive rates and inefficient threat detection. Therefore, the existing systems are not sufficient to provide accurate, intelligent, and real-time insider threat detection in modern cybersecurity environments..

IV. PROPOSED SYSTEM

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

The proposed system uses a neural network-based approach to detect insider threats by analyzing user behavior and system activity patterns. The system collects data such as login time, file access history, system usage, and network activity, and preprocesses it to prepare for analysis. A neural network model is trained using historical user activity data to learn normal behavior patterns. Once trained, the model continuously monitors real-time user activities and compares them with the learned patterns. If any abnormal or suspicious behavior is detected that deviates from normal activity, the system identifies it as a potential insider threat and generates an alert for security administrators. Unlike traditional systems, the proposed system has the ability to learn and adapt automatically, allowing it to detect both known and unknown threats with higher accuracy. This intelligent and automated approach improves threat detection efficiency, reduces false positives, and enhances overall system security by providing real-time monitoring and early detection of insider attacks.

V. SYSTEM ARCHITECTURE

The system architecture of the Neural Network-Based Insider Threat Detection System consists of several integrated components that work together to monitor and detect suspicious user activities. The process begins with the data collection module, which gathers user activity data from various sources such as login records, file access logs, system usage, and network activity. This collected data is then sent to the data preprocessing module, where it is cleaned, normalized, and converted into a suitable format for analysis. After preprocessing, the data is used in the neural network training module, where the model learns normal user behavior patterns from historical data. Once the model is trained, it is deployed in the detection module, which continuously monitors real-time user activity and analyzes it using the neural network. If the system detects any abnormal behavior that deviates from the learned patterns, it classifies it as a potential insider threat. Finally, the alert module generates warnings and notifications to the system administrator, allowing immediate action to prevent security breaches. This architecture ensures accurate, automated, and real-time detection of insider threats, thereby enhancing overall system security.

Fig 5.1: Structure of the Proposed System

The system architecture of the Neural Network-Based Insider Threat Detection System consists of several modules that work together to collect user data, analyze behavior, and detect insider threats accurately. Each module performs a specific function to ensure efficient and reliable threat detection.

The process begins with the Data Collection Module, which collects user activity data from various sources such as login records, file access logs, system usage history, and network activity. This data provides information about how users interact with the system and is essential for identifying behavioral patterns.

The collected data is then sent to the Data Preprocessing Module, where it is cleaned and prepared for analysis. This module removes unnecessary or duplicate data, handles missing values, and converts the data into a proper numerical format. Data normalization is also performed to improve the accuracy and performance of the neural network model.

After preprocessing, the data is passed to the Neural

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Network Training Module, where the neural network learns normal user behavior patterns from historical data. The model identifies relationships and patterns in the data and creates a trained model that can distinguish between normal and abnormal activities.

Once the model is trained, it is used in the Detection Module, which continuously monitors real-time user activity. The module compares current user behavior with the learned patterns. If any unusual or abnormal behavior is detected, it is considered a potential insider threat.

Finally, the Alert Module generates alerts and notifications when suspicious activity is detected. This allows the system administrator to take immediate action to prevent data breaches or system misuse. This architecture ensures real-time monitoring, accurate detection, and improved security against insider threats.

VI. IMPLEMENTATION

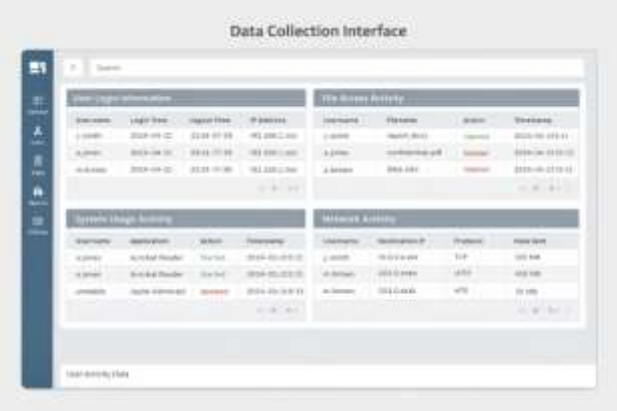

Fig 6.1: Data Collection Interface

Fig 6.2: Data Preprocessing and Cleaning Module

Fig 6.3: Feature Engineering and Selection Module

Fig 6.4: Model Training and Evaluation Module

Fig 6.5: Trend Forecasting and Prediction Dashboard

VII. CONCLUSION

The Neural Network-Based Insider Threat Detection System provides an intelligent and effective solution for identifying and preventing insider threats in

organizational environments. Traditional security systems are limited in detecting insider threats because they rely on predefined rules and cannot analyze complex user behavior patterns. In contrast, the proposed system uses neural network techniques to learn normal user behavior and detect abnormal activities in real time. By analyzing user activity data such as login patterns, file access, and network usage, the system can accurately identify suspicious behavior and generate alerts for immediate action. This approach improves detection accuracy, reduces false positives, and enhances overall system security. The system is automated, adaptive, and capable of detecting both known and unknown threats. Therefore, the proposed neural network-based approach plays a crucial role in strengthening cybersecurity and protecting sensitive organizational data from insider attacks.

VIII. FUTURE SCOPE

The Neural Network-Based Insider Threat Detection System can be further enhanced by integrating advanced deep learning techniques and modern security technologies to improve detection accuracy and efficiency. In the future, the system can be extended to use advanced models such as Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Transformer-based models to better analyze sequential user behavior and detect complex insider threats. The system can also be integrated with real-time monitoring tools and cloud-based platforms to provide scalable and continuous threat detection across large organizations. Additionally, incorporating automated response mechanisms can help the system take immediate action, such as blocking suspicious users or restricting access, without manual intervention. The use of larger and more diverse datasets can further improve model performance and reliability. Moreover, the system can be enhanced with visualization dashboards and explainable AI techniques to help administrators understand threat patterns more clearly. These improvements will make the system more robust, intelligent, and capable of providing stronger protection against insider threats in evolving cybersecurity environments.

IX. REFERENCES

[1] Nasir, R., Afzal, M., Latif, R., and Iqbal, W. Behavioral Based Insider Threat Detection Using Deep Learning. IEEE Access, 2021.DOI:https://doi.org/10.1109/ACCESS.2021.3118297

[2] Kim, J., Park, M., Kim, H., Cho, S., and Kang, P. Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms.Applied Sciences, 2019.DOI: https://doi.org/10.3390/app9194018

[3] Al-Shehari, T., Al-Razgan, M., and Alfaqih, T. Insider Threat Detection Model Using Anomaly-Based Isolation Forest Algorithm. IEEE Access, 2023.DOI: https://doi.org/10.1109/ACCESS.2023.3326750

[4] Al-Shehari, T., Rosaci, D., and Al-Razgan, M. Enhancing Insider Threat Detection in Imbalanced Cybersecurity Settings Using LOF Algorithm.IEEE Access, 2024.DOI: https://doi.org/10.1109/ACCESS.2024.3373694

[5] Yi, J., et al.Insider Threat Detection Model Enhancement Using Hybrid Learning Methods. Electronics Journal, 2024.DOI: https://doi.org/10.3390/electronics13050973

[6] Kim, J., et al.User Behavior Modeling and Anomaly Detection for Insider Threat Detection.Applied Sciences, 2019.DOI: https://doi.org/10.3390/app9194018

[7] Yuan, S., et al.Deep Learning for Insider Threat Detection: A Survey. Computers & Security, 2021.DOI: https://doi.org/10.1016/j.cose.2021.102474

[8] Tao, X., et al.Insider Threat Detection Based on Test-Time Training and ResNet. Software Impacts, 2025.DOI: https://doi.org/10.1016/j.simpa.2024.100530

[9] Kantchelian, A., et al.Facade: High-Precision Insider Threat Detection Using Deep Contextual Anomaly Detection. arXiv, 2024.DOI: https://doi.org/10.48550/arXiv.2412.06700

[10] Paul, S., and Mishra, S.LSTM Autoencoder for Insider Threat Detection. arXiv, 2020.DOI: https://doi.org/10.48550/arXiv.2008.0564
[11] Ali, A., Husain, M., and Hans, P.Real-Time Insider Threat Detection Using Deep Evidential Clustering. arXiv, 2025.DOI: https://doi.org/10.48550/arXiv.2505.15383
[12] Ye, X., et al.Insider Threat Detection Using Convolutional Neural Networks. Scientific Reports, 2025.DOI: https://doi.org/10.1038/s41598-025-04029-w
[13] Lopez, J., and Sartipi, K.Insider Threat Detection Using LSTM Neural Networks. Journal of Information Security, 2020. DOI:https://doi.org/10.1109/TNSM.2020.2967721
[14] ACM ResearchUser Behavior Analytics Using LSTM Autoencoder for Threat Detection. ACM Conference, 2020. DOI: https://doi.org/10.1145/3406601.3406610
[15] Dalhousie University ResearchUnsupervised Learning for Insider Threat Detection. IEEE Transactions on Network and Service Management, 2021. DOI:https://doi.org/10.1109/TNSM.2021.3051999