IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2

Mitigating Insider Threat : A Neural Network Approach for Enhanced Security

Ms Bejjanki Pooja[1], B. Aditya[2], Ch. Sirisha[3]
Gandamalla Samatha[4], Kandhi Gayathri[5], Yellaboina Harshith Kumar[6]
Assistant Professor, Department of CSE[1,2,3]
UG Student, Department of CSE[4,5,6]
CMR Technical Campus, Hyderabad, Telangana, India
poojareddybejjanki@gmail.com, Adi.sacs@gmail.com
237r1a05e6@cmrtc.ac.in, 237r1a05f2@cmrtc.ac.in, 237r1a05k1@cmrtc.ac.in

Abstract: *Insider threats represent a significant cybersecurity challenge within IoT-enabled institutional environments due to the exploitation of legitimate access for malicious activities. Traditional insider threat detection (ITD) approaches often struggle with issues such as data imbalance, high dimensionality, and evolving user behaviors. This research presents a detection model leveraging a neural network to address these challenges effectively. The proposed model captures complex patterns in insider threat data and improves the accuracy of detection.*

Additionally, Principal Component Analysis (PCA) is employed for feature extraction, while K-means clustering is used to group user activity patterns. To handle data imbalance, data augmentation techniques are applied. Furthermore, optimization techniques are used to fine-tune the model parameters, ensuring better performance. Experimental evaluation on the CMU CERT insider threat dataset demonstrates the effectiveness of the proposed model, achieving high detection accuracy and a low false alarm rate. Compared to existing methods, the approach enhances detection performance, model robustness, and computational efficiency, making it a reliable solution for securing IoT infrastructures against insider threats.

Keywords: *Traditional insider threat detection*

I. INTRODUCTION

The proliferation of the Internet of Things (IoT) in institutional environments has revolutionized operations across various domains, including education, healthcare, corporate enterprises, and government agencies. IoT systems, composed of interconnected devices, sensors, and communication protocols, facilitate real-time data collection, analysis, and decision-making. However, the increasing reliance on IoT infrastructure has simultaneously escalated the risk of cyber threats, particularly insider threats. Unlike external attacks, insider threats exploit legitimate access to infiltrate, manipulate, or exfiltrate sensitive information. These threats pose a severe security risk due to the perpetrators' familiarity with internal systems, enabling them to disguise malicious actions as regular activities. In response to these challenges, this research presents a Graph Convolutional Network (GCN)-based insider threat detection model to enhance the accuracy, reliability, and robustness of detection mechanisms in IoT-enabled environments To address these challenges, machine learning and neural network approaches have emerged as powerful tools for analyzing large datasets and identifying hidden behavioral patterns. Neural networks can learn complex relationships in user activity data and detect anomalies that may indicate potential insider attacks. By leveraging these capabilities, this project proposes a neural network-based approach to mitigate insider threats and enhance organizational security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2

II. PROBLEM DEFINITION

Insider threats have become one of the most significant challenges in modern cybersecurity because they originate from individuals who already possess authorized access to an organization's systems and sensitive information. Unlike external attacks, insider threats are difficult to detect since malicious activities often appear similar to legitimate user behavior.

Traditional security mechanisms such as rule-based monitoring, signature-based detection, and access control systems mainly focus on identifying known attack patterns and external intrusions, making them less effective in detecting subtle and evolving insider activities. Additionally, modern organizational networks and IoT-based environments generate massive volumes of high-dimensional user activity data, including login records, file access logs, communication patterns, and system usage information. Analyzing such complex data using conventional methods becomes inefficient and often leads to high false positive rates or missed detections.

Another major challenge is the imbalance in insider threat datasets, where normal user activities significantly outnumber malicious ones, causing many detection models to perform poorly in identifying rare insider attacks. Furthermore, insider behaviors may involve hidden relationships between users, systems, and resources that traditional models fail to capture.

Therefore, there is a need for an advanced detection approach capable of analyzing complex behavioral patterns, handling large-scale data, and accurately identifying suspicious activities. This research addresses these challenges by proposing a neural network-based approach for mitigating insider threats, aiming to analyze user behavior patterns, detect anomalies, and improve the overall effectiveness of insider threat detection systems.

III. METHODOLOGY

The proposed methodology focuses on developing an effective neural network-based framework to detect and mitigate insider threats by analyzing user activity patterns within an organizational environment. The process begins with data collection and preprocessing, where user activity logs such as login records, file access information, system usage details, and communication logs are gathered from available insider threat datasets. Since raw data often contains noise, missing values, and redundant features, preprocessing techniques such as data cleaning, normalization, and feature selection are applied to improve data quality and ensure better model performance. After preprocessing, the relevant behavioral features that represent user activities are extracted to create a structured dataset suitable for model training and analysis.

1. Data Collection

User activity data is collected from system logs such as login records, file access logs, network activity, and email communication

2. Data Preprocessing

The collected data is cleaned by removing missing values, duplicates, and inconsistent entries. The data is then formatted and normalized to prepare it for model training.

3. Feature Selection

Important features related to insider behavior are selected, such as login frequency, file access patterns, device usage, and communication behavior. This helps the model focus on the most relevent information.

4. Model Training

A Neural Network model is trained using the processed dataset. The model learns patterns of normal user activities and identifies unusual behaviors that may indicate insider threats.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2

5. Prediction

The trained model analyzes new user activity data and predicts whether the behavior is normal or suspicious, helping organizations detect insider threats early and improve security.

IV. PROPOSED SYSTEM

To address the limitations of existing ITD models, this research proposes an advanced detection framework that leverages a Graph Convolutional Network (GCN) alongside data augmentation and Bayesian optimization techniques. The proposed model introduces innovations in feature extraction, data balancing, and hyperparameter tuning to improve detection accuracy and reduce false alarms.

In this system, user activity data such as login details, file access records, system usage logs, and communication patterns are collected and analyzed to identify abnormal behavior that may indicate potential insider threats. The system first performs data preprocessing to remove noise, handle missing values, and normalize the dataset so that it becomes suitable for analysis. After preprocessing, relevant behavioral features are extracted to represent the activities of users within the system. These features are then used as input for a neural network model that learns patterns of normal and malicious behavior from historical data

V. IMPLEMENTATION & ARCHITECTURE

The implementation of the system involves integrating machine learning techniques with a web-based application. Initially, a dataset related to user behavior and activity patterns is collected. This data may include login frequency, file access patterns, time of system usage, and other behavioral indicators. The collected data is then preprocessed by removing inconsistencies, handling missing values, and normalizing the features to improve the efficiency of the machine learning model.

MODULES

A. User Module

The User module allows individuals to interact with the system. Initially, a new user registers by providing the required credentials, which are stored in the system database. After successful registration, the user can log in to the system using valid authentication details. Once authenticated, the user can access the main functionality of the system, which is making predictions. In this process, the user provides activity-related inputs or behavioral data. The system processes this information through the neural network model to determine whether the behavior represents normal activity or a potential insider threat. After completing the required operations, the user can securely log out of the system.

B. Admin Module

The Admin module is responsible for monitoring and managing the entire system. The administrator logs into the system with privileged credentials. Once authenticated, the admin can view all registered users in the system and manage their access. The admin has the ability to activate or deactivate user accounts depending on security requirements. In addition, the admin can monitor prediction results generated by the system. This allows the administrator to analyze user behavior patterns and detect suspicious activities. The admin can also view prediction ratios and statistics that summarize the number of normal activities and detected threats. These analytical insights help in making security-related decisions and maintaining system integrity.

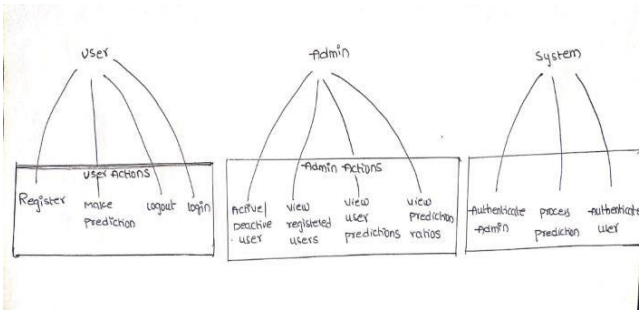
C. System Module

The System module acts as the core processing unit of the architecture. It handles authentication and prediction processing. The system verifies login credentials for both users and administrators to ensure secure access. After authentication, when a user submits behavioral data for prediction, the system processes this data through a neural network model. The neural network analyzes patterns in the input data and identifies whether the activity is normal or

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2

potentially malicious. This intelligent analysis enables the system to detect insider threats based on behavioral anomalies.

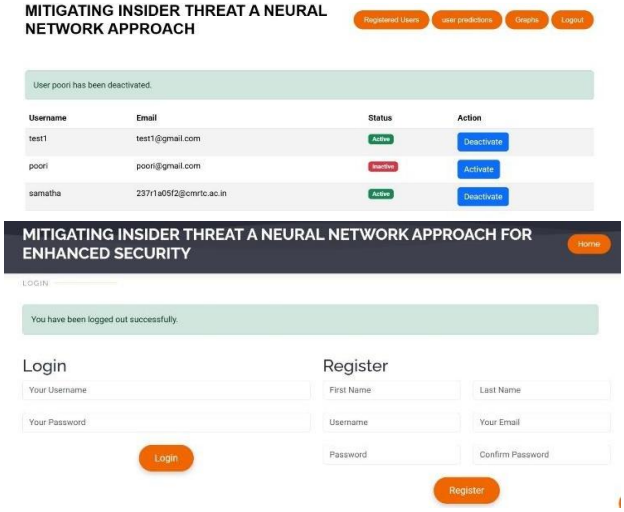
SYSTEM ARCHITECTURE



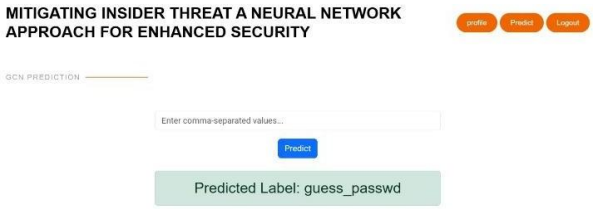
1. The system first allows a new user to register by providing the required details, after which the user can log in using valid credentials to access the application.
2. Once logged in, the user can perform actions such as making predictions, interacting with the system features, and logging out after completing the process.
3. When a prediction request is made, the system collects the user activity data and processes it using a neural network model to analyze behavioral patterns.
4. The administrator monitors the system by viewing registered users, checking user predictions, and activating or deactivating user accounts to maintain security.
5. The system authenticates both users and administrators to ensure that only authorized individuals can access the application.
6. Finally, the system processes the collected data and generates prediction results that help identify potential insider threats and support improved organizational security.

VI. EXPERIMENTAL RESULTS

The experimental phase of this project focuses on developing and testing a neural network–based system to detect insider threats. User activity data such as login records, file access logs, and system usage patterns are collected and preprocessed before being used to train the neural network model to identify normal and suspicious behavior.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2



The experimental results of the project Mitigating Insider Threats: A Neural Network Approach for Enhanced Security demonstrate the working of the developed system through user authentication and administrative control. The first interface shows the login and registration module, where new users can create an account and existing users can securely log into the system. This ensures that only authorized users can access the platform. The second interface represents the administrative dashboard, where the administrator can monitor registered users, view their details, and control their access status by activating or deactivating accounts. If any suspicious or abnormal user behavior is detected, the administrator can deactivate the user to prevent potential insider threats.

VII. CONCLUSION

Focuses on improving organizational security by detecting suspicious activities performed by authorized users within a system. The developed system utilizes a neural network model to analyze user behavior patterns such as login activities, access records, and system usage data to identify potential insider threats. Through the implementation and experimental evaluation, the system successfully demonstrates the ability to monitor users, predict abnormal behavior, and assist administrators in taking preventive actions such as activating or deactivating user access.

Machine learning and neural network techniques enhance the accuracy and efficiency of threat detection compared to traditional security mechanisms. Studies show that machine learning–based systems can effectively analyze user behavior patterns and identify malicious insiders with high accuracy, making them useful for modern cybersecurity solutions.

VIII. FUTURE SCOPE

Involves enhancing the system with more advanced technologies to improve the accuracy and efficiency of insider threat detection. In the future, the model can be trained with larger and more diverse datasets to better understand complex user behavior patterns. The system can also be integrated with real-time monitoring mechanisms to continuously track user activities and generate instant alerts when suspicious behavior is detected. Additionally, advanced deep learning techniques and improved neural network architectures can be incorporated to increase prediction accuracy and reduce false alarms. The project can further be expanded by integrating cloud-based security systems and data visualization dashboards to help administrators monitor threats more effectively. With these improvements, the system can be applied in large organizations to strengthen cybersecurity and protect sensitive information from potential insider threats.

REFERENCES

[1]. Khan, A. Y., Latif, R., Latif, S., Tahir, S., Batool, G., & Saba, T. (2020). Malicious Insider Attack Detection in IoTs Using Data Analytics. IEEE Access, 8, 11743–11753. DOI: 10.1109/ACCESS.2019.2959047

[2]. Marbut, A. R., & Harms, P. D. (2023). Fiends and Fools: A Narrative Review and Neo-Socioanalytic Perspective on Personality and Insider Threats. Journal of Business and Psychology, 39, 679–696. DOI: 10.1007/s10869-023-09885-9

[3]. Burhan, M., Rehman, R., Khan, B., & Kim, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), 2796. DOI: 10.3390/s18092796

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, March 2026
Impact Factor: 8.2

[4]. Peccatiello, R. B., Gondim, J. J. C., & Garcia, L. P. F. (2023). Applying One-Class Algorithms for Data Stream-Based Insider Threat Detection. IEEE Access, 11, 70560–70573. DOI: 10.1109/ACCESS.2023.3293825

[5]. Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A Review of Insider Threat Detection Approaches with IoT Perspective. IEEE Access, 8, 78847–78867. DOI: 10.1109/ACCESS.2020.2990195

[6]. Al-Shehari, T., & Alsowail, R. A. (2021). An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques. Entropy, 23(10), 1258. DOI: 10.3390/e23101258

[7]. Al-Mhiqani, M. N., Ahmed, R., Zainal, Z., & Isnin, S. N. (2021). An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection. International Journal of Advanced Computer Science and Applications, 12(1), 573–577. DOI: 10.14569/IJACSA.2021.0120166

[8]. Yuan, F., Shang, Y., Liu, Y., Cao, Y., & Tan, J. (2020). Data Augmentation for Insider Threat Detection with GAN. IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI), 632–638. DOI: 10.1109/ICTAI50040.2020.00104

[9]. Zhu, D., Huang, X., Li, N., Sun, H., Liu, M., & Liu, J. (2022). RAP-Net: A Resource Access Pattern Network for Insider Threat Detection. International Joint Conference on Neural Networks (IJCNN), 1–8. DOI: 10.1109/IJCNN55064.2022.9892637

[10]. Li, X., Li, X., Jia, J., Li, L., Yuan, J., Gao, Y., & Yu, S. (2023). A High Accuracy and Adaptive Anomaly Detection Model with Dual-Domain Graph Convolutional Network for Insider Threat Detection. IEEE Transactions on Information Forensics and Security, 18, 1638–1652. DOI: 10.1109/TIFS.2023.3245413

[11]. Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2023). Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. Computer Systems Science and Engineering, 44(2), 1679–1689. DOI: 10.32604/csse.2023.026526

[12]. Lavanya, P., Glory, H. A., & Sriram, V. S. (2024). Mitigating Insider Threat: A Neural Network Approach for Enhanced Security. IEEE Access, 12, 73752–73768. DOI: 10.1109/ACCESS.2024.3404814

[13]. Ullah, I., Mengersen, K., Hyndman, R. J., & McGree, J. (2021). Detection of Cybersecurity Attacks Through Analysis of Web Browsing Activities Using Principal Component Analysis. arXiv Preprint, arXiv:2107.12592

[14]. Lindauer, B. (2020). Insider Threat Test Dataset. Carnegie Mellon University. Available Online

[15]. Sandholtz, N., Miyamoto, Y., Bornn, L., & Smith, M. A. (2023). Inverse Bayesian Optimization: Learning Human Acquisition Functions in an Exploration vs Exploitation Search Task. Bayesian Analysis, 18(1), 1–24. DOI: 10.1214/22-BA1313

[16]. Kaplan, M. O., & Alptekin, S. E. (2020). An Improved BiGAN-Based Approach for Anomaly Detection. Procedia Computer Science, 176, 185–194. DOI: 10.1016/j.procs.2020.09.060

[17]. Fang, Y., Niu, M., Cheung, P., & Lin, L. (2022). Extrinsic Bayesian Optimizations on Manifolds. arXiv Preprint, arXiv:2212.13886