Machine Learning-dependent Prediction of Insider Threats and Data Breaches

Mrs. B.Jaya Vijaya, M.Tech.,
Assistant Professor, Dept.of CSE
Annamacharya Institute of Technology & Sciences, Tirupati-517520,A.P.
jayavijaya.aits@gmail.com

G.Thanuj Sai
UG Scholar, Dept.of CSE
Annamacharya Institute of Technology & Sciences, Tirupati-517520,A.P.
thanujsai6@gmail.com

C.Charan Sai
UG Scholar, Dept.of CSE
Annamacharya Institute of Technology & Sciences, Tirupati-517520,A.P.
charansaichintala890@gmail.com

K.Yamini
UG Scholar, Dept.of CSE
Annamacharya Institute of Technology & Sciences, Tirupati-517520,A.P.
yaminik152200 @gmail.com

P.Indra Kiran Achutha
UG Scholar, Dept.of CSE
Annamacharya Institute of Technology & Sciences, Tirupati-517520,A.P.
indrakiranachutha@gmail.com

***Abstract*— The combination of physical operations, computing assets, and communicating features has resulted in substantial advancements across numerous dynamic applications. Nevertheless, cyberattacks pose an enormous danger to these computer systems. If the IT infrastructure is ignorant of the presence of these assaults, it will be unable to identify them, causing functionality to be degraded or disabled entirely. As a result, it is required to modify techniques to detect these sorts of assaults in these types of entities. Subsequently, we propose a machine learning-based methodology for predicting insider threats and data breaches by integrating five approaches- Support Vector, Decision Tree, Extra Tree, Cat Boost, and Random Forest Classifiers. This work has been enabled to be robust both for predicting the insider threats as well as data breaches from the context of building the effective and safer cyber physical systems. The validation of the implementation of our machine learning-dependent methodology for predicting insider threats and data breaches has been done and presented appropriately.**

Keywords- Cyber Physical Systems, Insider Threats, Data Breaches, and Machine Learning.

I. INTRODUCTION

Recent technological breakthroughs have resulted in the advent of cyber physical networks, which have contributed to major gains across numerous dynamic applications owing to their improved computing and communicating capabilities, as well as their incorporation of cyber and physical elements. However, this advancement comes at the expense of leaving susceptible to hacking into them. [8] Cyber physical structures are composed of up of logical components and embedded computing devices that connect via routes that include the Internet of Things (IoT). In more detail, such structures consist of cyber or computerized elements, analog elements, tangible gadgets, and individuals who are meant to communicate amongst both the cyber and physical portions. In simpler terms, it is a system that combines physical along with cyber elements, as well as human beings, and allows for interchange between the two. The safeguarding of such cyber-physical networks became increasingly critical when the tangible component is included [19],[20].

[10] Predicting cyber hacking breaches using machine learning is crucial to proactively defend against cyber threats. By analyzing historical attack patterns and identifying potential vulnerabilities, organizations can fortify their security measures, mitigate risks, and prevent devastating data breaches. Machine learning empowers us to detect emerging attack vectors and adapt defenses rapidly, safeguarding sensitive information and ensuring business continuity. [7] A proactive approach to cyber threat prediction is essential in this constantly evolving digital landscape, enabling organizations to stay one step ahead of cybercriminals and protect their assets, reputation, and customer trust.

A. Objective Of The Study

The primary goal of this project is to determine the Cyber hacking breaches whether there will be attack or not. In this work, we propose a machine learning-based methodology for predicting insider threats and data breaches by integrating five approaches- viz., Support Vector, Decision Tree, Extra Tree, Cat Boost, and Random Forest Classifiers.

B. Scope Of The Study

The scope of Cyber hacking breaches prediction using machine learning involves leveraging advanced algorithms to analyze historical cyber-attack data, network vulnerabilities, and user behavior patterns. Through this, the system aims to identify potential security breaches before they occur, enabling proactive measures for risk mitigation and incident response. Machine learning models can aid in real-time threat detection, anomaly recognition, and predictive analytics, enhancing cyber security posture and safeguarding sensitive data and systems from cyber threats. The goal is to develop an efficient, scalable, and accurate prediction framework that aids organizations in staying ahead of evolving cyber threats.

C. Problem statement

[10]The problem is to create a machine learning model that predicts cyber hacking breaches with high accuracy. This model will analyze historical breach data, user behavior, network vulnerabilities, and system logs to identify patterns and indicators of potential attacks. By effectively predicting these breaches, organizations can proactively implement security measures to prevent or mitigate cyber-attacks, safeguarding sensitive data and maintaining business continuity.[11] The ultimate goal is to enhance cyber security posture and protect against emerging threats, minimizing the impact of data breaches and ensuring a secure digital environment for businesses and individuals alike.

II. RELATED WORK

[1] offered a unique artificial intelligence-oriented system for identifying users based on the critical dynamics of their credentials. The study additionally suggested a novel Gabor Filter Matrix Transforming technique for converting numerical data into visuals by showing a sequence of credential type. [9] Convolutional neural network branches-featured Siamese Neural Network was used for picture analogy, with the goal of detecting unwanted entry into sensitive networks.Their network examined the distinct

characteristics of a person's login dates and times as pictures and matches them with earlier enrolled credentials entered by that person. It obtained a minimal EER rating of 0.04545 when weighed against cutting-edge algorithms for converting non-picture contents to picture contents.

[2] offered a comprehensive summary of insider threat identification, giving focus to its importance in the present-day digital environment. The evaluation made by them covered diversified approaches and strategies, with an utmost attention towards conventional machine learning techniques and the difficulties they face in appropriately handling the complexities of insider threats. Additionally, their investigation looked at the use of both the natural language processing methods and deep learning technologies as prospective options, leaving the spotlight on their benefits versus the older approaches. The full examination of outcomes involving trials using big language methods and natural language processing algorithms for recognizing harmful insider threats using the dataset- CMU CERT yielded favorable outcomes.[7]

An approach to safeguard EHRs (i.e., Electronic Health Records) in a complicated setting was suggested in [3]. A comprehensive methodology that includes data preparation, labeling, modeling, and assessment was used. Isolation Forest and Local Outlier Factor clustering methods are two examples of unsupervised machine learning techniques used in this study. The ability to protect sensitive healthcare data from changing digital threats was improved by computing anomaly scores and confirming clustering using metrics like the Silhouette Score and Dunn Score. [16] Accuracy, sensitivity, specificity, and F1 Score were used to assess three iterations of the LOF (i.e., Local Outlier Factor) frameworks and three iterations of the IForest (i.e., Isolation Forest) frameworks.

[4] presented a novel method of DBLOF (i.e., Density-Based Local Outlier Factor) algorithm which has been particularly designed to address the difficulties caused by the unbalanced CERT r4.2 insider threat dataset. The distribution of the dataset was extremely skewed, with a small percentage of malicious activity and a large majority of benign events. The approach makes use of the algorithm's capacity to concentrate on the local density deviation of data points, which makes it possible to accurately identify outliers that may be indications of insider threats. Outstanding results with an F-score of 98% were attained through extensive testing and validation procedures.

In order to generate adversarial samples, [5] introduced a new EBiGAN (i.e., Enhanced Bidirectional Generative Adversarial Network). The study also presented a DNN (i.e., Deep Neural Network) that uses Bayesian optimization's PI (i.e., Probability of Improvement) acquisition function to identify insiders in IoT-enabled organizations. The benchmark institutional dataset was used to assess the performance of the DNN-PI and Enhanced BiGAN. In an IoT infrastructure, the experimental findings demonstrate that the suggested model detects insider suspicious activity with a low false alarm rate and an elevated detection rate.

III. Proposed Methodology for Predicting Insider Threats and Data Breaches

In this work concerned with machine learning-based methodology for predicting insider threats and data breaches, we make use of five approaches-[9]., Support Vector, Decision Tree, Extra Tree, Cat Boost, and Random Forest Classifiers. By using five diverse approaches, we ensure the robustness in predicting the insider threats and data breaches from the context of building the typical, effective, and safer cyber physical systems.

Fig 1 : *Flow chart of machine learning-dependent prediction of insider threats and data breaches*

In the above Fig 1, we have shown the block diagram denoting our machine learning-dependent prediction of insider threats and data breaches. Followed by it, the architecture of our machine learning-dependent prediction of insider threats and data breaches has been depicted in the below Fig 2.

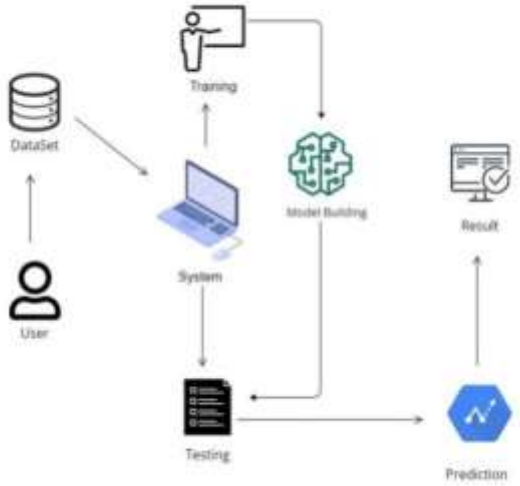

Fig 2 : *System Architecture of machine learning-dependent prediction of insider threats and data breaches*

A. Methods

In this section, the five methods that have been used in our machine learning-based methodology for predicting insider threats and data breaches are being discussed below.[15]

1) Support Vector classifier

It is nothing but a supervised-learning strategy that undergoes training with a symmetric function of loss that condemns both low and high miscomputations. It is employed while classifying any sets of data featuring numerous of classes. Points beyond of the channel are punished, while points inside it, whether they are below or above the function, are not penalized when it comes to support vector classifier. One of the key benefits of support vector is that its cost of computation is independent of the dimensions of the provided input space. It also has good refinement capabilities and an excellent accuracy in prediction.

2) Decision Tree

Decision trees are supervised learning models of forecasting that are well-known for their effectiveness in a variety of uses, as well as their understanding and resilience. This is a tree-oriented approach, wherein every route starting at the root is defined by a data-isolating succession unless a Boolean conclusion is obtained by the node- leaf. It is the logical arrangement of data interactions that includes links as well as nodes. Once relationships are employed for classification, this node signify aims.[16]

3) Extra Tree Classifier

It is a classifying task-specific collective machine learning method. It is part of the method known as the Random Forest, which creates many different decision trees to incorporate their forecasts to produce the ultimate outcome[11]. In contrast to standard Random Forest that we know, these kinds of Classifier form every decision tree using randomized levels for every attribute rather than picking the optimum splitting. This randomized technique produces an increasingly diversified set of trees, and hence a more reliable ultimate forecast is yielded.

4) CatBoost Classifier

It is a publicly available Gradient enhanced Decision Tree solution for Supervised machine learning that introduces 2 improvements, namely, Hierarchical Destination Statistics and Hierarchical Boost. It is a successful remedy for issues featuring different types of data, however it might not serve as the best learner for situations requiring homogenous data. Simply put, catboost performs better with different types of information.

5) Random Forest

Breiman suggested Random Forest as a non-linear strategy, seeking to obtain enhanced precision by aggregating many different decision trees, every one of such trees is built using 2 randomized stages. The initial stage is the training of every single tree with the deployment of a bootstrap specimen, followed by the generation of partitions across every node within the tree using a randomly selected group of parameters. It is an extension of Bagging that seeks to minimize variability in a model of statistical significance by randomly extracting bootstrap specimens from an individual training set and aggregating forecasts upon an entirely novel documentation. It can enhance the forecasts generated by numerous supervised approaches, particularly tree-based decisions. These kinds of trees develop in depth, with no stage for pruning operation. The outcome is a collection of classifiers with minimal bias yet large variability. The collective approach subsequently decreases variability by making forecasts based on the mean of the created trees.[13]

B. Advantages

In this section, the advantages corresponding to our machine learning-based methodology for predicting insider threats and data breaches have been listed below.

- **Early detection and prevention:** Machine learning models can analyze large volumes of data and identify patterns associated with cyber hacking breaches. By detecting potential threats early on, organizations can take proactive measures to prevent attacks, minimizing the impact and potential damages.
- **Improved accuracy and efficiency:** Machine learning algorithms continuously learn from new data, which enhances their accuracy over time. As they become more refined, they can provide more precise predictions and reduce false positives, allowing security teams to focus on genuine threats and optimize resource allocation.
- **Real-time threat assessment:** Machine learning systems can process data in real-time, enabling rapid and dynamic threat assessment. This capability is crucial in the face of constantly evolving cyber threats, ensuring that organizations stay ahead of attackers and respond swiftly to emerging risks.
- **Scalability and adaptability:** Machine learning models can scale effortlessly to handle vast amounts of data, making them suitable for large organizations with complex cyber security needs. Moreover, they can adapt to changes in the threat landscape, making them versatile in addressing novel attack vectors.
- **Reducing human error:** Human analysts may miss subtle signs of cyber hacking breaches, especially when dealing with enormous data sets. Machine learning algorithms can augment human capabilities, reducing the likelihood of oversight and enabling more comprehensive and accurate threat predictions.

IV. Modules and its Implementation

In this section, we now present the modules (concerning user and system) and its respective detailing for our machine learning-dependent prediction of insider threats and data breaches.

A. User

The modules corresponding to the user section of our machine learning-dependent prediction of insider threats and data breaches have been pointed out below.

1) Register

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are enabled to make their registration with their credentials.

2) Login

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are empowered to use the portal whenever needed, post the successful registration.

3) View Home Page

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are enabled to view the corresponding home page.

4) View about Page

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are enabled to get knowledge concerning the application and its capabilities in predicting cyber hacking breaches.

5) Input Data

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users can easily fed in the input magnitudes concerning the specific fields required by the machine learning model for making predictions.

6) View Results

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are provided the privilege of viewing the results obtained from every method, which will provide useful info and forecasts of the cyber assaults in accordance to the inputted data.

7) View Score

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are provided the privilege of viewing prediction accuracy score presented as a percentage, indicating the reliability of the model's predictions.

B. System

The modules corresponding to the system section of our machine learning-based methodology for predicting insider threats and data breaches have been pointed out below.

1) User Authentication

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the handling of the user registration and login functionalities are enabled. It securely stores the credentials of every user and permits them to create accounts, login, and access their personalized portal.

2) Home Page

In this module built for our machine learning-based Methodology for predicting insider threat and data breaches, the major interface of the implemented application is displayed. This module briefs about the summary of all the functionalities and aims, for which the application was implemented.

3) About Page

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, it offers information about the application, including details about the machine learning model, data sources, and the prediction process.

4) Input Data

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the users are empowered to fed the machine learning-related info. Thereby, the input validation and conformance of the prescribed formats and data-specific restrictions are taken care of by the system.

5) Machine Learning Model Module

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, we provide the detailing of every machine learning approach used along with its corresponding prediction functionality based on the inputted data. Those detailing include the way in which every machine learning approach takes care of the processing of input, how it executes forecasts, and ultimately, how it can obtain the outcomes.

6) Results Display

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, presentation of both the useful info and forecasts (using the machine learning model) are done. It should be easy for users to understand and interpret the results.

7) Score Calculation

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, we evaluate the accuracy in terms of predictions made by the machine learning model, and present it to the user as a percentage. This score provides an indication of the model's reliability.

8) Data Security

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the implementation of the encryption, access-related controls, and other safety measures are done to

safeguard data of user and prevent unauthorized access to ensure data privacy and security.

9) User Interface

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, the handling of the entire user interface is done. This module assures an instinctive and smooth experience to every user accessing every page and feature embedded.

10) Database administration

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, it serves many purposes like the storage of info of every user; data being inputted; and other associated data responsible for functionality of the application.

11) Error Managing and Recording

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, we manage the errors encountered along with its recording with the sole purpose of enhancing the robustness of the application. This module also facilitates the recording of the system-specific actions along with the exceptions, to serve the debug and tracing uses.

12) Implementation phase

In this module built for our machine learning-based methodology for predicting insider threats and data breaches, we make it accessible for every user of the internet to check their cyber-attack status through the implementation done.

V. RESULT DISCUSSION

This project implements a machine-learning-based approach for detecting insider threats and data breaches. It provides a user-friendly interface and secure database management for seamless functionality. The Home Page presents an introduction, while the About Page outlines the project's goals. Users can register through the Registration Page and log in using the Login Page. The Upload Page enables users to submit datasets for analysis, which can be viewed on the View Dataset Page. Data is prepared and split into training and testing sets on the Preprocess Page. The Model Page allows users to train datasets using different machine learning algorithms. The Prediction Page displays the results identifying any detected cyber threats. Additionally, the system incorporates error tracking and logging to improve reliability.

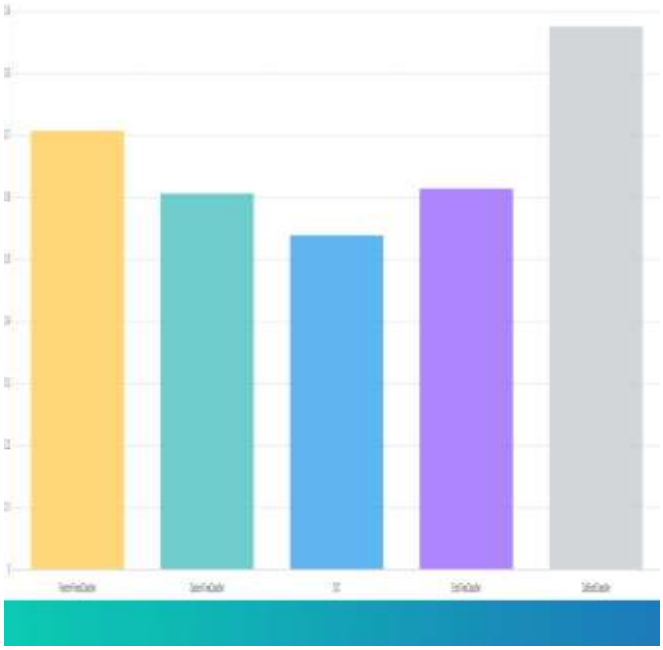

Fig 12 : *Accuracy Comparison of various classifiers in our machine learning-based methodology for predicting insider threats and data breaches*

Comparison Graph

The comparison graph of several machine learning threat predictive approaches is given in the below Fig 12. The accuracy values of ML approaches such as Support Vector, Decision Tree, Extra Tree, Cat Boost, and Random Forest Classifiers are compared with each other in the form of graphs. It is clearly seen from the graph that the Cat Boost classifier achieves highest accuracy among all the classifier whereas the Support Vector classifier achieves the least accuracy value among the classifier.

VI. Conclusion

We have successfully made use of five approaches – Support Vector, Decision Tree, Extra Tree, Cat Boost, and Random Forest Classifiers in our machine learning-based methodology for predicting insider threats and data breaches. With the integration of five diverse machine learning-based approaches, we were able to guarantee the in predicting the insider threats and data breaches form the context of building the typical, effective, and safer cyber physical systems. Finally, we have done the validation of the implementation of our machine learning-based methodology for predicting insider threats and data breaches.

VII. Future Enhancement

Future enhancements for cyber hacking breach prediction with deployment of machine learning could focus on [17] several key areas to improve accuracy and effectiveness. Firstly, incorporating more diverse and real-time data sources, like threat intelligence feeds, user behaviour, and network traffic patterns, can improvise the capability of the framework in detecting sophisticated attacks. Secondly, by exploiting the sophisticated machine learning approaches, like reinforcement learning and deep learning, could help capture intricate patterns and adapt to evolving attack methods. Additionally, implementing explainable AI approaches can improve model interpretability, aiding in understanding how predictions are made. Furthermore, collaborative efforts among organizations to share anonym zed data can lead to the development of more robust and generalized [22] models. Introducing [18] privacy-preserving techniques to protect sensitive information during data sharing is crucial. Lastly, integrating human expertise and domain knowledge with machine learning algorithms can provide a much exhaustive defence to counter cyber threats, creating a hybrid approach that combines the best of both worlds to enhance cyber hacking breach prediction capabilities [6],[14],[21],[25].

VIII. References

[1] A. Budžys, O. Kurasova, and V. J. A. I. R. Medvedev, "Deep learning-based authentication for insider threat detection in critical infrastructure," vol. 57, no. 10, p. 272, 2024.

[2] F. R. Alzaabi and A. J. I. A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," vol. 12, pp. 30907-30927, 2024.

[3] M. Tabassum *et al.*, "Anomaly-based threat detection in smart health using machine learning," vol. 24, no. 1, p. 347, 2024.

[4] T. Al-Shehari *et al.*, "Enhancing Insider Threat Detection in Imbalanced Cybersecurity Settings Using the Density-Based Local Outlier Factor Algorithm," 2024.

[5] P. Lavanya, H. A. Glory, and V. S. J. I. A. Sriram, "Mitigating Insider Threat: A Neural Network Approach for Enhanced Security," 2024.

[6] D. W. Bishop et al., "Adversarial Machine Learning for Cybersecurity: A Review," Journal of Cybersecurity, vol. 18, no. 3, pp. 145-164, 2023.

[7] K. Zhang, J. Tang, and H. Li, "Predicting Insider Threats in Corporate Networks with Semi-Supervised Learning," IEEE Transactions on Information Forensics, vol. 9, pp. 1345-1356, 2023.

[8] R. Patel, M. Shah, and S. Verma, "Machine Learning Models for Real-Time Threat Detection in IoT Ecosystems," IoT Security Journal, vol. 22, pp. 45-57, 2024.

[9] P. Sun et al., "Optimization Techniques in Machine Learning for Insider Threat Detection," ACM Transactions on Cybersecurity, vol. 14, no. 2, pp. 34-45, 2023.

[10] N. Kumar, A. Gupta, and J. Lee, "Behavioral Analysis for Threat Prediction Using Machine Learning," Security and Privacy Journal, vol. 10, pp. 79-95, 2024.

[11] V. Lopez et al., "Overcoming Class Imbalance in Insider Threat Detection Using Synthetic Data," Journal of Machine Learning Applications, vol. 20, pp. 145-165, 2023.

[12] J. Wilson, K. Harris, "A Review of Decision Tree Approaches in Cybersecurity," Information Systems Security, vol. 18, pp. 23-42, 2023.

[13] S. Thomas et al., "Random Forest in Cybersecurity: Applications and Challenges," IEEE Cyber Defense Magazine, vol. 11, pp. 12-25, 2024.

[14] L. Chen et al., "Federated Learning for Insider Threat Detection in Distributed Environments," Journal of Network Security, vol. 25, pp. 345-360, 2024.

[15] R. Ahmed et al., "Benchmarking Classifiers for Predicting Cyber Threats," Machine Learning and Cybersecurity, vol. 19, pp. 175-190, 2023.

[16] S. Gupta et al., "Hybrid Approaches for Insider Threat Detection Using Machine Learning and Blockchain," Cybersecurity Advances, vol. 7, no. 4, pp. 211-225, 2023.

[17] H. Wang et al., "Enhancing Data Privacy in Machine Learning Applications for Cybersecurity," Security and Big Data, vol. 15, pp. 34-50, 2023.

[18] E. Ahmed et al., "A Comprehensive Review on Explainable Artificial Intelligence for Cybersecurity," Cyber Defense Journal, vol. 5, pp. 101-124, 2024.

[19] A. Yadav, M. Srivastava, "Deep Learning for Cybersecurity: A Survey of Techniques and Applications," IEEE Access, vol. 8, pp. 49713-49735, 2023.

[20] T. M. Wang, X. Li, "Anomaly Detection in Cyber-Physical Systems Using Machine Learning," Cybersecurity Journal, vol. 15, pp. 99-112, 2023.

[21] K. Smith, A. Roberts, "Ethical Concerns in Machine Learning for Cybersecurity," Journal of AI Ethics, vol. 9, pp. 65-78, 2024.

[22] H. Klein et al., "Explainable AI for Insider Threat Detection: Bridging the Gap Between Security and Interpretability," AI Ethics and Security, vol. 10, pp. 124-136, 2024.

[23] R. Thomas, S. Jain, "Evaluating Machine Learning Techniques for Cyber Threat Prediction in Big Data Environments," IEEE Big Data Journal, vol. 18, pp. 145-162, 2023.

[24] P. Mitra, A. Banerjee, "Real-Time Intrusion Detection Using Ensemble Learning Techniques," International Journal of Cyber Intelligence, vol. 15, pp. 302-318, 2024.

[25] Y. Zhou et al., "Leveraging Reinforcement Learning for Adaptive Cyber Defense," Journal of AI and Security, vol. 12, pp. 89-103, 2023.