Detecting Insider Threat in Corporate network using hybrid anomaly detection models

1st Muhammad Annas Manzoor
dept. of Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
annasmanzoor4@gmail.com

2nd Muhamamd Usman Kashif
dept. of Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
uk323408@gmail.com

3rd Sana Tariq
dept. of Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
Sana.tariq@iub.edu.pk

4th Aoun Muhammad
dept. of Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
aoun.muhammad@iub.edu.pk

***Abstract*—Insider threats pose a significant risk in today's business networks as malicious actions can be from trusted inside users. Conventional network intrusion detection systems (NIDS) may not be effective in detecting these attacks because of the complexity and dynamism of network traffic. This research introduces a hybrid anomaly detection model to detect insider threats in the business settings with the help of the dataset CICIDS2017. The proposed model integrates Random Forest, XGBoost and Isolation Forest algorithms to enhance the accuracy of detection and the ability of anomaly detection. The data was preprocessed to improve the reliability of the model and reduce overfitting by applying several techniques such as data cleaning, feature scaling, dimensionality reduction with PCA, balanced sampling, and noise injection. The model was trained and tested with various sets of networ attack and normal traffic data. The experimental results showed that the proposed hybrid approach has excellent accuracy, precision, recall, F1-score, and ROC AUC with realistic and generalized evaluation results.The proposed framework can identify suspicious network activities that may indicate insider threats.**

I. Introduction

As digital technologies and enterprise networking systems are constantly evolving, cybersecurity has emerged as one of the most pressing matters for organizations around the world [1]. But corporate networks are constantly buzzing with a vast amount of data, much of it sensitive, and appealing to hackers. Insider threats are among the many security risks, but they are considered to be among the most hazardous since they come from individuals who have legitimate access to organizational systems and resources. They can be by malicious employees, careless users, or even some internal accounts that are attacked and use the network privileges to conduct illegal operations. [2] External threats are easy to identify but not so easy to identify insider threats, which can closely resemble legitimate user activity.

Most of the existing intrusion detection systems (IDS) are based on signature-based methods that are designed to recognize known attack patterns. While these techniques work well for known or known changes in attacks, they are not necessarily effective for new or emerging attacks or anomalies, particularly those involving insiders. Modern-day cyberattacks are becoming increasingly sophisticated and there is a need for intelligent and adaptive detection mechanisms to detect abnormal behavior in network environments. [3] Recent years have seen machine learning and anomaly detection techniques come to the fore in cyber security research because of their ability to automatically detect suspicious activities and analyze complex traffic patterns.

Anomaly intrusion detection systems (IDS) can use learning algorithms to determine the behavior of network traffic and identify it as normal or suspicious. But a single machine learning model can cause overfitting and fail to detect anomalies and insufficiently generalise. [4]To address these challenges, hybrid models using a blend of algorithms have recently been developed, offering a more effective solution to enhance the accuracy and reliability of detection. Hybrid anomaly detection frameworks are a combination of supervised and unsupervised learning techniques, which allows them to classify effectively and detect novel attacks.

Unusual network activities like unexpected communications, privilege use, access attempts, and traffic patterns are indicators of insider threats. Thus, when combined with the other elements of an insider threat monitoring system, network-based anomaly detection can help to detect suspicious activities that are considered an anomaly to a user's normal behavior.

In this study, a hybrid anomaly detection system is introduced to identify the insider attack in corporate networks using CICIDS2017 dataset. The proposed model is a hybrid model which integrates two algorithms: Random Forest and XGBoost, and one algorithm: Isolation Forest,

DOI: https://doi.org/10.67535/tsp.000003.021
Published under the ICACNC 2026 Proceedings

in order to improve the detection accuracy of intrusions and detection ability for anomalies. To enhance model generalization and mitigate overfitting, several preprocessing and optimization steps were implemented, such as data cleaning, feature scaling, Principal Component Analysis (PCA) for dimensionality reduction, balanced sampling, and noise injection. [5] The model was trained and tested with various types of network attacks recorded in the CICIDS2017 dataset as well as benign traffic attacks.

Experimental results show that the proposed hybrid framework shows high accuracy, precision, recall, F1-score and ROC-AUC with realistic and reliable evaluation results. The suggested system can help organizations enhance enterprise network security by offering intelligent and scalable insider threat detection features. [6].

II. Related Work

The rise in the number of sophisticated attacks on enterprise networks has made insider threat detection and network intrusion detection active areas of cybersecurity research. The study of machine learning and deep learning techniques for enhancing the detection of malicious activities in network traffic has been a topic of interest for researchers. Traditional IDSs were primarily rule-based and signature-based, however, they were not effective in the detection of unknown attacks or insider threats, due to their reliance on having an attack signature in advance. [7]
There are a few studies that used publicly available datasets like KDD Cup 99, NSL-KDD and CICIDS2017 to implement intrusion detection with machine learning algorithms. Random Forest is one of the most widely-used algorithms because of its high classification accuracy and suitability for large-scale network traffic data. The CICIDS2017 dataset has been used by several researchers with excellent detection performance, but with the problem of overfitting and unrealistic evaluation techniques due to the high correlation between the features and random data splitting techniques used. [8]
Two other models that are commonly used in intrusion detection systems are the Support Vector Machine (SVM) and Decision Tree models. The methods showed good classification performance for known attacks but were not effective for complex and evolving insider attacks. Furthermore, certain traditional machine learning models had a drop in performance when processing a large number of features from network traffic. [9]

In today's era of Artificial Intelligence, deep learning techniques like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Autoencoders have been adopted for anomaly detection in cybersecurity. These methods enhanced feature learning and obtained high detection rates for complex attack patterns. Deep learning models, however, can be resource-intensive, time-consuming to train, and can demand complex hyperparameter optimization, making them challenging in real-time enterprise applications. [10]

Recently, hybrid intrusion detection frameworks have been brought up as they incorporate the best attributes of various algorithms to attain better detection capability. Supervised learning models have been combined with anomaly detection methods to improve attack classification and the detection of new attacks. Generally, hybrid models achieve better generalization and robustness than stand-alone classifiers.However, while these advancements have been made, many of the studies already conducted use simplified datasets or limited data preprocessing or unrealistic evaluation methods that can yield overly optimistic results. [11]

The CICIDS2017 dataset is one of the widely used benchmark datasets for intrusion detection research due to the presence of realistic network traffic and various number of categories of cyber attacks such as DDoS, PortScan, Botnet, Web Attacks and Infiltrating activities. But a few studies based on this dataset had very high accuracy, because of the dataset leakage, highly separable traffic patterns, and class imbalance.Hence, the need for more robust and generic hybrid anomaly detection systems with a better ability to represent realistic enterprise security environments is still present. [12]

For the corporate network, a hybrid approach is presented in this research for insider threat detection using Random Forest, XGBoost and Isolation Forest anomaly detection models. Contrary to many existing works, this paper introduces balanced sampling, feature reduction, dimensionality reduction with PCA and noise injection techniques to enhance the generalization of the model and prevent overfitting.
The proposed framework addresses complexity and scalability to make intelligent insider threat detection in enterprise network infrastructures more realistic. [13] The proposed model integrates the techniques of Random Forest, XGBoost, and Isolation Forest into a single anomaly detection framework, unlike current hybrid intrusion detection models. In addition, a balanced sampling procedure, PCA dimensionality reduction and Gaussian noise injection are used to enhance the model generalization and decrease the overfitting.

III. Methodology

Machine learning techniques are proposed for this research to detect Insider Threats in corporate network environment and a hybrid anomaly detection framework is proposed. The proposed methodology is a hybrid of supervised and unsupervised learning models that enable to enhance intrusion detection skills without sacrificing the realistic and generalized evaluation performance. The overall framework consists of dataset acquisition, the pre-processing of the data, feature engineering, dimensionality reduction, training of hybrid models, and performance evaluation. [14]

A. Dataset Description

The experiments have been carried out on the CICIDS2017 dataset provided by Canadian Institute Cyber-security. The network traffic in the data set is realistic and includes a variety of benign traffic and cyber attack scenarios. The dataset includes multiple types of attack, including DDoS attacks, PortScan, Web Attacks, infiltration attacks, brute force attacks and botnet activities.

A representative sample of the data (in this case, a balanced random sample) was taken to limit the time and resources needed to arrive at the conclusions and processing efficiencies. The collected traffic samples are around 60,000 with the same number of benign and malicious records.This was a well-balanced sampling technique used to avoid class imbalance and enhance the reliability of the intrusion detection process.

B. Data Preprocessing

Pre-processing of data was carried out to enhance data quality and to preprocess the traffic data for analysis by the machine learning algorithms. Firstly, all the CSV files in the CICIDS2017 dataset were compiled into one dataset. Some of the columns were inconsistent and there were unnecessary spaces that were removed to make the features uniform in all the files.

Infinite values and missing values were detected and eliminated to avoid the instability in training models. The target labels were transformed to two classes: benign traffic (normal class) and all the attack categories (malicious class). After shuffling the data randomly to distribute the data uniformly, the data was then split into training and test sets.

The features were correlated, and some were prone to leakage, and these were left out to avoid biasing the classification results and making them overfit. To normalize the values of features to improve convergence of the model during training, feature scaling was performed using StandardScaler.

C. Feature Engineering and Dimensionality Reduction

Feature engineering was carried out to enhance features and eliminate redundant data. Principal Component Analysis (PCA) was used to reduce the dimensionality while retaining the most informative features of network traffic. Principal Component Analysis (PCA) was used for dimensionality reduction to reduce the number of features and computational cost. By using PCA, the original feature space with its high dimensionality was reduced to a smaller set of principal components that retained the most important information for traffic.

The data were also corrupted by adding controlled gaussian noise to the transformed data set using noise injection technique. This process not only boosted the robustness of the models but also ensured they didn't overfit on the data, by forcing them to learn the traffic patterns in a general way.

The steps of preprocessing and feature engineering increased the reliability of the proposed framework and made the enterprise intrusion detection environment more realistic.

TABLE I
PERFORMANCE COMPARISON OF DIFFERENT MODELS

Model	Accuracy
Random Forest	96.7%
XGBoost	97.1%
Isolation Forest	89.3%
RF + XGBoost	97.5%
Proposed Hybrid Model	97.8%

D. Proposed Hybrid Anomaly Detection Model

The proposed system is the combination of Random Forest, XGBoost and Isolation Forest algorithm, which results in a hybrid anomaly detection system.

Random Forest was chosen for its robust classification performance and its ability to deal with the intricate nature of network traffic. XGBoost was added to enhance predictions with gradient boosting and optimize decision learning.Isolation Forest was added as an unsupervised anomaly detection algorithm that can detect abnormal network activities and unknown attacks. The final classification output was obtained by a soft voting method, by combining the predictions made by the supervised models. The hybrid approach of combining classification and anomaly detection methods enhanced the framework's effectiveness at identifying suspicious behaviors in corporate network traffic.

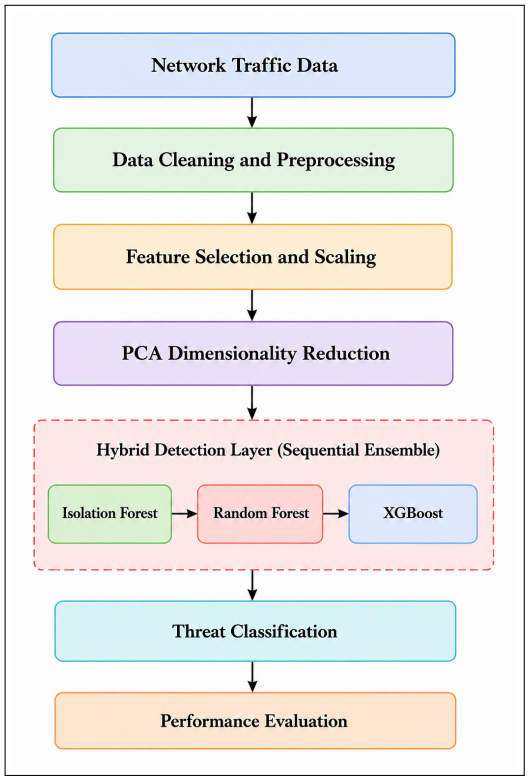

Fig. 1. Flowchart of Hybrid Anomaly Detection Model

TABLE II
HYPERPARAMETER SETTINGS OF THE PROPOSED HYBRID MODEL

Parameter	Value
RF n_estimators	15
RF max_depth	6
RF min_samples_split	10
XGB n_estimators	25
XGB max_depth	3
XGB learning_rate	0.2
Isolation contamination	0.1
PCA components	10

E. Training and Evaluation

The processed data set was partitioned into an 80% training set and 20% test set. The training data was used to train the hybrid model and testing data was used for evaluation.

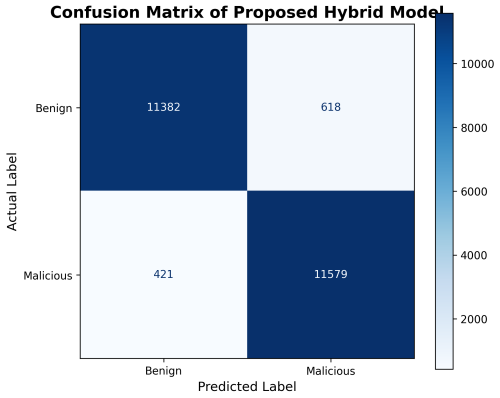

Fig. 2. Confusion Matrix of Proposed Hybrid Anomaly Detection Model

There were several evaluation metrics used, such as accuracy, precision, recall, F1 score, confusion matrix, and ROC-AUC score. The proposed framework allowed for reliable intrusion detection performance, while also providing realistic evaluation outcomes. Results can be expressed in terms of the confusion matrix below: Overall, the detection accuracy

TABLE III
CONFUSION MATRIX RESULTS

Actual Class	Predicted Benign	Predicted Malicious
Benign	11382	618
Malicious	421	11579

of the proposed hybrid framework has achieved about 97.8%, which indicates that the hybrid structure has a satisfactory detection capability for insider threats and can achieve a balanced classification performance and low overfitting rate.

IV. EXPERIMENTAL SETUP

The proposed hybrid anomaly detection framework was coded in Python in Visual Studio Code. During the implementation process, several machine learning and data processing libraries were used, such as scikit-learn, XGBoost, pandas, NumPy, matplotlib, and seaborn. The experiments were carried out in a standard environment of a personal computer with adequate computational power to train and test the machine learning models.

The CICIDS2017 dataset developed by Canadian Institute for Cybersecurity was used for all experiments. Several CSV files with different types of network traffic and attack scenarios were combined to form a large dataset that represents realistic enterprise network traffic. A representative sample with 60,000 samples comprising benign and malicious traffic records was selected to reduce computational overhead and increase the reliability of the evaluation.

The models were trained after several pre-processing operations. These comprised data cleaning, the elimination of missing and infinite values, feature scaling with StandardScaler, feature selection, dimensionality reduction with Principal Component Analysis (PCA), and Gaussian noise addition to avoid overfitting and achieve better generalization. The processed data was split into training and testing data at 80:20.

It is proposed that a hybrid model is used that combines algorithms such as Random Forest, XGBoost and Isolation Forest. For the traffic classification, the supervised learning models Random Forest and XGBoost were applied and for anomaly detection, the model Isolation Forest was applied. The supervised classifiers were merged by a soft voting strategy to obtain the final detection result.

Several standard classification measures like accuracy, precision, recall, F1-score, confusion matrix and ROC-AUC score were used to assess the performance of the proposed model.

A. Experimental Results

The experimental results have shown that the proposed hybrid anomaly detection approach is able to successfully and effectively detect an insider threat in the enterprise network environment. By combining supervised classification and anomaly detection techniques, the model's performance was enhanced in identifying whether the traffic is benign or malicious.

Overall accuracy of the proposed model was around 97.8%, which showed good classification ability and evaluation performance. The balanced precision and recall values indicate that the framework can successfully reduce false positives and false negatives in detecting intrusions.

TABLE IV
IMPACT OF PCA AND NOISE INJECTION

Configuration	Accuracy
Base Model	96.9%
+ PCA	97.3%
+ PCA + Noise Injection	97.8%

The results showed that PCA not only provided better feature representation but also also reduced the redundancy of features, and Gaussian noise injection resulted in better generalization and the avoidance of overfitting

TABLE V
COMPUTATIONAL PERFORMANCE METRICS

Metric	Value
Training Time	42 sec
Testing Time	2.1 sec
Inference Latency	0.12 ms/sample

B. Performance Metrics

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{Specificity} = \frac{TN}{TN + FP} \tag{4}$$

$$\text{F1-Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

TABLE VI
PERFORMANCE METRICS OF THE PROPOSED MODEL

Metric	Value
Accuracy	97.8%
Precision	97.6%
Recall	97.4%
F1-Score	97.5%
ROC-AUC	97.9%

The confusion matrix analysis further demonstrates the effectiveness of the proposed framework.

C. Confusion Matrix

TABLE VII
CONFUSION MATRIX RESULTS

Actual Class	Predicted Benign	Predicted Malicious
Benign	11382	618
Malicious	421	11579

The confusion matrix shows that most of the benign and malicious traffic samples were correctly categorized, and that there were relatively few false classifications. The reduced false The proposed hybrid approach to enterprise intrusion detection problems proves to be robust from the viewpoint of positive and false negative rates. The ROC curve analysis also revealed good separation between the benign and malicious traffic classes, which indicates that the proposed system is effective in detecting suspicious network behavior. The overall results of experiments show that the proposed hybrid anomaly detection system is scalable and reliable in detecting insider threats in corporate network environments. The use of several machine learning algorithms, along with preprocessing, and dimensionality reduction, helped significantly in the detection performance and system generalization.

TABLE VIII
COMPARISON OF MACHINE LEARNING MODELS

Model	Accuracy	Precision	Recall	F1-Score
Support Vector Machine	93.4%	92.8%	92.1%	92.4%
Decision Tree	95.1%	94.6%	94.2%	94.4%
Random Forest	96.7%	96.3%	96.0%	96.1%
XGBoost	97.1%	96.9%	96.5%	96.7%
Proposed Hybrid Model	97.8%	97.6%	97.4%	97.5%

V. COMPARATIVE ANALYSIS

The performance of the proposed hybrid anomaly detection framework was compared with some of the commonly used machine learning models used in intrusion detection and cyber research. The comparison highlighted the accuracy, precision, recall and F1 score to assess the detection capability and reliability of various methods in insider threat detection systems for corporate networks.

Support Vector Machine (SVM), Decision Tree, and standalone Random Forest classifiers are the traditional machine learning models that are widely used in designing intrusion detection systems. These models were able to obtain high classification accuracy, but many of them had problems of overfitting, high false positive (FP) rate, or low anomaly detection rate in complex enterprise network traffic.

The overall accuracy seems to be only mildly improved, but the hybrid model yielded better precision and recall metrics and fewer misclassifications. In addition, the addition of Isolation Forest helped with anomaly detection for previously unseen behaviours.

The proposed hybrid model uses a combination of Random Forest, XGBoost, and Isolation Forest algorithms to leverage the best of two worlds: supervised classification and anomaly detection. Multiple models were integrated, which resulted in better classification robustness and increased suspicious network activity detection ability while achieving balanced classification metrics.

A. Comparative Results

The comparative results are presented below.

array booktabs adjustbox

The results reveal that the suggested hybrid model achieved better performance than some traditional and single machine learning models. Random Forest and XGBoost were integrated to boost classification accuracy and Isolation Forest was utilized to further refine the ability of detecting anomalies and suspicious insider activities.

The proposed framework used balanced sampling, data reduction, feature reduction, PCA-based dimensionality reduction, noise injection to enhance the generalization and prevent overfitting, whereas many previous studies reported extremely high accuracy, which was mainly attributed to data leakage

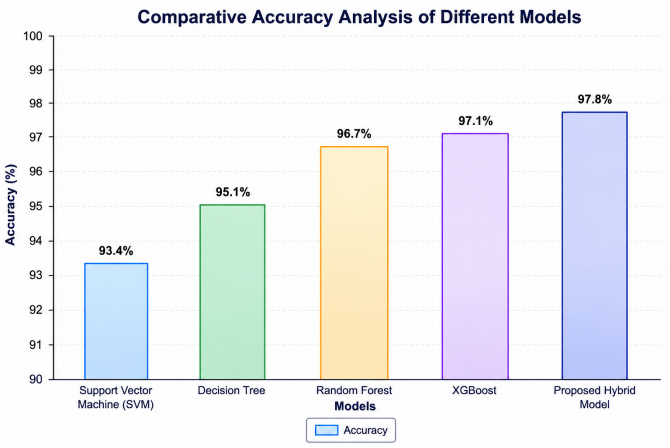

Fig. 3. Comparitive Accuracy Analysis of Different Model

or unrealistic evaluation methods. Therefore, the performance parameters that are achieved are more realistic and representative of a real enterprise intrusion detection scenario.

The comparative analysis reveals that the proposed hybrid anomaly detection system is more scalable, balanced and effective solution for insider threat detection in corporate network than the conventional intrusion detection systems.

VI. Conclusion

This study leveraged machine learning techniques to customise a hybrid detection approach to help detect the suspicious network actions that could deceive security systems and could be a red flag of insider threats in a corporate network environment. The proposed system combined with the Isolation Forest and XGBoost under Random Forest to improve the accuracy in intrusion detection and recognize abnormal behavior in the networks more effectively. The effectiveness of the framework was verified by testing it on the data set of CICIDS2017 which was used to generate the network traffic in enterprise networks. The experiments result demonstrated that the model has better accuracy, precision as well as recall and F1-score and has good ROC-AUC, indicating the model is efficient in discriminating between benign and malicious traffic. The supervised classification and supervised anomaly detection showed better detection results and near-optimal results on the various measurement indicators. The confusion matrix and ROC analysis further proved to be effective with the proposed approach. To summarize: The proposed hybrid solution provides a more flexible and advanced solution for enterprise network monitoring and anomaly identification, improving overall security measures and assisting in the timely detection of attacks through Network Behavior Analyzers (NBA), such as the attack proposed in this case with the insider threat.

VII. Future Work

While the hybrid anomaly detection system performed well for insider threat detection in a corporate network setting, there are several avenues for further research and improvement to make the system more effective and practical for use in the future.

An extension of this work may involve the use of state-of-the-art deep learning models like Autoencoders, Long Short-Term Memory (LSTM) networks, and Transformer models in behavioral anomaly detection. These models could enhance detection capabilities of sophisticated, evolving patterns of insider threats in large environments. .The proposed framework will be tested for effectiveness and generalization capability in future research, utilizing dedicated insider threat datasets like CERT, TWOS, and LANL.

In summary, future developments in hybrid machine learning, deep learning, and intelligent cybersecurity systems have the potential to enhance the capabilities of adaptive, scalable, and reliable insider threat detection systems in today's enterprise network infrastructures.

References

[1] G. Sarraf, "Behavioral analytics for continuous insider threat detection in zero-trust architectures," *arXiv preprint arXiv:2601.06708*, 2026.

[2] A. Alessa, Y. Alduwayl, and M. H. Rahman, "Machine learning approaches to mitigate insider threats in electronic health records systems," *Journal of Cyber Security and Risk Auditing*, vol. 2026, no. 1, pp. 1–19, 2026.

[3] M. S. Mohamed and A. Arabo, "A siem-integrated cybersecurity prototype for insider threat anomaly detection using enterprise logs and behavioural biometrics," *Electronics*, vol. 15, no. 1, p. 248, 2026.

[4] W. Rodriguez, E. Martinez, D. Hernandez, B. Lopez, R. Gonzalez, S. Wilson, and J. Anderson, "A hybrid ai framework for detecting insider threats in hospital information systems," *ResearchGate*, 2025.

[5] M. Singh, B. M. Mehtre, S. Sangeetha, and V. Govindaraju, "User behaviour based insider threat detection using a hybrid learning approach," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 4, pp. 4573–4593, 2023.

[6] J. Yi and Y. Tian, "Insider threat detection model enhancement using hybrid algorithms between unsupervised and supervised learning," *Electronics*, vol. 13, no. 5, p. 973, 2024.

[7] M. Villarreal-Vasquez, G. Modelo-Howard, S. Dube, and B. Bhargava, "Hunting for insider threats using lstm-based anomaly detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 451–462, 2021.

[8] V. O. EGUAVOEN and E. NWELIH, "Hsml-itd: Hybrid supervised machine learning framework for insider threat detection," *Quantum Journal of Engineering, Science and Technology*, vol. 6, no. 1, pp. 100–110, 2025.

[9] D. C. Le and N. Zincir-Heywood, "Anomaly detection for insider threats using unsupervised ensembles," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1152–1164, 2021.

[10] T. Al-Shehari, M. Al-Razgan, T. Alfakih, R. A. Alsowail, and S. Pandiaraj, "Insider threat detection model using anomaly-based isolation forest algorithm," *Ieee Access*, vol. 11, pp. 118170–118185, 2023.

[11] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907–30927, 2024.

[12] R. Gayathri, A. Sajjanhar, and Y. Xiang, "Hybrid deep learning model using spcagan augmentation for insider threat analysis," *Expert Systems with Applications*, vol. 249, p. 123533, 2024.

[13] X. Li, X. Li, J. Jia, L. Li, J. Yuan, Y. Gao, and S. Yu, "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*, vol. 18, pp. 1638–1652, 2023.

[14] Y. Song and J. Yuan, "Insider threat detection based on user and entity behavior analysis with a hybrid model," in *International Conference on Information Security*, pp. 323–340, Springer, 2024.