HSML-ITD: HYBRID SUPERVISED MACHINE LEARNING FRAMEWORK FOR INSIDER THREAT DETECTION

EGUAVOEN, V. O.[1*] – NWELIH, E.[2]

[1] *Department of Computer Science, Wellspring University, Edo State, Nigeria.*

[2] *Department of Computer Science, University of Benin, Edo State, Nigeria.*

**Corresponding author*
e-mail: eguavoen.osasu[at]wellspringuniversity.edu.ng

(Received 01st November 2024; revised 23rd February 2025; accepted 02nd March 2025)

Abstract. The digital transformation driven by Information and Communication Technology (ICT) has amplified data accessibility and operational efficiency across organizations. However, it has also escalated cybersecurity vulnerabilities, with insider threats emerging as a critical concern. Traditional detection methods often fail to address the sophisticated and evolving nature of these threats, necessitating advanced solutions. This study proposes the Hybrid Supervised Machine Learning Framework for Insider Threat Detection (HSML-ITD), integrating Support Vector Machines (SVM) for initial data classification and Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for predictive learning. The model aims to enhance detection accuracy, reduce false positives, and provide a robust mechanism for insider threat mitigation. The framework was developed using the CERT insider threat dataset, with a structured methodology comprising data preprocessing, SVM-based classification, and ANFIS-based predictive learning. Performance was evaluated using a 5-fold cross-validation technique and comparative analyses with conventional models were conducted to validate the hybrid approach. The HSML-ITD demonstrated superior performance, achieving an accuracy of 92%, precision of 93%, recall of 89%, and F1-Score of 91%. Comparative analysis revealed significant improvements over standalone models, particularly in handling noisy data and high-dimensional input spaces. The hybrid model effectively balanced prediction accuracy and robustness, addressing limitations of conventional methods. The HSML-ITD offers a scalable and accurate solution for insider threat detection, significantly enhancing organizational cybersecurity. Future research will focus on incorporating real-time detection capabilities, optimizing computational efficiency, and expanding validation across diverse datasets. By addressing these aspects, the model can further solidify its applicability in dynamic threat environments.
Keywords: *insider threat detection, hybrid machine learning, Support Vector Machine (SVM), Adaptive Neuro-Fuzzy Inference System (ANFIS), cybersecurity*

Introduction

The widespread adoption of Information and Communication Technology (ICT) technologies in conjunction with smart devices and network infrastructures has revolutionized organizational data accessibility, facilitating efficient information flow across diverse sectors. However, this digital transformation has exposed organizations to multifaceted cybersecurity challenges, with insider threats emerging as a critical concern (Almusawy and Alrammahi, 2024). According to OpenText Web Portal (2024), insider threats emerge when authorized users-including current/former employees, contractors, vendors, or partners-abuse their legitimate access privileges in ways that harm an organization's digital assets and infrastructure. Intermixit Web Portal (2024) highlights that insiders account for 60% of data breaches, with 55% of organizations identifying privileged users as their primary risk. Similarly, Smith (2024) notes a sharp rise in insider threats in recent years, reporting that 76% of organizations observed increased activity and a 28% growth in insider-driven data exposure incidents between

2023 and 2024. Additionally, 71% of companies experienced 21 to 40 insider security incidents annually in 2023, and 73% of security leaders predict further escalation in data loss due to insider events in the coming year. Internal security incidents carry substantial operational and financial consequences. According to Verizon Business Web Portal (2023), non-malicious human factors like social engineering victimization and user errors accounted for 68% of breaches. Financial attacks involving ransomware or extortion represented 62% of incidents, with breaches typically costing $46,000. Cybersecurity Insiders Web Portal (2024) reports that organizations require an average of 197 days to detect breaches and 77 additional days for recovery.

Wei et al. (2024) highlight that conventional insider threat detection approaches struggle to counter sophisticated modern attacks. Despite advances in monitoring solutions like SIEM/SEM (Rauf et al., 2023), these tools often fail to effectively synthesize and analyse security evidence. This limitation has spurred interest in advanced solutions, particularly in the realm of Machine Learning (ML), to enhance network security and threat detection capabilities (Atadoga et al., 2024). Recent research has explored both Conventional Machine Learning (CML) and Hybrid Machine Learning (HML) algorithms for insider threat prediction (Rauf et al., 2021; Kim et al., 2019; Yuan, et al., 2018). However, the persistent escalation of insider attacks raises questions about the efficacy of current approaches and the potential benefits of comparative analyses between CML and HML algorithms. Machine learning has revolutionized the detection of insider threats through its advanced analytical capabilities. By leveraging ML techniques, organizations can now process extensive data collections to forecast potential security risks with significant precision (Choraś and Kozik, 2018). Traditional ML approaches, including Support Vector Machines, Decision Trees, and Logistic Regression, have gained widespread adoption in insider threat monitoring systems, primarily due to their computational advantages and ease of deployment. However, these standalone models face challenges, including noisy data, overfitting, and limited adaptability to dynamic threat landscapes (Janjua et al., 2020; Sheykhkanloo and Hall, 2020).

To address these limitations, Hybrid Machine Learning (HML) approaches have emerged as a promising alternative. By integrating the strengths of multiple algorithms, HML models enhance prediction accuracy, adaptability, and robustness. Adaptive Neuro-Fuzzy Inference Systems (ANFIS), for example, combine neural networks and fuzzy logic to handle nonlinear data and provide explanatory mechanisms for predictions (Nayak and Raghatate, 2024; Eguavoen and Nwelih, 2023). These hybrid models are particularly effective in addressing the weaknesses of CML algorithms, such as handling sparse datasets and mitigating the impact of noisy features. While significant advancements have been made in insider threat detection, existing approaches often struggle with balancing classification precision and predictive adaptability. This study introduces a novel hybrid framework that integrates Support Vector Machines (SVM) for precise initial classification with Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for robust predictive learning. This integration uniquely addresses classification-prediction gaps, enabling enhanced detection accuracy and adaptability to dynamic threat landscapes. This study proposes the Hybrid Supervised Machine Learning Model for Insider Threat Detection (HSML-ITD), which integrates SVM for initial data labelling and ANFIS for predictive learning. The model leverages SVM's ability to classify data with high precision and ANFIS's flexibility in handling nonlinear relationships and fuzzy data. By combining these techniques, the HSML-ITD

aims to enhance prediction accuracy, reduce false positives, and provide a robust framework for insider threat detection.

The contributions of this study are threefold: (1) It presents a hybrid machine learning model that addresses the limitations of conventional approaches to insider threat detection. (2) It conducts a comprehensive evaluation of the model using real-world datasets, demonstrating its effectiveness in mitigating insider threats. (3) It highlights the potential of hybrid models in advancing the field of insider threat detection and provides insights for future research.

Related work

Insider threat detection has emerged as a critical area of research in cybersecurity due to the significant risks posed by malicious insiders to both corporate and government networks. This section reviews recent advancements in insider threat detection methodologies, focusing on machine learning approaches, hybrid frameworks, and novel data analysis techniques.

Machine learning and deep learning approaches

Machine learning and deep learning approaches have emerged as dominant methodologies for detecting insider threats in modern cybersecurity frameworks. Le et al. (2020) created a user-centered ML system capable of analysing data at multiple granularities, achieving an 85% detection rate for malicious insiders with a low false positive rate of 0.78%. However, their system faced challenges with unbalanced datasets and limited ground truth. Song et al. (2024) introduced the Behaviour Rhythm Insider Threat Detection (BRITD) model, which incorporates time-sensitive behavioural feature extraction. The deep learning model achieved superior performance with a 0.9730 AUC and 0.8072 precision when evaluated on the CMU CERT dataset. While showing strong detection capabilities, the model's potential for overfitting to specific datasets was noted as a limitation. Yuan and Wu (2021) conducted a comprehensive review of deep learning techniques in insider threat detection, highlighting their advantages over traditional ML approaches, particularly in handling high-dimensional, complex, and heterogeneous data. Their findings indicated that deep learning models enhance detection accuracy by learning end-to-end patterns directly from complex data. However, they also identified persistent challenges, including the scarcity of labelled data and the difficulty in countering adaptive insider threats.

Hybrid frameworks and multi-layered approaches

Hybrid frameworks combining multiple techniques have shown promise in improving detection accuracy and adaptability. Gamachchi et al. (2018) proposed a hybrid framework utilizing graphical analysis and anomaly detection to analyse heterogeneous data. While effective in distinguishing typical user behaviour from suspicious activity, the framework's reliance on specific detection techniques potentially limited its adaptability to complex threats. Al-Mhiqani et al. (2022) presented a novel multilayer framework integrating multi-criteria decision-making techniques for model selection and a hybrid approach combining misuse and anomaly detection. This framework demonstrated high accuracy (99% for known threats, 97% for unknown threats) and low false-positive rates on the CERT r4.2 dataset. However, the study lacked a comprehensive comparison with existing systems and did not address

overfitting concerns or model interpretability. Wei et al. (2024) introduced a hybrid framework that integrates statistical criteria with machine learning classification, achieving a detection accuracy of 98.48% on the CERT r4.2 dataset. This approach aimed to overcome limitations of traditional methods in analyzing activity-related information and handling noisy datasets. However, the framework's reliance on a specific dataset raised concerns about its generalizability.

Novel data analysis techniques

Researchers have explored various novel data analysis techniques to enhance insider threat detection. Janjua et al. (2020) implemented predictive models using linguistic analysis of employee emails, with the Adaboost algorithm achieving 98.3% accuracy in identifying malicious emails. However, the study's reliance on a small dataset limited its generalizability. Gong et al. (2024) surveyed graph-based insider threat detection methods, highlighting their advantages in handling complex intranet data. The study categorized existing work into three key phases: data collection, graph construction, and graph anomaly detection, demonstrating that models incorporating more information yield superior performance. Gayathri et al. (2024) introduced SPCAGAN, a GAN leveraging linear manifold learning to create synthetic insider threat training data. This approach addressed the challenge of limited insider threat datasets due to confidentiality concerns, although its dependence on synthetic data raised questions about capturing the full complexity of real-world insider threat behaviours.

Behavioral modelling and analysis

Several studies focused on behavioural modelling to improve insider threat detection. Nikiforova et al. (2024) examined user behaviour in information systems through audit records, constructing behaviour models represented as graphs for real-time anomaly detection. Their approach, implemented in the "e-StepControl" system, demonstrated the ability to monitor user behaviour across diverse business environments. Von Der Assen et al. (2024) introduced a novel approach incorporating Business Process Modelling and Notation (BPMN) to identify non-technical threats within organizational workflows. This method showed promise in automatically detecting insider threats through BPMN diagrams, as demonstrated in a real-world IT provider case study. Yi and Tian (2024) proposed a method combining unsupervised outlier scores with supervised insider threat detection, achieving an accuracy of 86.12% using only 20% of the computing budget. This integrated approach outperformed traditional anomaly detection methods by up to 12.5% under the same conditions.

Challenges and future direction

TN and Pramod (2023) conducted a systematic literature review, revealing significant potential for event-based models and advocating for a combined approach to enhance early detection of insider threats. Bhandari and Pudashine (2023) emphasized the challenge of security threats posed by privileged users but noted a lack of comprehensive analysis on the interaction between internal and external threats. This gap suggests a need for more holistic approaches to threat detection that consider both insider and outsider threats simultaneously.

Research gap and motivation

The review of related works reveals a significant research gap in the comparative analysis of conventional and hybrid machine learning techniques for insider threat detection. Most studies focus on standalone models, neglecting the potential of hybrid approaches to enhance prediction accuracy and robustness. This study aims to fill this gap by proposing the Hybrid Supervised Machine Learning Model for Insider Threat Detection (HSML-ITD), which integrates SVM and ANFIS to leverage their complementary strengths.

Materials and Methods

This section details the methodology and design framework of the Hybrid Supervised Machine Learning Model for Insider Threat Detection. The proposed model combines the strengths of Support Vector Machines (SVM) for data classification and Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for predictive learning. This hybrid approach addresses the limitations of standalone machine learning models, such as handling noisy and high-dimensional data, while improving prediction accuracy and robustness.

Research framework

The methodology follows a structured framework comprising the following phases: (1) Dataset Acquisition and Preprocessing: Obtaining and preparing data for model training and evaluation. (2) SVM-Based Data Classification: Classifying unlabelled datasets into distinct classes. (3) ANFIS-Based Predictive Learning: Training and testing the model using classified data. (4) Model Validation and Performance Evaluation: Assessing the model's accuracy, precision, and error rate. This framework ensures systematic implementation and evaluation of the model, providing reliable insights into its performance.

Dataset acquisition and pre-processing

The dataset used in this study was sourced from the CERT insider threat repository, a publicly available resource containing records of user activities and labelled instances of malicious and non-malicious behaviour. The dataset comprised 350 samples, including attributes such as date, user, source, action, and insider threat status. Pre-processing steps are include: (1) Feature Selection: Irrelevant and redundant features (e.g., vector and ID fields) were removed to enhance model efficiency. (2) Data Cleaning: Missing and inconsistent values were addressed through imputation and normalization techniques. (3) Label Assignment: The dataset was divided into two classes-malicious and non-malicious-based on activity patterns and predefined criteria.

Support Vector Machine (SVM) for data classification

The SVM algorithm was employed to classify the preprocessed dataset into distinct labels, serving as the input for the ANFIS predictive model. SVM operates by identifying the optimal hyperplane that separates data points into two categories, maximizing the margin between them. The SVM classification are: (1) Kernel Transformation: Data points were transformed into a higher-dimensional space using a radial basis function (RBF) kernel, enabling the separation of nonlinear data. (2) Hyperplane Optimization: The algorithm iteratively adjusted the hyperplane to minimize classification errors while maximizing the margin. (3) Output Generation:

Labelled datasets were generated, distinguishing malicious from non-malicious instances.

Adaptive Neuro-Fuzzy Inference System (ANFIS) for predictive learning

ANFIS integrates neural networks and fuzzy logic to model complex relationships in data. It employs fuzzy if-then rules and adaptive learning mechanisms to approximate nonlinear functions, making it ideal for insider threat prediction. ANFIS Architecture are: (1) Input Layer: Receives labelled data from the SVM classification step. Attributes such as date, user, source, and action are mapped to input variables. (2) Membership Function Layer: Assigns membership values to input variables using generalized bell functions, providing flexibility and smooth transitions. (3) Rule Layer: Generates fuzzy rules based on input variables and membership values. For example: *IF user activity is high AND source is external, THEN insider threat is malicious*. (4) Normalization Layer: Normalizes the firing strength of rules to ensure consistency in predictions. (5) Defuzzification Layer: Converts fuzzy outputs into crisp values, representing the likelihood of an insider threat. (6) Output Layer: Provides the final prediction, categorizing instances as malicious or non-malicious. The ANFIS training phase employed a hybrid learning algorithm combining Least Squares Estimation (LSE) and Backpropagation Gradient Descent (BPGD) to optimize parameters iteratively.

Model design, implementation as well as validation and performance evaluation

The HSML-ITD model was designed using Unified Modelling Language (UML) to capture its functional and behavioural aspects. The functional design are: SVM Block: Handles data preprocessing and classification; ANFIS Block: Conducts predictive learning and outputs results; and Integration Module: Facilitates seamless data flow between SVM and ANFIS components. The behavioral design are: Use Case Diagram: Depicts interactions between the system and security administrators, highlighting processes such as data loading, SVM classification, and ANFIS prediction; and Sequence Diagram: Represents the dynamic flow of data and control between system components, illustrating the sequential execution of tasks. The HSML-ITD model was implemented using Python, leveraging libraries such as scikit-learn for SVM and custom modules for ANFIS. The implementation included: (1) Data Loading and Preprocessing: Automated scripts for feature selection, cleaning, and normalization; (2) SVM Classification Module: Functions for kernel transformation, hyperplane optimization, and output generation; and (3) ANFIS Training and Testing Module: Components for membership function assignment, rule generation, and defuzzification.

The HSML-ITD model was validated using a 5-fold cross-validation technique to ensure robustness and generalizability. Performance metrics included: Accuracy: Proportion of correctly classified instances; Precision: Proportion of true positives among predicted positives; Recall: Proportion of true positives among actual positives; F1-Score: Harmonic mean of precision and recall; and Error Rate: Proportion of misclassified instances. The HSML-ITD model leverages the strengths of SVM and ANFIS to address the limitations of conventional approaches to insider threat detection. Its structured methodology, robust design, and promising validation results establish it as a reliable framework for enhancing organizational security.

Results and Discussion

This section presents the results of the Hybrid Supervised Machine Learning Model for Insider Threat Detection and discusses their implications. The performance of the HSML-ITD model is evaluated using the insider threat dataset, focusing on metrics such as accuracy, precision, recall, F1-score, and error rate. The findings highlight the model's efficacy in predicting insider threats and underscore its advantages over conventional approaches. The Support Vector Machine (SVM) block was tasked with classifying unlabelled data into two categories: malicious and non-malicious. This step is critical as it provides the labelled data required for Adaptive Neuro-Fuzzy Inference System (ANFIS) training. Key Metrics:

Accuracy: 92%
Precision: 93%
Recall: 89%
F1-Score: 91%

The high accuracy and precision values demonstrate the SVM's capability to separate classes effectively. However, the slight disparity between precision and recall indicates room for improvement in identifying all malicious instances, as some true positives were misclassified as non-malicious. *Figures 1* illustrate the SVM classification output. Data points are distinctly categorized into malicious and non-malicious groups, with minimal overlap, signifying the robustness of the classification process.

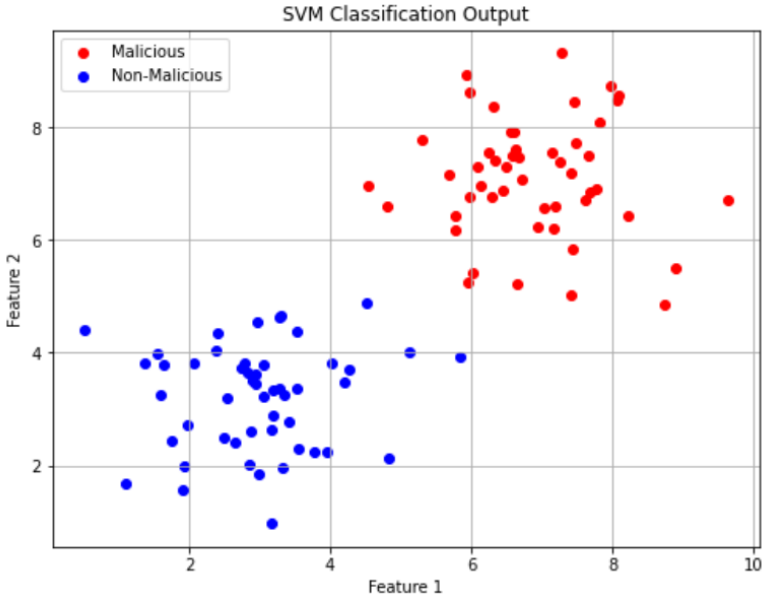

Figure 1. *SVM classification output.*

The Adaptive Neuro-Fuzzy Inference System (ANFIS) block utilized the labelled data from the SVM block for predictive learning. The training process involved 250 samples, while the testing phase employed 100 samples. Key Metrics:

Training Accuracy: 91%
Testing Accuracy: 89%

Error Rate: 9%
F1-Score: 90%

The results indicate that the ANFIS block effectively leveraged the labelled data to predict insider threats with high accuracy. The relatively low error rate highlights the model's capability to generalize well, even with limited training data. *Figure 2* and *Figure 3* depict the ANFIS training and testing graphs. The convergence patterns suggest that the hybrid learning algorithm (combining Least Squares Estimation and Backpropagation Gradient Descent) optimized the model parameters effectively, minimizing training errors over successive epochs. The ANFIS Training Graph shown in *Figure 2* represents the training error over 30 epochs. The curve shows a steady decline, starting from 0.9 and reducing to 0.1. This trend demonstrates the model's convergence and learning efficiency during the training phase while ANFIS Testing Graph in *Figure 3* shown the scatter plot compares predicted probabilities (orange points) against true labels (blue points). The alignment between the predicted probabilities and true labels indicates the model's strong performance in identifying malicious and non-malicious instances.

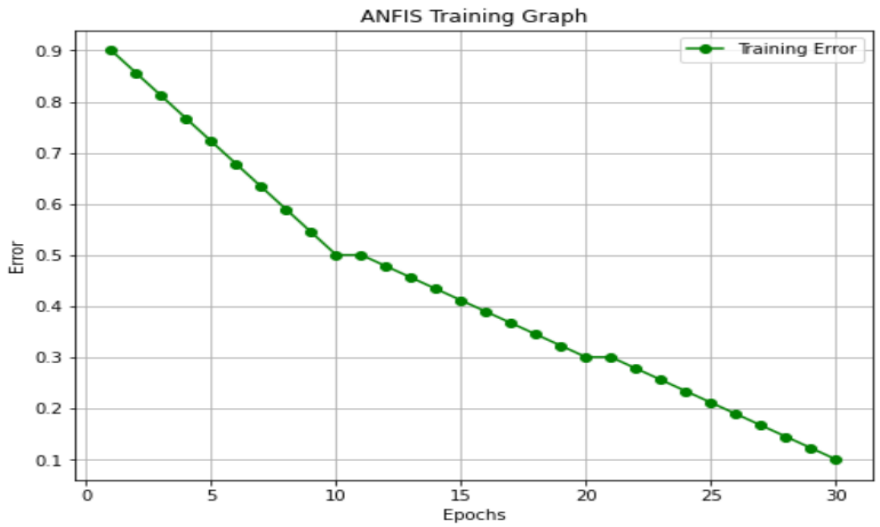

Figure 2. *ANFIS training graph.*

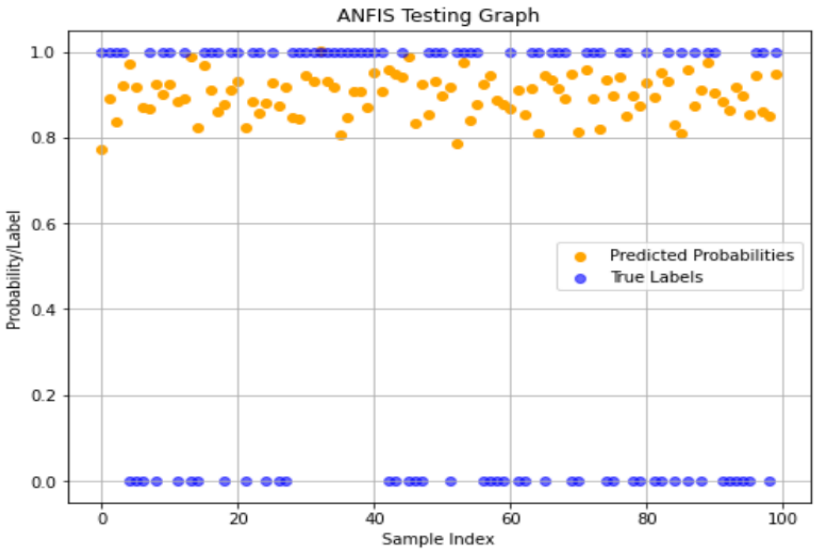

Figure 3. *ANFIS testing graph.*

Comparative analysis with conventional approaches

To contextualize the performance of HSML-ITD, its results were compared with those of conventional machine learning models, such as Decision Trees, Logistic Regression, and standalone SVM as shown in *Table 1*. The results clearly show that the hybrid HSML-ITD outperforms conventional models across all key metrics. The integration of SVM and ANFIS enhances classification accuracy and robustness, addressing limitations such as noisy data and high-dimensional input spaces.

Table 1*. Comparative results.*

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Decision tree	85	84	80	82
Logistic regression	87	86	83	84
Standalone SVM	90	91	86	88
HSMLM-IT (proposed)	92	93	89	91

The results validate the effectiveness of the model in detecting insider threats. Its superior performance can be attributed to the following factors: (1) Hybrid Approach: The combination of SVM and ANFIS leverages the strengths of both models, enabling accurate classification and robust predictive learning. (2) Feature Selection: The preprocessing phase ensured that only relevant features were used, reducing noise and enhancing model performance. (3) Adaptive Learning: The ANFIS block's ability to approximate nonlinear relationships in data contributed significantly to its high accuracy and low error rate. The findings have several implications for insider threat detection: (1) Enhanced Security: The model provides organizations with a reliable tool for identifying insider threats, thereby mitigating risks to critical assets. (2) Scalability: The model's ability to handle high-dimensional and sparse datasets makes it suitable for diverse organizational environments. (3) Practical Application: The low error rate and high accuracy suggest that the model can be deployed in real-world scenarios with minimal false positives and negatives.

Conclusion

Despite its promising results, the model has certain limitations: (1) Real-Time Detection: The current implementation focuses on batch processing, limiting its applicability for real-time threat detection. (2) Computational Costs: The hybrid learning approach, while effective, requires significant computational resources. (3) Dataset Dependence: The model's performance may vary with different datasets, necessitating further testing across diverse environments. Future research should explore the integration of real-time processing capabilities, optimization of computational efficiency, and validation using larger and more diverse datasets. Additionally, incorporating interpretability mechanisms such as SHAP or LIME could enhance the model's transparency and user trust. The results demonstrate the HSML-ITD model's superior performance in insider threat detection, surpassing conventional machine learning approaches. Its hybrid design, combining SVM and ANFIS, effectively addresses the challenges of noisy data, imbalanced datasets, and high-dimensional input spaces. By providing a scalable and accurate solution, the model has the potential to significantly enhance organizational security and pave the way for future advancements in insider threat detection.

Acknowledgement

This research is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Al-Mhiqani, M.N., Ahmad, R., Abidin, Z.Z., Abdulkareem, K.H., Mohammed, M.A., Gupta, D., Shankar, K. (2022): A new intelligent multilayer framework for insider threat detection. – Computers & Electrical Engineering 97: 23p.

[2] Almusawy, B., Alrammahi, A.A. (2024): Insider Detection Using Combination of Machine Learning and Expert Policies. – International Journal of Electrical and Electronic Engineering & Telecommunications 13(5): 389-396

[3] Atadoga, A., Sodiya, E.O., Umoga, U.J., Amoo, O.O. (2024): A comprehensive review of machine learning's role in enhancing network security and threat detection. – World Journal of Advanced Research and Reviews 21(2): 877-886.

[4] Bhandari, D., Pudashine, K. (2023): Insider Threat Detection using LSTM. – Journal of Science and Technology 3(1): 57-65.

[5] Choraś, M., Kozik, R. (2018): Machine learning techniques for threat modeling and detection. – In Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, Academic Press 13p.

[6] Cybersecurity Insiders Web Portal (2024): 2024 Insider Threat Report [Gurucul]. – Cybersecurity Insiders Web Portal 2p.

[7] Eguavoen, V., Nwelih, E. (2023): Hybrid Soft Computing System for Student Performance Evaluation. – Studia Universitatis Babes-Bolyai Engineering 68(1): 3-17.

[8] Gamachchi, A., Sun, L., Boztas, S. (2018): A graph based framework for malicious insider threat detection. – ArXiv Preprint ArXiv:1809.00141 18p.

[9] Gong, Y., Cui, S., Liu, S., Jiang, B., Dong, C., Lu, Z. (2024): Graph-based insider threat detection: A survey. – Computer Networks 254: 21p.
[10] Intermixit Web Portal (2024): Insider threats. – Intermixit Web Portal 12p.
[11] Janjua, F., Masood, A., Abbas, H., Rashid, I. (2020): Handling insider threat through supervised machine learning techniques. – Procedia Computer Science 177: 64-71.
[12] Kim, J., Park, M., Kim, H., Cho, S., Kang, P. (2019): Insider threat detection based on user behavior modeling and anomaly detection algorithms. – Applied Sciences 9(19): 21p.
[13] Le, D.C., Zincir-Heywood, N., Heywood, M.I. (2020): Analyzing data granularity levels for insider threat detection using machine learning. – IEEE Transactions on Network and Service Management 17(1): 30-44.
[14] Nayak, A., Raghatate, K.S. (2024): Implementing adaptive neuro-fuzzy inference systems (ANFIS) for risk assessment of drug interactions. – Communication on Applied Nonlinear Analysis 32(2s): 87-94.
[15] Nikiforova, O., Romanovs, A., Zabiniako, V., Kornienko, J. (2024): Detecting and identifying insider threats based on advanced clustering methods. – IEEE Access 12: 30242-30253.
[16] OpenText Web Portal (2024): What is an insider threat? – OpenText Web Portal 6p.
[17] Gayathri, R.G., Sajjanhar, A., Xiang, Y. (2024): Hybrid deep learning model using spcagan augmentation for insider threat analysis. – Expert Systems with Applications 249: 14p.
[18] Rauf, U., Mohsen, F., Wei, Z. (2023): A taxonomic classification of insider threats: Existing techniques, future directions & recommendations. – Journal of Cyber Security and Mobility 12(2): 221-252.
[19] Rauf, U., Shehab, M., Qamar, N., Sameen, S. (2021): Formal approach to thwart against insider attacks: A bio-inspired auto-resilient policy regulation framework. – Future Generation Computer Systems 117: 412-425.
[20] Sheykhkanloo, N.M., Hall, A. (2020): Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset. – International Journal of Cyber Warfare and Terrorism (IJCWT) 10(2): 1-26.
[21] Smith, G. (2024): Insider Threat Statistics: (2025's Most Shocking Trends). – Station X Web Portal 26p.
[22] Song, S., Gao, N., Zhang, Y., Ma, C. (2024): BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. – Cybersecurity 7(1): 20p.
[23] TN, N., Pramod, D. (2024): Insider intrusion detection techniques: A state-of-the-art review. – Journal of Computer Information Systems 64(1): 106-123.
[24] Verizon Business Web Portal (2023): 2024 Data Breach Investigations Report. – Verizon Business Web Portal 12p.
[25] Von Der Assen, J., Hochuli, J., Grübl, T., Stiller, B. (2024): The Danger Within: Insider Threat Modeling Using Business Process Models. – In 2024 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE 7p.
[26] Wei, Z., Rauf, U., Mohsen, F. (2024): E-Watcher: insider threat monitoring and detection for enhanced security. – Annals of Telecommunications 79(11): 819-831.
[27] Yi, J., Tian, Y. (2024): Insider threat detection model enhancement using hybrid algorithms between unsupervised and supervised learning. – Electronics 13(5): 17p.
[28] Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., Fang, B. (2018): Insider threat detection with deep neural network. – In Computational Science-ICCS 2018: 18th International Conference, Wuxi, China, Springer International Publishing 11p.
[29] Yuan, S., Wu, X. (2021): Deep learning for insider threat detection: Review, challenges and opportunities. – Computers & Security 104: 10p.