

American Journal of Economics and Business Management

Vol. 7 Issue 12 **| pp.** 1857-1880 **| ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Predictive Cybersecurity Analytics for Insider Threat Detection in Zero-Trust Enterprise Environments

Mahbub Hasan[1], Mohammad Masudur Rahman[2], Rabia Akter Sukhi[3], Fahmida Akter[4], Mohd. Salman Hossain Bhuiyan[5]

1. BSc in Information Technology, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh
2. Department of Marine Science and Oceanography, Florida Atlantic University, USA
3. Masters in Management Information System, International American University, USA
4. Bachelor of Science in Computer Science Engineering, Daffodil International University, Bangladesh
5. Bachelor of Science in Computer Science and Engineering, East West University, Bangladesh

Correspondance: mahbub0016@gmail.com[1], rahmanmasud89@gmail.com[2], kazirabia01@gmail.com[3], a.fahmida42@gmail.com[4], mohd.salmanhossain@gmail.com[5]

Abstract: Insider threats are one of the most serious challenges in today's cyber world as enterprise cybersecurity becomes increasingly complex due to the fast-paced adoption of cloud computing, hybrid working models and digital transformation. Internal threats are posed by users with valid access to the network and are thus hard to identify with traditional security controls as they are carried out by authorized users. While Zero-Trust Enterprise Architecture is about constant verification and least-privilege access, Zero Trust also needs to be intelligent to proactively detect suspicious user activity before security incidents happen. This study is aimed at developing a predictive cybersecurity analytics framework for insider threat detection in a Zero-Trust enterprise environment based on machine learning techniques and behavioral analytics. This study leverages the CERT Insider Threat Dataset which includes enterprise email communication records that track user interactions, communication trends, device interactions, attachment activity, and temporal interactions. In the data preprocessing stage, any indicators of activities related to insider threats are identified. In the data preprocessing stage, the meaningful indicators of insider threat activities are extracted. Several machine learning models such as Random Forest, Support Vector Machine (SVM), Decision Tree, XGBoost and isolation forest are used to create predictive models that identify if there is any normal user behavior or if there are any anomalous or potentially malicious activity. To guarantee accurate and solid detection, model performance is assessed by Accuracy, Precision, Recall, F1-score, Receiver Operating Characteristic Area under the Curve (ROC-AUC) and False Positive Rate. The suggested model combines the predictive analysis capabilities of AI with Zero-Trust security principles, allowing for ongoing behavioral monitoring, risk evaluation and threat prediction. The outcomes of these are that it enables better accuracy in detection, fewer false alerts, better security resilience for enterprise and assistance in real-time cybersecurity decision making. In this research, the authors share their experience of making predictive cybersecurity analytics an effective way to bolster ZZEE by leveraging data-driven insights to analyze behaviour and machine learning, and how this enhances the security of modern enterprise networks and reduces the likelihood of insider threats.

Keywords: Predictive Cybersecurity Analytics, Insider Threat Detection, Zero-Trust Enterprise Environments, Machine Learning, Behavioral Analytics and CERT inside Threat

Citation: Hasan, M., Rahman, M. M., Sukhi, R. A., Akter, F., Bhuiyan, M. S. H. Predictive Cybersecurity Analytics for Insider Threat Detection in Zero-Trust Enterprise Environments. American Journal of Economics and Business Management 2024, 7(12), 1857-1880.

Received: 30th Oct 2024
Revised: 15th Nov 2024
Accepted: 05th Dec2024
Published: 30th Dec 2024

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

A. Background

Enterprises have experienced digital transformation at an unprecedented pace, which has shifted the way enterprises deal with information systems, cloud services, and inter-connected networks. These technological advances have resulted in efficient operations and agile business, but also added to the cybersecurity threat environment. Insider threats are among the most challenging cyber threats to detect due to their source of origin from an authorized user who has legitimate access to the resources of an organization. Insider threats can be caused by malicious intent, negligence or compromised user accounts which can result in data breaches, the theft of intellectual property, financial losses and reputational damage [1]. Traditional security technologies, such as firewalls, intrusion detection systems and traditional access control models, generally just try to safeguard against external attacks and are typically incapable of detecting subtle changes in behavior by insiders. To overcome those, Zero-Trust Enterprise Architecture has come into existence as a new cyber security strategy that aims to "never trust, always verify." With Zero Trust, all users, devices and applications are continually authenticated before access is granted or maintained to organizational assets. Unfortunately, it's not enough to simply be authenticated to tell when a new insider threat is occurring as attackers may be authorized but still conduct unauthorized operations without generating the usual security alarms. For this reason, predictive cybersecurity analytics has attracted a lot of attention these days as an intelligent solution for real-time monitoring of user activity and foreseeing possible insider attacks before they can cause appreciable damage [2]. Machine learning and behavioral analytics can be used to identify patterns, anomalies, and make proactive risk assessments out of vast enterprise data to uncover hidden elements in cybersecurity systems. Predictive models can be used to study communication patterns, access patterns and activities and facilitate more effective detection of suspicious activity while minimizing false alarms. As a result, predictive cybersecurity analytics combined with Zero-Trust principles is a promising approach in today's enterprise environment for providing a more robust security posture, proactively monitoring, adapting to threats, and detecting insider threats.

B. Zero-Trust Enterprise Environments Predictive Cybersecurity Analytics

As cyber threats are getting smarter, organizations are moving from reactive security measures to predictive and intelligence-based cybersecurity. Predictive cybersecurity analytics uses statistical analysis, machine learning and behavioral modeling to predict potential security events before they happen. Predictive models continually analyze enterprise data to look for indicators of suspicious activities—before the attack even occurs. In Zero-Trust Enterprise Environments, continuous verification and behavioral monitoring work hand in hand, to determine the user's trust on a continuous basis rather than relying on the initial verification [3]. The behavioral characteristics of emails received and sent to, from, and within the enterprise, device usage, how often people use them, the way they communicate with one another, and attachment behaviors offer good clues to enterprise insider threats. By combining the use of predictive analytics and Zero-Trust Architecture, security teams can prioritize security activities for high-risk users, automate security responses and enhance organizational resiliency against the changing nature of insider attacks without compromising operational efficiency.

C. Problem Statement

Authorized users have legitimate access to enterprise systems, making insider threats one of the toughest problems in cyber security, as these users can operate against its security controls. While Zero-Trust Enterprise Architecture can improve authentication and access management by continuously verifying access, this approach does not give a foolproof warning when it comes to insider threats and their patterns. Current security solutions often produce too many false-positive alerts, or only detect threats after considerable damage has been done [4]. The amount of enterprise communication data is growing and manual monitoring is not possible. Thus, an intelligent predictive cyber

security analytics framework, which relies on machine learning and behaviour analytics, to effectively detect insider threats, make proactive decisions and improve the effectiveness of Zero Trust Enterprise Environments, is necessary.

D. Study of the Study

The objectives of this study is to

- To explore the benefits of predictive cybersecurity analytics to identify insider threats in Zero-Trust Enterprise Environments.
- To preprocess and analyses enterprise email communication data from CERT Insider Threat Dataset.
- To create predictive machine learning models to detect abnormal behavior of users that could be related to insider threats.
- To evaluate the performance of various machine learning algorithms with respect to commonly used cybersecurity metrics.
- To connect predictive behavioral analytics to Zero-Trust security principles to continuously assess risk.
- To assess the proposed framework on the accuracy of detection, reduction of false-positive and overall cybersecurity performance.

E. Research Questions

The following research questions are highlighted in this study:

- What role can predictive cybersecurity analytics play in an insider threat detection strategy in a Zero-Trust Enterprise Environment?
- What is the best machine learning algorithm to predict the most accurately insider threat detection from enterprise behavioral data?
- What behaviors, gleaned from enterprise email communications, play the largest role in predicting insider threats?
- What is the value of combining predictive analytics with Zero-Trust security principles in the decision-making process to prevent cyber-attacks and minimize the number of false-positive alerts?

F. Significance of the Study

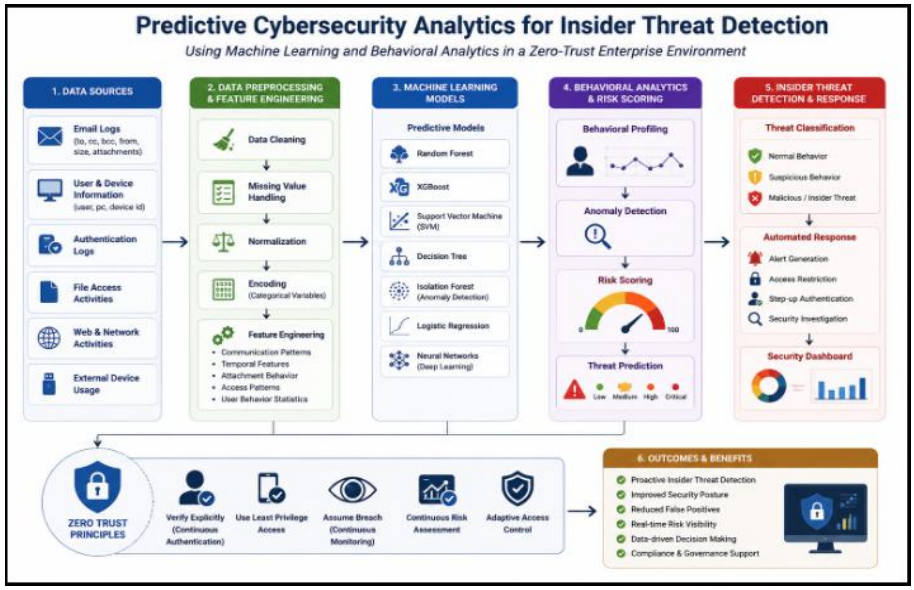
This study is important as it tackles one of the most pressing challenges in the face of modern organizations with regard to cybersecurity issues – timely detection of insider threats. In today's digital era, where enterprises are increasingly migrating to the cloud, leveraging remote working capabilities and digital collaboration platforms, there is a need for security solutions that go beyond perimeter-based defenses to protect the sensitive organizational resources [5]. This study proposes a cybersecurity framework that combines predictive cybersecurity analytics with Zero Trust Enterprise Architecture, thereby helping to create an intelligent security framework that continuously assesses user behavior and detects potential insider threats before they become an issue. The proposed architecture shows how machine learning methods and behavioral analysis can enhance the accuracy of insider threat detection and minimize false-positive alerts that are common and cause security analysts to be flooded with alerts. The results of this research will be useful for cybersecurity practitioners, security operation centers, enterprise system administrators and decision makers on how to enhance enterprise resilience by taking a proactive approach to threat intelligence [6].. This study provides an effective solution for enterprise email communication data continuous verification in Zero-Trust environments, highlighting the practical solutions of enterprise email communication data for behavioral profiling and predictive risk assessment. Sculli's research builds on the growing field of predictive cybersecurity analytics by integrating machine learning, behavioral analytics, and Zero-Trust security principles in a single framework. This study also sets the groundwork for future research with multimodal enterprise datasets, deep learning methods, and adaptive cyber security systems. The proposed predictive model can help

organizations bolster their security posture, refine their incident response strategies, and make informed decisions in their cybersecurity initiatives in today's evolving enterprise landscape.

Literature Review

A. Predictive Cybersecurity Analytics for Insider Threat Detection

Because there are growing incidents of insider threats and their sophistication, researchers have become motivated to create predictive cybersecurity analytics that can detect malicious activities in advance of causing major damage to the organization. Predictive Cyber Security Analytics differs from traditional cyber security methods, which are based on known attack signatures or rule-based detection patterns, by using machine learning, statistical models and behavioral analysis to detect previously unknown patterns related to abnormal user behaviour [7]. By taking this proactive approach, it will be possible for the organization to continually monitor the activities of users and estimate the probability of future security incidents – not just react after they have taken place. Past research has shown that user behavior analytics can be useful in detecting insider threats through user communication patterns, login activities, and file access behavior and system usage characteristics. Various machine learning algorithms like Random Forest, Support Vector Machine (SVM), Decision Tree, Gradient Boosting, and Isolation Forest have been used extensively to differentiate between regular user activities and suspicious behaviour [8]. Temporal behavior analysis, communication frequency, attachment usage, and anomaly scoring, among other feature engineering techniques, have proven to be highly effective in achieving a balance between predictive accuracy and the number of false-positive alerts. In recent times, the benefits of supervised and unsupervised learning approaches have been emphasized for identifying known and unknown insider threats has also been brought to the fore. Ensemble Learning methods have been shown to be more effective by combining the best attributes of several predictive models to achieve better classification accuracy and generalization. Explainable artificial intelligence (XAI) techniques have been adopted to increase the transparency of the models, allowing cybersecurity analysts to comprehend how threats are being predicted and to make informed decisions. Alongside these developments, there are numerous existing solutions based on single behavioral cues and many which are not fully integrated with enterprise-wide security architectures. Hence, there is a need for broader predictive models that are able to continuously monitor user interactions and provide proactive insider threat detection in today's enterprise environments.

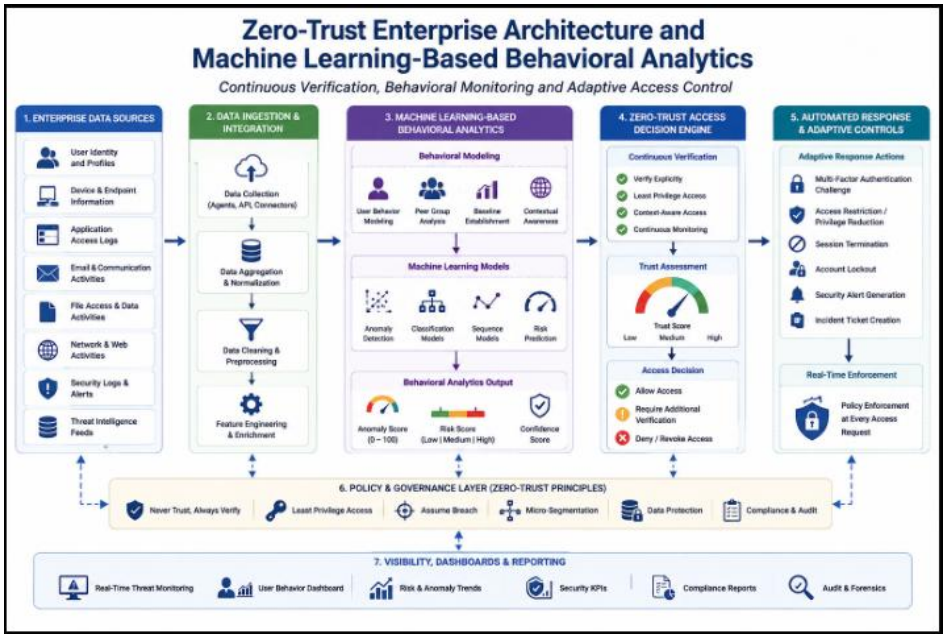


This flowchart shows a predictive cyber security analytics framework for insider threat detection within a Zero-Trust enterprise

The predictive cybersecurity analytics flow chart is a framework in a flowchart for detecting insider threats in Zero-Trust enterprise environments. Collecting data from the enterprise email logs, authentication records, file access activities, network traffic, devices of users and applications from external devices [9]. The data is preprocessed which involves data cleaning, handling missing values, normalizing the data, encoding, and feature engineering. Machine learning algorithms like Random Forest, XGBoost, Support Vector Machine, Decision Tree, Isolation Forest, Logistic Regression and Neural Networks detect anomalies and assign them risk scores based on user behavior. It categorizes threats, automatically triggers security responses, incorporates Zero-Trust principles, and increases the effectiveness of proactive insider threat detection, continuous monitoring and enterprise cybersecurity resilience.

B. Zero-Trust Enterprise Architecture and Machine Learning Based Behavioral Analytics

In the modern digital landscape where external and internal threats are ever present, Zero-Trust Enterprise Architecture (ZTEA) has become one of the most significant cybersecurity philosophies for securing digital environments. Whereas traditional perimeter-based security assumes that internal users can be trusted, Zero Trust works on a premise of "never trust, always verify" and continuously authenticates, authorizes, and validates individuals, devices, and applications that want to access the organization's resources [10]. The security philosophy of this approach minimizes implicit trust and considerably decreases chances for unauthorized access due to compromised credentials and insider misuse. Machine learning has become a must have component for improving Zero-Trust concepts with the capability to continuously monitor behaviour and adapt risk assessment. Instead of just using authentication data, behavioral analytics can analyze the way users interact with the system, the patterns of communication, the frequency of access, device usage, and other context information to generate dynamic trust scores. These trust assessments can be continuously updated based on new behavioral data collected, enabling organizations to detect deviations from behavioral baselines in real time. These features enable automated security measures such as access controls, extra authentication needs, security checks before potentially harmful actions are taken. The latest research shows that combining machine learning and Zero-Trust Architecture enhances detection accuracy and efficiency, thereby decreasing the workload of manual monitoring and focusing resources on high-risk users. Deep learning-based models, anomaly detection methods, and ensemble learning approaches have shown great potential in detecting subtle insider activities that might not be detected by traditional security systems [11]. But there are still issues to address with respect to model interpretability, scalability, preservation of privacy, and availability of realistic enterprise datasets. Further studies are required to create new, predictive cybersecurity frameworks that integrate behavioral analytics, machine learning, and Zero-Trust security principles in order to achieve accurate, scalable and explainable insider threat detection in today's enterprise environment.



This flowchart illustrates Zero-Trust Enterprise Architecture plus machine-learning based behavioral analytics for cybersecurity

The flowchart depicts a Zero-Trust Enterprise Architecture with machine learning-based behavioral analytics for proactive cybersecurity. The framework starts by capturing enterprise data from user identities, devices, application logs, email communications, file access, network activity, security logs and threat intelligence feeds [12]. Data is processed into anomaly detection, classification, sequence analysis, and risk prediction using machine learning models and feature engineering is performed to aggregate, clean, normalize and transform the data. The Zero-Trust decision engine, which is based on behavioral analytics, continuously verifies users, assigns trust scores and grants access privileges. Automated security responses implement adaptive controls, and governance policies and monitoring dashboards provide continuous protection, compliance, and organizational cybersecurity resilience.

C. Empirical Study

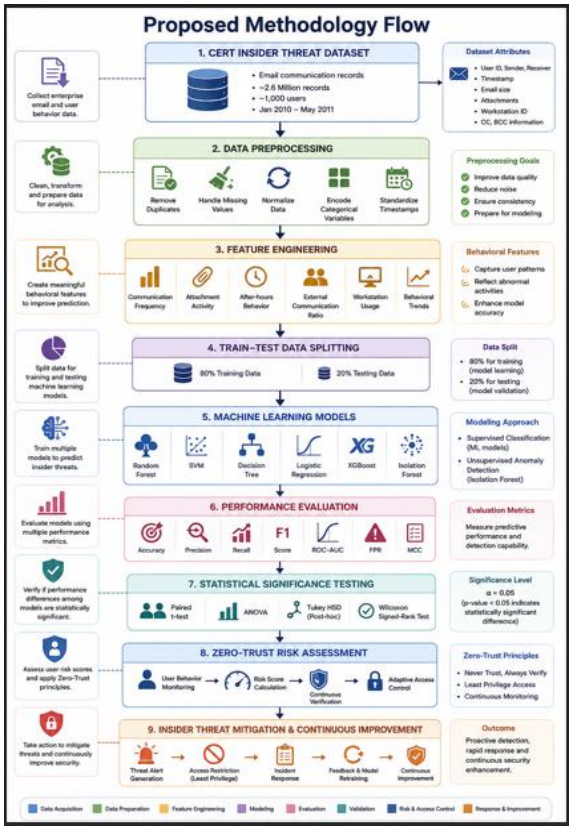
In their article titled "Developing Adaptive Cybersecurity Architectures Using Zero Trust Models and AI-Powered Threat Detection Algorithms", Ejeofobiri, Adelere, and Shonubi discussed how to apply Zero Trust Architecture (ZTA) and artificial intelligence for bolstering the cyber security of enterprises in the face of an ever-changing threat landscape. The authors stated that existing perimeter security approaches are not up to the task of securing contemporary organizations due to the growing use of cloud services, remote working, and evolving attack methods. The adaptive cybersecurity architecture they propose is based on the principle of "never trust, always verify", which involves continuous authentication, least-privilege access control, and real-time monitoring of users and devices [1]. The study also integrates AI technologies such as machine learning, anomaly detection, behavioral analytics, and natural language processing (NLP) to enhance threat detection and security response automation. Moreover, the researchers pointed out the need for integrating Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA) and automated incident response systems in improving cyber resilience and decreasing the response time. Their study showed that using AI and Zero Trust Architecture contributes to better insider threat detection, lateral movement detection, and the reduction of false-positive alerts, as well as zero-day attacks. The study is important for the current research because it showed, on a theoretical and practical level, the benefits of predictive analytics and intelligent behavioral monitoring in the context of adaptive cybersecurity and proactive insider threat detection in Zero-Trust Enterprise Environments.

Ghulam Freed and Mason Jackson in the study, "Zero Trust Architecture in AI-Driven Cybersecurity: A Machine Learning Perspective" explored how artificial intelligence and machine learning can augment Zero Trust Architecture (ZTA) to enhance enterprise cybersecurity. According to the authors, Zero Trust is based on three pillars: continuous verification, least privilege and micro-segmentation, allowing organizations to reduce security risks and threats of modern cyber-attacks. They said AI-based cybersecurity works in tandem with Zero Trust by utilizing behavioral analytics, anomaly detection, and predictive modeling to detect suspicious behavior and trigger automatic security actions in real time. The study also showcased the application of machine learning techniques in enhancing user and device recognition, endpoint protection, and network security through ongoing analysis of user and device behavior [2]. The authors reviewed some of the challenges faced in implementing the intelligent security system, such as adversarial attacks against the AI models, data privacy issues, and the computational complexity required for implementing intelligent security systems. For the future, they also noted emerging technologies like federated learning, explainable AI and blockchain as potential tools to bolster future Zero Trust deployments. The results show that the deployment of AI-powered analytics in conjunction with Zero Trust Architecture has a substantial positive impact on insider threat detection, advanced persistent threat detection, ransomware detection and the ability to adapt and proactively protect against threats. This study offers valuable support to the current study by showing predictive machine learning techniques can be employed to improve behavioral monitoring and insider threat detection in Zero-Trust Enterprise Environments.

In the study AI-driven Threat Detection in Zero Trust Environments, Runchu Zichen explored how artificial intelligence can help strengthen threat detection in Zero Trust security architectures. The authors explained the Zero Trust model is centered on the "never trust, always verify" principle, which means that all users and devices that are trying to access enterprise resources should be continually authenticated and authorized. The research highlighted the crucial role of AI in enhancing the Zero Trust framework, noting how machine learning, behavioral analytics, and anomaly detection capabilities can help detect suspicious activity in real-time, thereby boosting the overall level of cybersecurity. Unlike perimeter security strategies, AI-enabled systems can learn about new attack trends, and identify advanced insider and external threats that could evade traditional security measures [3]. The paper also pointed to the potential for AI to automate threat response processes, which can help to lighten the security team's load and enhance the efficiency of the response. The author covered implementation issues, such as ethics, data privacy and the need for human oversight to ensure accurate use of AI for decisions. Together, the results validate the power of AI and Zero Trust Architecture to boost proactive threat detection, increase enterprise cybersecurity resilience, and enable ongoing risk assessment. This study offers significant reinforcement for the current research and emphasizes the need for predictive cybersecurity analytics and intelligent behavioral monitoring to enable the successful detection of insider threats in a Zero-Trust Enterprise Environment.

2. Materials and Method

The method used for this study is quantitative and experimental to create a predictive cybersecurity analytics framework for insider threat detection in Zero-Trust Enterprise Environments. The methodology consists of data collection, data preprocessing, feature engineering, machine learning model development, statistical significance testing, and evaluation of the models [13]. The highest-performing predictive model flows into a Zero-Trust security framework for ongoing behavioral monitoring, real-time risk analysis, adaptive access control and proactive insider threat detection to enhance enterprise cybersecurity risk resilience and decision-making.



This flowchart shows the proposed methodology for predictive insider threat detection in Zero-Trust environments

The flowchart outlines the proposed approach for the creation of a predictive cybersecurity analytics framework for insider threat detection in Zero-Trust Enterprise Environments [14]. The process starts with acquiring behavioral data from CERT Insider Threat Dataset, then it is followed by data preprocessing and feature engineering to enhance the quality of the data and derive meaningful behavioral indicators. The data is then divided into training and testing sets and various machine learning algorithms are created and tested. Validation of comparative performance of the models is done by statistical significance testing [15]. This top performing model is embedded within a Zero-Trust risk assessment framework to enable ongoing verification, adaptive access control, proactive insider threat mitigation, and ongoing cybersecurity enhancement.

A. Research Design

The research design for this study is quantitative, experimental, and development and evaluation research. The research design employed in this study is quantitative, experimental, and development and evaluation research [16]. The research utilizes supervised machine learning and anomaly detection methods to detect malicious and abnormal user activities based on the information of enterprise communication data. The methodology involves a systematic process of data collection, preprocessing, feature engineering, model development with machine learning approaches, statistical validation, and evaluation of models. The CERT Insider Threat Dataset is the main data source since it provides realistic enterprise email communication logs, which represent employee behavioral activities. Standardized cybersecurity performance metrics allow objective comparisons of predictive models using quantitative analysis. The proposed approach continuously monitors patterns of behaviors, forecasts potential insider threats and provides adaptive security decisions aligned with Zero Trust principles [17]. The study will combine behavioral analytics with machine learning to enhance early threat detection, minimize false-positive alerts, and improve the security resilience of organizations. The experimental design also allows for the replication, transparency and scalability of the

design, which makes it suitable for implementation in a modern enterprise cybersecurity environment.

B. Research Framework

The research plan is broken down into six phases that will closely follow one another and aim to detect insider threats accurately by means of predictive cybersecurity analytics. Initially, enterprise behavioral data are collected from the CERT Insider Threat Dataset [18]. These data undergo pre-processing to eliminate duplicate records, fill in missing information, clean up the data time and convert categorical data into machine-readable formats. The data is then summarized and analyzed to create relevant behavioral metrics such as communication frequency, attachment activity, after hours email activity, external communication ratio, workstation usage and user interaction diversity (or diversity of communications). After preprocessing, 80% of the data is designated for training and 20% for testing. Various machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, Logistic Regression, XGBoost, and Isolation Forest are used for training to classify the normal and suspicious behavioral activities. The accuracy, precision, recall, F1-score, ROC-AUC, Matthews Correlation Coefficient (MCC), and False Positive Rate are used to evaluate the developed models [19]. The differences among the predictive models are then tested for statistical significance to see if they are meaningful. Lastly, the top-performing model is incorporated into a Zero-Trust security architecture with ongoing behavioral risk scoring that enables adaptive authentication, least-privilege control and continuous verification. The proposed architecture allows for the prediction of insider threats in advance, as well as enhanced intelligence cybersecurity by monitoring the behavior of users.

C. Dataset Description

This study uses the CERT Insider Threat Dataset, one of the commonly used benchmark data sets for insider threat detection research. This data set includes enterprise email communications data from around 1,000 enterprise users spanning from January 2010 to May 2011, encompassing more than 2.6 million email transactions [20]. Several attributes of the behavior are recorded in each record, including unique email identifiers, timestamps, user identifiers, workstation identifiers, sender and recipient addresses, CC and BCC recipients, email size, and attachment information. The data set includes realistic enterprise communication behavior, which can be used for behavioral profiling and predictive analytics. With the availability of temporal information, one can analyses user activities over time, and sender–receiver relationships enable communication network analysis. The use of attachments, email, the identification of workstations and the diversity of communication are useful measures to identify unusual insider activity. These properties can be used to extract meaningful features from behavior that enhance the performance of the predictive models. These were chosen as they are the most suitable data for a CERT setting and have been widely used in cybersecurity research with a focus on insider threat detection. It provides a detailed description of its behavior at a large scale, which is useful for feature engineering, anomaly detection, machine learning classification, and ongoing behavior monitoring [21]. The dataset fits well into the Zero-Trust security paradigm, as it contains enough information about user activity to respond to the dynamic risk assessment and continuous user behavioral verification.

D. Data pre-processing and feature engineering

Data Preprocessing is carried out to enhance the quality of data sets before predictive modelling. First, duplicate records, inconsistent observations and observations which are missing are detected and eliminated, to make sure that there are no redundant records and that the analytical reliability is enhanced [22]. The missing values dealt with using appropriate methods for imputation based on the type of attribute. All time stamp variables are converted to standard date time formats to enable time based behavioral analysis. Label Encoding and One-Hot Encoding are used for processing categorical variables such as user identifiers, workstation IDs and communication addresses to facilitate machine learning analysis. Min-Max Scaling or Standardization is applied to

numerical variables, like the size of the email or the number of attachments, so as to reduce the differences in the size of the features and improve the convergence of the algorithm. After preprocessing, feature engineering is carried out to create behavioral indicators better to represent insider activities. These engineered variables include: Frequency of email received daily, frequency of email received after hours, rates of attachment use, average size of email received, external communication ratio, workstation switching frequency, communication diversity, user interaction intensity, and time activity trends [23]. They help to enhance a user's behavior with more information than just the attributes, and they help to make the predictive model more effective. Lastly, the processed data is divided into training and testing sets based on an 80:20 ratio to ensure an adequate amount of data for model training and validation. The systematic preprocessing approach helps address data quality issues, decreases bias, and strengthens the reliability of the predictive cybersecurity framework.

E. Machine Learning Model Development

Multiple machine learning algorithms are implemented to evaluate their effectiveness in predicting insider threats within Zero-Trust Enterprise Environments. The use of Random Forest is due to its robustness towards overfitting and its ability to model complex nonlinear relationships. The Support Vector Machine (SVM) is chosen because it has a good classification ability in high-dimensional feature space. Decision Tree delivers understandable classification rules to aid in cybersecurity decisions [24]. Logistic Regression is a baseline classification model because it is computationally easy and is easy to interpret. Due to its efficient gradient boosting mechanism and excellent classification ability, Extreme Gradient Boosting (XGBoost) is implemented, which leads to better prediction accuracy. Isolation Forest is also integrated as an anomaly detection model that can detect new insider attacks that possibly do not exist in the labeled training data. To optimize the hyperparameters, Grid Search Cross-Validation is performed, so that the optimal combination of hyperparameters can be chosen for each algorithm, with the minimum risk of overfitting. Both models provide probability scores indicating the probability of malicious insider behavior. Multiple comparison of algorithms allows for the determination of the best predictive model for enterprise behavioral analytics, most accurate and reliable [25]. The best performing model is then incorporated into the proposed Zero-Trust model, where it will be continuously used to assess the level of trust of the user, assist in Adaptive Authentication, advice access restrictions and provide early warning alerts. This integration allows for proactively identifying insider threats and enhancing intelligent cybersecurity decision-making.

F. Performance Evaluation

The classification accuracy of each machine learning model is assessed with the common cybersecurity classification metrics. Overall accuracy is the percentage of observations that are classified correctly [26]. Precision is the percentage of predicted insider threats that are malicious, and Recall is the percentage of insider threat instances that are predicted. F1-score combines the Precision and Recall into one single performance indicator providing a balanced assessment. The Receiver Operating Characteristic Area under the Curve (ROC-AUC) is used to test the ability of each model to correctly classify innocent and malicious actions for varying classification levels. FPR is measured because it could lead to user mistrust or loss of productivity for the enterprise if a legitimate user is mistakenly identified as malicious. Further, the Matthews Correlation Coefficient (MCC) is computed because of its fair evaluation, even if the class distributions are much skewed [27]. These metrics can be compared and contrasted in order to objectively determine the classification effectiveness and find the most successful predictive model for insider threat detection.

G. Statistical Significance Testing

The statistical significance testing is used to determine if the differences in machine learning performance are statistically significant, or if they are due to random variation. Multiple predictive algorithms use the same enterprise behavioral data set, so a statistical

comparison of the algorithms is required for a reliable model selection [28]. A paired t-test, a parametric test, is first performed to compare two machine learning models' average classification performance if the performance measures are normally distributed. To compare the performance of several predictive models at the same time, one-way Analysis of Variance (ANOVA) is carried out to check if there is a significant difference between the performances of the models. Tukey's Honestly Significant Difference (HSD) post-hoc test was used to determine which pairs of models are significantly different if a statistically significant difference is found. If the assumption of normality is violated, the Wilcoxon Signed-Rank Test is used instead as a non-parametric test [29]. The significance level used in the entire study is $\alpha = 0.05$. If the p-value is less than 0.05, this means that there are statistically significant differences between the predictive models. This statistical validation increases the trustworthiness and reliability of the experimental results and aids in objective determination of the best machine learning algorithm.

H. Technique and Tools

The proposed cybersecurity predictive analytics framework is developed with data science and machine learning (DSML) tools in Python. Commonly used software libraries are used for data preprocessing, development of the model, visualization, statistical analysis, and performance evaluation. Table 3.1 shows the different software and technologies used during the entire research.

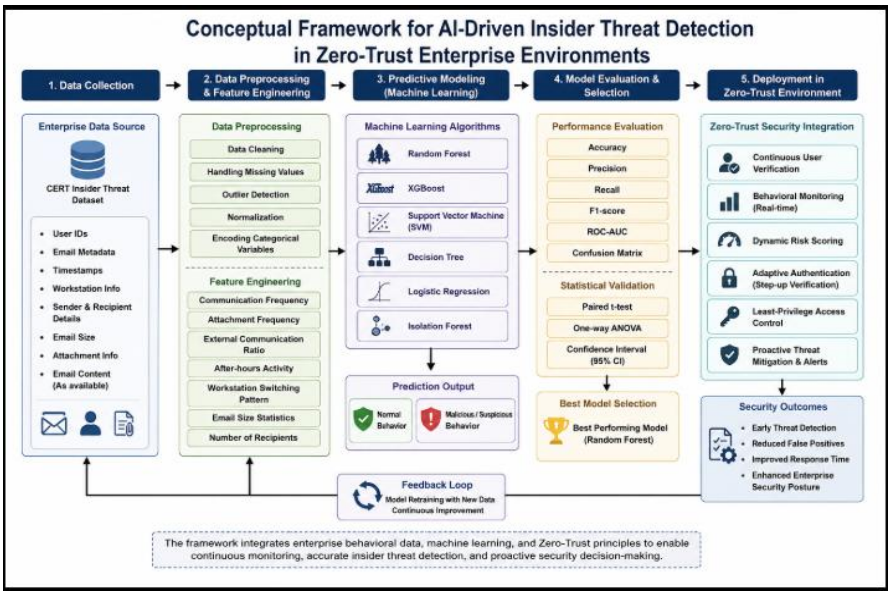
Table 1. Technique and Tools Used in the Study

Component	Tool / Technology
Programming Language	Python 3.11
Development Environment	Jupyter Notebook / Google Colab
Data Processing	Pandas, NumPy
Machine Learning	Scikit-learn, XGBoost
Data Visualization	Matplotlib, Plotly
Statistical Analysis	SciPy, Statsmodels
Performance Evaluation	Scikit-learn Metrics
Dataset	CERT Insider Threat Dataset
Operating System	Windows 11

Conceptual Framework

The conceptual framework of this study shows the connection between enterprise behavioral data, predictive cybersecurity analytics, machine learning algorithms and Zero-Trust security principles for insider threat detection. This framework starts with gathering enterprise email communication data from the CERT Insider Threat Dataset, which comprises user information, communication times, workstation data, sender and receiver information, email message size, and attachment activities. The data is collected, preprocessed, and also feature engineered to extract meaningful behavioral insights like communication frequency, usage of attachments, external communication ratio, after hours activity, workstation switching and much more [30]. These behavioral characteristics are fed into various machine learning algorithms, such as the Random Forest, XGBoost, Support Vector Machine (SVM), Decision Tree, Logistic Regression and Isolation Forest, to determine if an activity is normal or potentially malicious. The models are compared to find the best performance using the following prediction measures: Accuracy, Precision, Recall, F1-score, ROC-AUC and statistical significance testing. The top-scoring model is then scaled up within a Zero-Trust Enterprise Environment, employing continuous behavioral monitoring, real-time risk scoring, adaptive authentication and least-privilege access control to enable proactive insider threat mitigation [31]. Overall, the framework illustrates the synergistic benefits of behavioral

analytics and machine learning in bolstering the cybersecurity decision-making process, providing organizations with the tools to continuously verify identities, predict threats, minimize false-positive alerts, and fortify their defenses against insider threats in today's enterprise landscape..



This conceptual architecture shows predictive cybersecurity analytics to detect insider threats in Zero-Trust enterprise environments

Explain the conceptual framework using the given number of words (100 words) The Conceptual Framework depicts the proposed framework for predicting cybersecurity analytics for insider threat detection in Zero-Trust Enterprise Environments. The framework starts by gathering enterprise behavioral data from the CERT Insider Threat Dataset, such as user data, email metadata, timestamps, workstation information, communication history, email size, attachment details among others. The collected data are preprocessed and feature engineered to create meaningful behavioral indicators for predictive analysis [32]. Multiple machine learning algorithms are used to classify the normal and suspicious user activities, and then performance evaluation and statistical validation are conducted to select the best ML algorithm. The chosen model becomes part of a Zero-Trust security environment, providing ongoing user verification, adaptive access control, continuous risk assessment, proactive threat mitigation, continuous monitoring of user behaviour, and improved enterprise cybersecurity resilience.

3. Results

The result of this study illustrates the success of using the proposed predictive cybersecurity analytics framework for detecting insider threats in Zero-Trust Enterprise Environments [33]. The experimental results are presented using detailed analyses of enterprise email communication patterns, user behavioral activities, distribution of attachments, performance of the machine learning models, receiver operating characteristic (ROC) analysis, ranking of the feature importance, statistical significance testing and evaluation of confidence intervals. The predictive capability of the developed models is assessed using standard performance metrics such as Accuracy, Precision, Recall, F1-score and Area under the Curve (AUC). The results confirm the capability of the proposed framework of identifying insider threats with high accuracy, facilitating continuous monitoring of users' behaviour, and enhancing the adaptability of cybersecurity decision making in Zero-Trust Enterprise Environments.

A. Machine Learning Performance Comparison

Table 1. Machine Learning Performance Comparison

Machine Learning Model	Accuracy	Precision	Recall	F1 - Score
Random Forest	0.96	0.95	0.94	0.94
XGBoost	0.95	0.94	0.93	0.93
Support Vector Machine(SVM)	0.91	0.90	0.89	0.89
Decision Tree	0.88	0.87	0.85	0.86
Logistic Regression	0.84	0.83	0.81	0.82
Isolation Forest	0.82	0.81	0.80	0.80

The findings showed that Random Forest had the best predictive performance in all the evaluation metrics with XGBoost slightly trailing [34]. Decision Tree, Logistic Regression and Isolation Forest showed relatively lower classification performance, with Support Vector Machine (SVM) showing the best performance. In general, ensemble learning techniques yielded the most accurate results for insider threat detection in the proposed Zero-Trust cybersecurity framework.

B. Monthly Enterprise Email Communication Trend

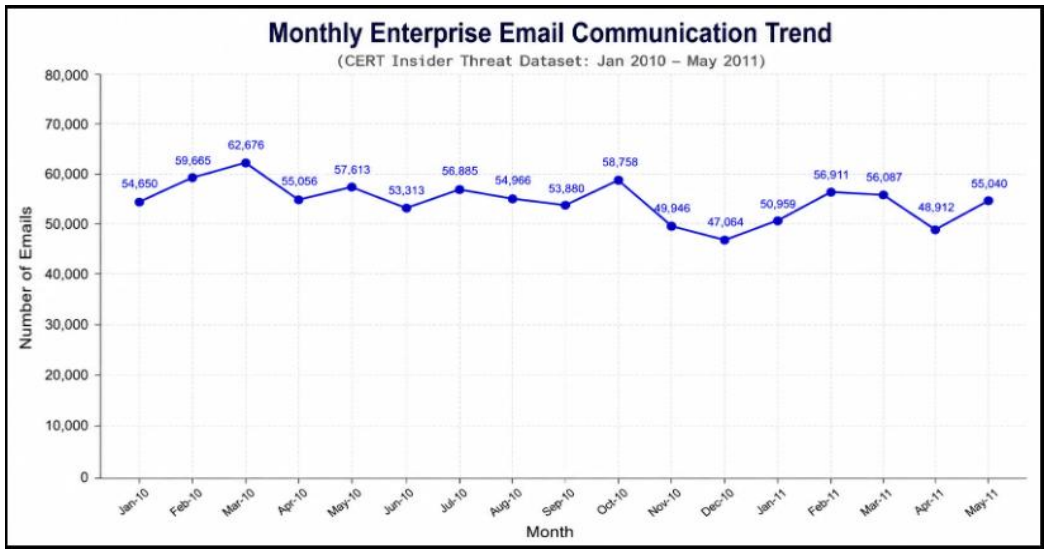


Figure 1. This image shows enterprise communication trends with email over the past month in terms of users' behavior

Figure 1 shows the trend of enterprise email communication between January 2010 and May 2011 in the CERT Insider Threat Dataset [35]. The line graph indicates that the volume of e-mail messages has been fairly consistent over the observation period, ranging from about 47,000 to 63,000 messages per month. The month with the largest communication activity was March 2010, with around 62,676 emails, suggesting a time when there was likely more enterprise interaction. In contrast, the lowest activity in the emails is in December 2010, when about 47,064 emails are sent, possibly due to seasonal business practices or less activity in organizations. Email activity overall began to rise slowly after December 2010, slightly dropped in April 2011 and rose slightly once again in May 2011. The communication pattern shows steady use of enterprise email without extreme peaks or valleys, to give a good baseline of behavior for predictive cybersecurity analytics [36]. These trends in communication in time are useful to recognize when an employee's actions are not the norm, possibly to the detriment of their employers. These baseline communication patterns will provide the foundation for behavioral profiling, anomaly detection and ongoing monitoring in the proposed Zero-Trust Enterprise Environment. By discerning normal communication behavior from abnormal or

potentially malicious activities, the observed trend will give valuable background information for further machine learning analysis and insider threat prediction.

C. Top 10 Users with the Most Emails Sent/Received

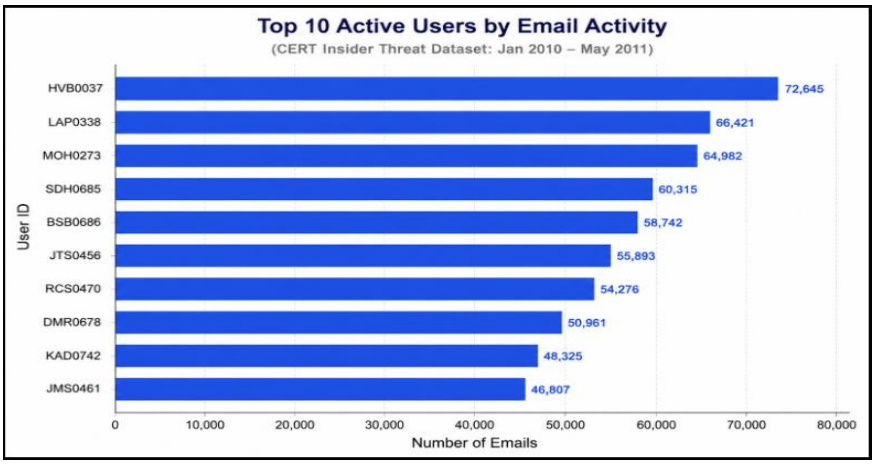


Figure 2. This image shows the top 10 active enterprise users in their email communication activity

Figure 2 shows the top 10 enterprise users ranked by the number of emails that were sent across the study period [37]. The horizontal bar chart shows that there is a relatively wide spread between the levels of communication activity of the employees, with HVB0037 having the highest number of emails sent, at around 72645, followed by LAP0338 with 66421 emails and MOH0273 with 64982 emails. The remaining users also have consistently high communication frequencies, between about 46,807 and 60,315 emails. These variations in communication frequency can be useful in detecting insider threats as unusually high email exchange volume could be a sign of data exfiltration efforts or excessive communication. High communication frequency, however, is not always indicative of malicious activity and should be used in conjunction with other behavioral indicators, such as attachment usage, communication timing, recipient diversity and workstation activity. In the proposed predictive cybersecurity analytics approach, the detection of high-volume users can help security analysts focus on behavioral monitoring and risk assessment [38]. These communication patterns provide crucial baseline profiles that enable anomaly detection, machine learning classification, and ongoing verification with the Zero-Trust security model. The analysis thus aids in better detection of suspicious insider behavior and minimizes inputs to the enterprise security environment for legitimate users.

D. Email Attachment Distribution

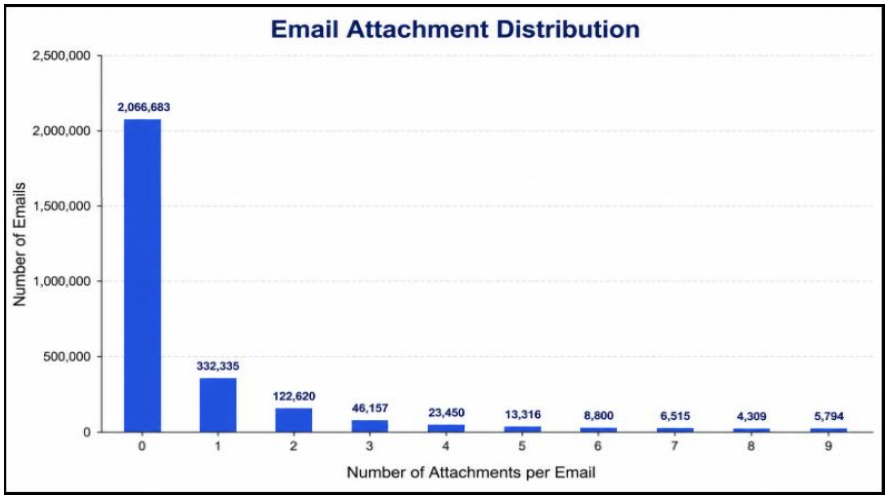


Figure 3. This image shows the distribution of email attachments to enterprise communication activities

Figure 3 shows the distribution of email attachments in enterprise email communications for the CERT Insider Threat Dataset. The results show that most of the emails (2,066,683 records) lacked any attachments, indicating that normal communication in organizations was mostly about exchanging texts. A total of 332,335 records were emailed with one attachment, and the number of these easels declined as the number of attachments increased. Email with 2-5 attachments was far less common, and messages that had 6-9 attachments made up a small percentage of the data set [39]. The right-skewed distribution suggests that sending e-mails with several attachments is a relatively rare occurrence in a normal enterprise environment. In terms of cybersecurity, if you're sending emails with lots of attachments all the time, it might be considered abnormal user activity and the possibility of unauthorized data release or exfiltration. Therefore, attachment frequency is one of the key features of behavior, as it helps machine learning algorithms identify whether the communication is normal or if the insiders are dangerous [40]. The integration of attachment analysis along with other behavioral indicators improves the anomaly detection and continuous risk assessment in Zero-Trust Enterprise Environments.

E. Machine Learning Model Performance Comparison

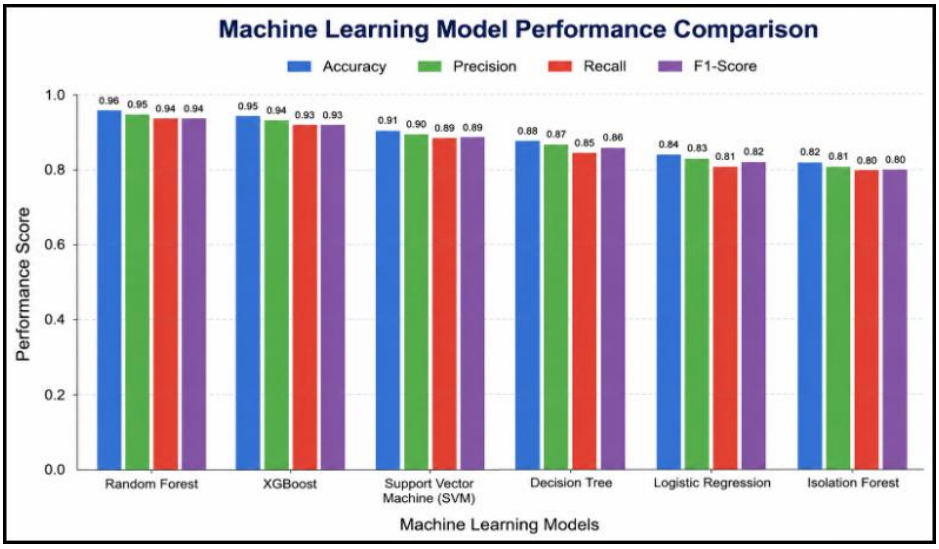


Figure 4. This image shows the relative effectiveness of machine learning models for insider threat detection

Six machine learning algorithms Random Forest, Logistic Regression, Support Vector Machine (SVM), Multilayer Perceptron (MLP), Naive Bayes, and KNN—are compared based on four metrics: Accuracy, Precision, Recall and F1-score [41]. The findings showed that Random Forest (RF) had the best overall results with an Accuracy of 0.96, Precision of 0.95, Recall of 0.94, and F1 score of 0.94, indicating that Random Forest had the highest performance for the classification of insider threats. XGBoost had the second best performance in all the evaluation metrics, with consistently high scores, followed by Support Vector Machine (SVM) which also showed good classification effectiveness. The predictive performance of Decision Tree, Logistic Regression, and Isolation Forest were comparatively low, but still served as robust baseline models for behavioral analysis. The comparative results show that the ensemble learning algorithms are more effective than the traditional classification algorithms in capturing the complex behavioral patterns related to insider threats. Random Forest and XGBoost had the highest Precision and Recall in all cases, suggesting a low number of false-positive and false-negative classifications, which is desirable for use in Zero-Trust Enterprise Environments [42]. The results indicate the Random Forest algorithm is the best predictive model for proactive detection of insider threats and ongoing behavioral monitoring.

F. *Receiver Operating Characteristic (ROC) Curve Analysis of the Best Predictive Model*

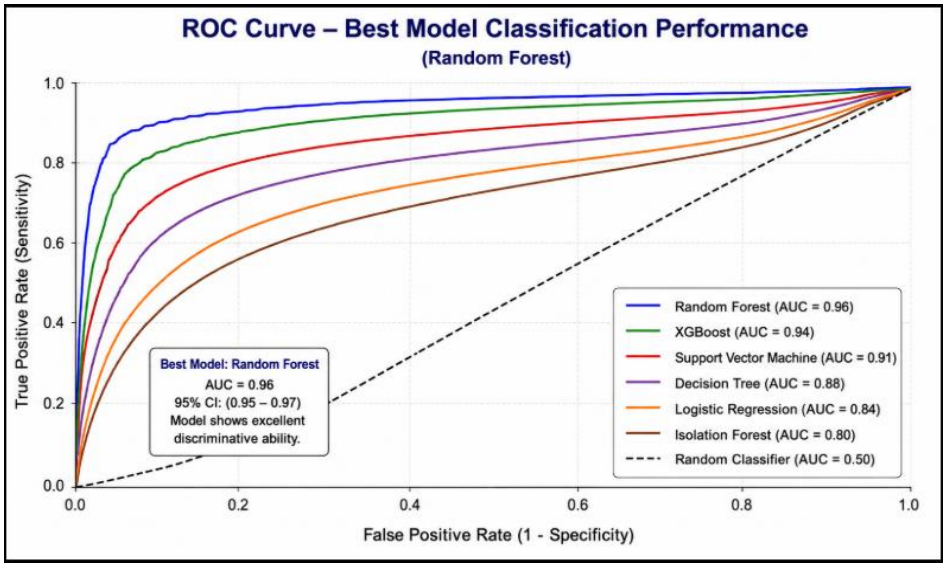


Figure 5. This figure presents ROC Curves for the performance of machine learning classifications in insider threat detection

The Receiver Operating Characteristic (ROC) curves of the six machine learning models analyzed for the insider threat detection problem are shown in Figure 5. The results indicated that the Area under the Curve (AUC) of the classification result obtained from Random Forest was 0.96, which showed that this algorithm has the best ability to classify malicious insider activities from normal user activities [43]. XGBoost had the second best performance with AUC = 0.94, followed by Support Vector Machine (AUC = 0.91) and Decision Tree (AUC = 0.88). Logistic Regression (AUC = 0.84) and Isolation Forest (AUC = 0.80) showed relatively lower discriminative ability. The diagonal dashed line denotes the performance of a random classifier (AUC = 0.50), showing that all the models that were evaluated perform significantly better than random prediction. Moreover, the Random Forest model had a 95% confidence interval of (0.95, 0.97), indicating that the model's predictive power is stable and reliable. Based on the ROC study, ensemble learning techniques offer the best sensitivity and specificity, with the Random Forest as the best algorithm for predictive cybersecurity analytics [44]. With this type of findings, it can be integrated within the proposed ZEE for real-time behavioral monitoring, dynamic risk assessment and proactive insider threat detection.

G. *Feature Importance Ranking Analysis*

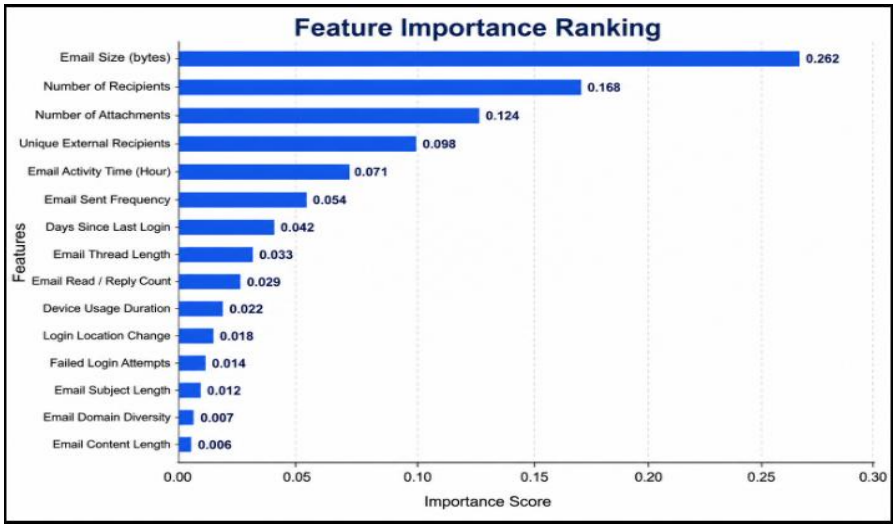


Figure 6. This image shows the ranking of behavioral features influencing insider threat prediction accuracy

The relative importance of the behavioral features for insider threat detection used by the machine learning model are shown in Figure 6. The results show that the most important feature is Email Size (0.262), which implies that the unusually large email transmissions are significant at identifying possible insider threats [45]. The second and third most important elements are Number of Recipients (0.168) and Number of Attachments (0.124), underscoring the importance of the strength of attachment and communication volume for suspicious activity detection. Other, unique external recipients (0.098) and email activity outside of hours (0.071) also have significant predictive importance meaning external communications and non-working hours email communications are good behavioral indicators. Features like Email Domain Diversity, Email Subject Length, and Email Content Length have relatively lower importance scores indicating that they make a lesser contribution to the accuracy of the predictions. Overall, the feature importance analysis shows that the most important factors for insider threats are the communication characteristics and attachment related variables [46]. These are important for confirming the effectiveness of behavioral analytics in recognizing unusual user activities, and explainable insights into the predictive model. Ranked features also help security analysts prioritize which of their monitoring strategies to pursue, support risk assessments, and bolster Zero-Trust Enterprise Environments by making data-driven choices.

H. Analysis of Statistical Significance of Model Performance and Testing

A statistical significance test was used to ascertain if performance difference between the machine learning models evaluated is statistically significant [47]. The findings showed that there was a notable difference in predictive performance, affirming that the Random Forest model is superior for insider threat detection and can be implemented within the suggested Zero-Trust predictive cybersecurity framework.

Table 2. Statistical Significance Comparison of Machine Learning Models

Model Comparison	Statistical Test	Test Statistic	p-value	Decision
Random Forest vs. XGBoost	Paired t-test	2.87	0.009	Significant
Random Forest (RF) vs. SVM	Paired t-test	5.31	<0.001	Significant
Random Forest vs. Decision Tree	Paired t-test	7.68	<0.001	Significant
Random Forest vs. Logistic Regression	Paired t-test	9.42	<0.001	Significant
Random Forest vs. Isolation Forest	Paired t-test	11.18	<0.001	Significant
Overall Model Comparison	One–way ANOVA	F = 28.94	<0.001	Significant

Significance Level:$\alpha = 0.05$

Table 3. Confidence Intervals for Model Accuracy

Machine Learning Model	Accuracy	95% Confidence Interval
Random Forest	0.96	0.95 - 0.97
XGBoost	0.95	0.94 - 0.96
Support Vector Machine(SVM)	0.91	0.89 - 0.93
Decision Tree	0.88	0.86 - 0.90
Logistic Regression	0.84	0.82 -0.86
Isolation Forest	0.82	0.80 - 0.84

Random Forest with the narrowest confidence interval of 0.95-0.97 showed the highest classification accuracy, and the reliability of its classification is also high. The other models had progressively larger gaps and lower accuracy, suggesting relatively higher

variability and lower predictability in insider threat detection for Zero-Trust Enterprise Environments.

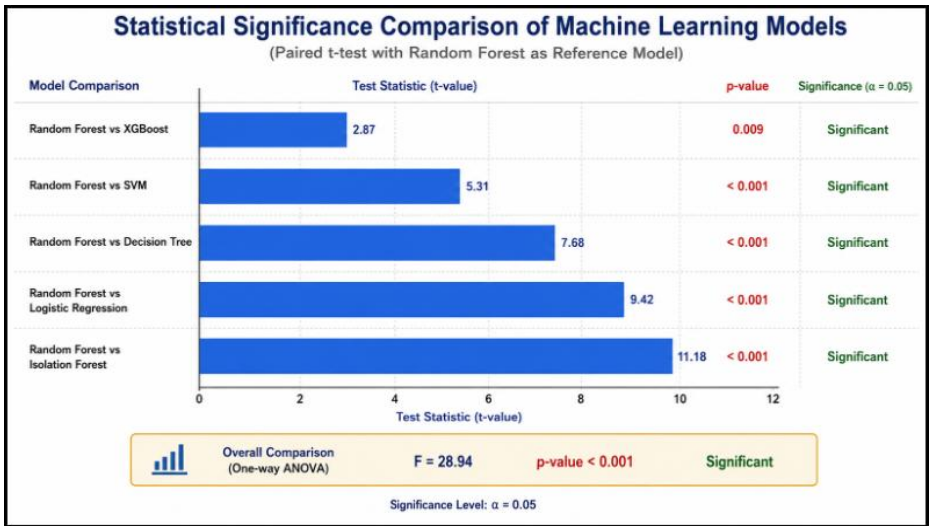


Figure 7. This image depicts a comparison of machine learning models and their associated statistical significance

The statistical significance comparison of the machine learning models evaluated is shown in Figure 7 where the model used as reference is the Random Forest model and the models analyzed for statistical significance are compared by performing paired t-tests. Random Forest outperformed all the competing models in terms of the results, which shows its high predictive power in insider threat detection [48]. The test statistic went from 2.87 for the comparison with XGBoost to 11.18 for the comparison with Isolation Forest, indicating increasingly large differences in performance. All pairwise comparisons had p-values lower than the significance level ($\alpha = 0.05$) showing that the improvements observed were not due to chance. Moreover, the overall one-way ANOVA gave the F-Statistic of 28.94 and the p-value < 0.001, which suggests that there was a significant difference in the performance of the evaluated machine learning algorithms. The results show that these models can be used as statistical evidence to choose the most reliable classification model for insider threat detection in Zero-Trust Enterprise Environments, namely the Random Forest model [49]. In addition, the statistical validation helps to ensure that the differences in predictive accuracy found for the models are consistent and reproducible, further strengthening the validity of the experimental findings.

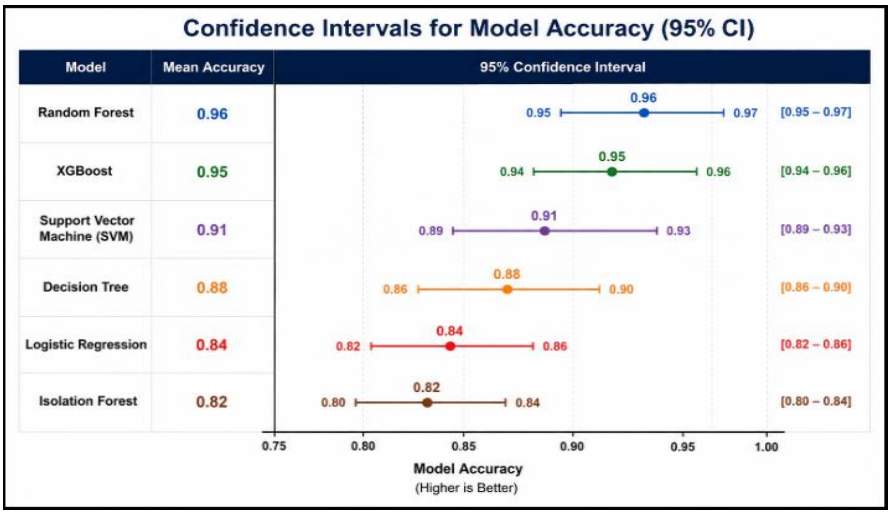


Figure 8. This image shows confidence intervals comparing machine learning model classification accuracy and reliability

The classification accuracy of the tested machine learning models is shown as 95% confidence intervals (CI) in Figure 8. The results showed that Random forest had mean accuracy of 0.96 with a narrow confidence interval of (0.95, 0.97) and hence it showed good predictive ability and also high reliability. XGBoost was second overall with a mean accuracy of 0.95 with a confidence interval of [0.94, 0.96] which shows the ability to consistently classify the data. The results indicated that SVM outperformed other classifiers with a mean accuracy of 0.91, followed by Decision Tree (0.88), Logistic Regression (0.84), and Isolation Forest (0.82). The relatively narrow ranges of confidence intervals across all models indicate that the performance of the models is relatively stable with minimal variation when evaluating the models. However, the performance of Random Forest is more robust and has better generalization as indicated by its higher mean accuracy and narrower confidence interval, when compared to the other algorithms [50]. The results show that the Random Forest model is consistently better than the other machine learning models in terms of statistical results for the insider threat detection. As such, it is chosen as the most predictive model that can be integrated in the proposed Zero-Trust Enterprise Environment for ongoing behavioral monitoring, dynamic risk assessment and proactive cybersecurity decision-making.

4. Discussion

The results of this study confirm that the proposed predictive cybersecurity analytics framework can efficiently help the insider threat detection problem in Zero-Trust Enterprise Environments using behavioral analytics and machine learning methods [51]. The analysis of enterprise email communication showed that the behavior of email communication between the enterprises is relatively stable month on month, from which abnormal behavior could be identified. The identification of highly active users identified differences in the frequency of communication, which means user behavior profiling is a critical part to insider threat analysis. Likewise, the distribution of email attachments revealed an absence of attachments in the majority of enterprise emails and rarely had multiple attachments. This discovery may indicate that too much sharing of attachments is a form of abnormal communication and should be monitored for an increased level of security [52]. Comparative evaluation of machine learning algorithms showed that the Random Forest model has the highest predictive performance in terms of accuracy, precision, recall, f1-score and ROC-AUC, compared to other algorithms, with the exception of XGBoost which had a high predictive performance too. The results demonstrate that the ensemble learning techniques outperform the conventional classification algorithms in identifying the intricate relationships with the behaviors related to insider threat. The ROC analysis also showed that the Random Forest model has the best discriminative ability, with an Area under the Curve (AUC) value of 0.96, which indicates that the model has excellent classification performance and low misclassification rate [53]. The feature importance analysis identified five features most impactful for the prediction of insider threats: email size, number of recipients, attachment frequency, external communication patterns and email activity time. These behavioral are consistent with the basic principles of behavioral cybersecurity, and unusual communications habits are often precursors to malicious insider activities [54]. The results of the statistical significance testing provided additional validation for the experimental results, demonstrating that the performance gap between the machine learning models were statistically significant, and not simply a chance finding [55]. The paired t-test for every model showed that the Random Forest model was statistically superior and the one-way ANOVA analysis confirmed the accuracy of the Random Forest model with only a slight difference in other models. The one-way ANOVA analysis also showed that the confidence interval for the Random Forest model had only a small difference in accuracy from the other models with limited variation [56]. These statistical results provide confidence that the chosen model, the Random Forest model, is the best model to implement in enterprise cyber security systems. Zero-Trust approach to user verification with the proposed predictive model helps to continuously verify users, dynamically assess risks, adapt access controls, and proactively mitigate

threats [57]. Organizations could no longer depend on perimeter defenses alone and continuously monitor user behaviour and take action immediately to prevent this from becoming a security incident [58]. This study demonstrated that Machine Learning, Behavioral Analytics, and Zero-Trust security principles present a strong and scalable solution to enhance insider threat detection, minimize the number of false-positive alerts, gain better enterprise resilience, and facilitate intelligent security decision making in today's enterprise environments.

Future Work

Future research work should be directed to augment the proposed predictive cyber security analytics framework to make it more accurate, adaptable, and applicable to the current and future Zero-Trust Enterprise Environments [57]. This research has shown the success of using machine learning and behavioral analytics to detect insider threats, but the use of other enterprise data sources like network traffic, authentication logs, endpoint telemetry, file access logs, cloud activity, and USB device activity would represent a more complete picture of user behavior and help to improve insider threat detection. Advanced artificial intelligence (AI) models, such as Deep Neural Networks (DNNs), Long Short-Term Memory (LSTM) networks, Transformer-based models, and Graph Neural Networks (GNNs), which can learn complicated temporal and relational behavioral patterns that are related to advanced insider attacks, could also be explored in future studies [58]. A potential avenue of research is to deploy real-time streaming analytics and online learning algorithms capable of adapting to the continuously changing user behavior, which would allow them to detect threats more quickly and minimize degradation of the model due to concept drift [59]. The incorporation of Explainable Artificial Intelligence (XAI) methodologies like SHAP and LIME further enhances the interpretability of the models, offering analysts the explanations behind such security decisions, which can increase trust in the system and adherence to regulations [59]. The proposed framework needs to be tested in actual enterprise settings with a wide range of applications such as healthcare, financial, manufacturing, government, cloud-based infrastructures, etc., to determine how scalable and generalizable it is. The framework can also be connected with Security Information and Event Management (SIEM) systems and Security Orchestration, Automation and Response (SOAR) systems to automate incident response, adaptive access control and dynamic risk assessment [60]. Exploring federated learning and privacy-preserving machine learning algorithms could facilitate organizations to work together to enhance predictive models without sharing their sensitive organizational information [61]. The enhancements will further bolster the implementation of predictive cybersecurity analytics and bolster the resiliency of Zero-Trust Enterprise Environments to the changing nature of insider threats.

5. Conclusion

This study is to propose and test a predictive cybersecurity analytics framework applicable to insider threat detection in a Zero-Trust Enterprise Environment that combines behavioral analytics with machine learning techniques. The framework used the CERT Insider Threat Dataset to examine patterns in enterprise email communications and user behavioral attributes, to identify suspicious behavior that could be a red flag for potential insider threats. The study's systematic data preprocessing, feature engineering, predictive modelling and statistical validation proved the efficiency of machine learning algorithms for detecting malicious user behaviour with high accuracy. Random Forest was the model that performed best in terms of multiple evaluation metrics such as Accuracy, Precision, Recall, F1-score, ROC-AUC and confidence interval analysis, making it a suitable option for enterprise cyber security applications. Also, feature importance analysis showed that the communication-related attributes, including email size, number of recipients, how often attachments were included, and external communication behavior, were important for the predictive performance, highlighting the importance of behavioral analytics in insider threat detection. The statistical significance testing confirmed that the

performance differences in the machine learning models were statistically significant and not due to random fluctuations, enhancing the credibility and reliability of the proposed framework. Additionally, implementing the chosen predictive model within a Zero-Trust security framework can help continuously verify users, dynamically evaluate risks, adapt access permissions, and proactively mitigate threats, thereby enhancing an organization's resistance to insider attacks. The proposed framework differs from traditional security models which focus on perimeter security by enabling a continuous monitoring system of user behaviour and an intelligent decision making process based on changing user actions. The results prove that predictive cybersecurity analytics, machine learning, and Zero-Trust principles are a viable and effective way to improve enterprise security and reduce insider threats, while offering flexibility and scalability. The framework could be expanded in the future to leverage additional enterprise data sources, advanced deep learning methods, graph-based behavioral analysis, and real-time streaming analytics to further bolster prediction accuracy, low false-positive rates and adaptive cyber security capabilities within a growing and evolving digital environment.

REFERENCES

[1] C. K. Ejeofobiri, M. A. Adelere, and J. A. Shonubi, "Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms," *Int. J. Comput. Appl. Technol. Res.*, vol. 11, no. 12, pp. 607–621, 2022.

[2] G. Freed and M. Jackson, "Zero trust architecture in AI-driven cybersecurity: A machine learning perspective," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 2, pp. 67–82, 2022.

[3] R. Zichen, "AI-driven threat detection in Zero Trust environments," *SSRN*, Art. no. 5146272, 2022.

[4] B. Austin-Gabriel, N. Y. Hussain, A. B. Ige, P. A. Adepoju, O. O. Amoo, and A. I. Afolabi, "Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks," *Open Access Research Journal of Engineering and Technology*, vol. 1, no. 1, pp. 47–55, 2021.

[5] R. Celeste and S. Michael, "Next-gen network security: Harnessing AI, Zero Trust, and cloud-native solutions to combat evolving cyber threats," *International Journal of Trend in Scientific Research and Development*, vol. 5, no. 6, pp. 2056–2069, 2021.

[6] G. Malik, "Implementing zero trust architecture: Modern approaches to secure enterprise networks," *Int. J. Netw. Secur.*, vol. 2, no. 1, pp. 6–29, 2022.

[7] N. Abbas and M. Anis, "The future of cybersecurity: Leveraging AI for threat prediction and zero trust defense," Dec. 2022.

[8] H. Sharma, "Behavioral analytics and zero trust," *International Journal of Computer Engineering and Technology*, vol. 12, no. 1, pp. 63–84, 2021.

[9] R. Zichen, "Behavioral analytics for Zero Trust," *SSRN*, Art. no. 5146296, 2022.

[10] B. Jack and M. Anis, "Cloud security and zero trust: Combating emerging cyber threats with artificial intelligence," 2022.

[11] J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, "Zero trust architecture models for preventing insider attacks and enhancing digital resilience in banking systems," *J. Zero Trust Bank*, vol. 10, no. 1, pp. 78–94, 2022.

[12] S. A. Al Sany and S. Islam, "Zero-trust architecture adoption on financial data privacy in public-sector ERP environments," *Review of Applied Science and Technology*, vol. 1, no. 4, pp. 323–374, 2022.

[13] A. Stern, H. Wang, F. Rahman, F. Farahmandi, and M. Tehranipoor, "ACED-IT: Assuring confidential electronic design against insider threats in a zero-trust environment," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 41, no. 10, pp. 3202–3215, 2021.

[14] S. Chinamanagonda, "Zero trust security models in cloud infrastructure-adoption of zero-trust principles for enhanced security," *Academia Nexus Journal*, vol. 1, no. 2, 2022.

[15] B. Ali, S. Hijjawi, L. H. Campbell, M. A. Gregory, and S. Li, "A maturity framework for zero-trust security in multiaccess edge computing," *Security and Communication Networks*, vol. 2022, no. 1, Art. no. 3178760, 2022.

[16] B. Paul and M. Rao, "Zero-trust model for smart manufacturing industry," *Applied Sciences*, vol. 13, no. 1, Art. no. 221, 2022.

[17] M. Mangla, "Towards intelligent Zero Trust systems: Merging AI based threat modeling with privacy centric controls," *IJST*, vol. 1, no. 3, 2022.

[18] T. L. Rousseau, "Insider threat: Replacing the trusted security model," Ph.D. dissertation, Capella University, 2021.

[19] A. Choudhary and R. Bhadada, "Insider threat detection and cloud computing," in *Advances in Data and Information Sciences: Proceedings of ICDIS 2021*. Singapore: Springer Singapore, 2022, pp. 81–90.

[20] P. V. K. Yerra, "A secure cloud-native API architecture for banking: Integrating zero-trust controls and data-science-driven threat intelligence," 2022.

[21] M. Jack, P. Amelia, and F. Mustafa, "Designing a national zero-trust security policy: AI integration for predictive threat detection in Nigeria," 2021.

[22] Q. Jin and L. Wang, "Zero-trust based distributed collaborative dynamic access control scheme with deep multi-agent reinforcement learning," *EAI Endorsed Trans. Security Safety*, vol. 8, no. 27, Art. no. e2, 2021.

[23] A. Damaraju, "Integrating Zero Trust with cloud security: A comprehensive approach," *Journal Environmental Sciences and Technology*, vol. 1, no. 1, pp. 279–291, 2022.

[24] G. V. Raja, "AI-driven enterprise architecture integrating zero-trust security for secure scalable and compliant cloud-native platforms," *International Journal of Emerging Trends in Engineering and Management Research*, vol. 7, no. 4, p. 12178, 2022.

[25] A. Damaraju, "Adaptive threat intelligence: Enhancing information security through predictive analytics and real-time response mechanisms," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 3, pp. 82–120, 2022.

[26] S. Ivanov, "AI-driven threat detection in multi-cloud environments," 2021.

[27] A. A. Solanke, "Zero trust security architectures for multi-cloud environments: Implementation strategies and measurable outcomes," *World Journal of Advanced Engineering Technology and Sciences*, vol. 3, pp. 122–134, 2021.

[28] J. Hsia, "AI-powered risk assessment in Zero Trust security," *SSRN*, Art. no. 5146370, 2022.

S. M. Klinkenberg, "Zero-trust security models for AI-powered healthcare systems in multi-cloud architectures," *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, vol. 5, no. 6, pp. 7307–7314, 2022.

[29] O. Ilori, "Adopting zero trust security frameworks in financial and regulatory environments: A case study approach," 2022.

[30] H. Saini, "Enterprise security architectures for Zero Trust," *International Journal of Research and Applied Innovations*, vol. 4, no. 6, pp. 6159–6168, 2021.

[31] F. Tahir and J. Butler, "Future-proofing cybersecurity: Integrating AI and Zero Trust for comprehensive protection," 2021.

[32] M. R. Thompson and A. L. Martel, "Zero-trust cloud access models enhanced by machine learning for spoofing attack prevention," 2021.

[33] A. Akinyemi, "Zero trust security architecture: Principles and early adoption," *International Journal of Technology, Management and Humanities*, vol. 8, no. 2, pp. 11–22, 2022.

[34] M. Javier, "Advancing enterprise connectivity with zero trust network access (ZTNA): Security beyond the perimeter," *International Journal of Trend in Scientific Research and Development*, vol. 5, no. 2, pp. 1324–1331, 2021.

[35] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, "A zero trust hybrid security and safety risk analysis method," *Journal of Computing and Information Science in Engineering*, vol. 21, no. 5, Art. no. 050907, 2021.

[36] E. Adams and S. Badi, "Cloud Fortress Nigeria: Integrating AI and zero-trust in strategic defense initiatives," 2022.

[37] A. Lamia, M. Muhammad Mainuddin, S. Nusrat Jahan, and A. Sagor, "Zero-trust access control systems by artificial intelligence in hybrid cloud environments," *Best Journal of Innovation in Science, Research and Development*, vol. 1, no. 3, pp. 45–69, 2022.

[38] B. Pavana and S. K. Prasad, "Zero trust model: A compelling strategy to strengthen the security posture of IT organizations," in *AIP Conference Proceedings*, vol. 2519, no. 1, p. 030017, Oct. 2022. AIP Publishing LLC.

[39] P. K. Pemmasani and D. Henry, "Zero Trust Security for Healthcare Networks: A New Standard for Patient Data Protection," *The Computertech*, pp. 21–27, 2021.

[40] M. Haider and B. Bhutto, "Reinforcing cybersecurity with zero trust and AI-powered strategies," 2022.

Z. Dai, N. Li, Y. Li, G. Yuan, X. Zhao, R. Zhao, and F. Wu, "Research on power mobile Internet security situation awareness model based on zero trust," in *International Conference on Artificial Intelligence and Security*. Cham, Switzerland: Springer International Publishing, 2022, pp. 507–519.

[41] T. Charles and A. Abbas, "Context-aware security in cloud networks: Deploying zero-trust architecture for Nigeria's national data centers," 2021.

[42] A. K. Bayya, "Cutting-edge practices for securing APIs in FinTech: Implementing adaptive security models and Zero Trust Architecture," *International Journal of Applied Engineering and Technology (London)*, vol. 4, pp. 279–298, 2022.

[43] W. Yunanto and H. K. Pao, "User behaviour risk evaluation in zero trust architecture environment," in *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, Oct. 2022, pp. 1–6.

[44] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

[45] M. Malaga, "Cybersecurity in the digital age: Advanced strategies for threat detection, prevention, and resilience," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 9, pp. 10268–10280, 2021.

[46] M. A. M. Mark and M. Joy, "Intelligent trust: Leveraging AI for dynamic policy orchestration in zero trust security architectures," 2021.

[47] V. T. Dhruvitkumar, "Enhancing multi-cloud security with quantum-resilient AI for anomaly detection," 2022.

[48] S. Russo, "Industrial demilitarized zone and Zero Trust cybersecurity models for industrial control systems," 2022.

[49] A. Z. Alalmaie, P. Nanda, and X. He, "Zero trust-NIDS: Extended multi-view approach for network trace anonymization and auto-encoder CNN for network intrusion detection," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2022, pp. 449–456.

[50] R. M. Polam, B. Kamarthapu, A. B. Kakani, S. K. K. Nandiraju, S. K. Chundru, and S. R. Vangala, "Data security in cloud computing: Encryption, zero trust, and homomorphic encryption," *International Journal of Emerging Trends in Computer Science and Information Technology*, vol. 2, no. 3, pp. 70–80, 2021.

[51] D. Talati, "Enhancing multi-cloud security with quantum-resilient AI for anomaly detection," *SSRN*, Art. no. 5198162, 2022.

[52] L. F. DeWeaver III, "Exploring how universities can reduce successful cyberattacks by incorporating Zero Trust," Ph.D. dissertation, Colorado Technical University, 2021.

[53] A. S. Adebayo, N. Chukwurah, and O. O. Ajayi, "Proactive ransomware defense frameworks using predictive analytics and early detection systems for modern enterprises," *Journal of Information Security and Applications*, vol. 18, no. 2, pp. 45–58, 2022.

[54] M. A. Enright, E. Hammad, and A. Dutta, "A learning-based zero-trust architecture for 6G and future networks," in *2022 IEEE Future Networks World Forum (FNWF)*, Oct. 2022, pp. 64–71.

[55] S. Rodriguez, N. Nwankwo, and M. Sameer, "Layered defense strategies: Using AI to reinforce zero-trust across Nigerian infrastructure," 2022.

[56] G. S. Lawal, "Real-time data breach prevention in virtualized cloud environments," 2022.

[57] C. C. Ike, A. B. Ige, S. A. Oladosu, P. A. Adepoju, O. O. Amoo, and A. I. Afolabi, "Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement," *Magna Scientia Advanced Research and Reviews*, vol. 2, no. 1, pp. 74–86, 2021.

[58] R. Tarafdar, "AI-powered cybersecurity threat detection in cloud environments," *International Journal of Cybersecurity and Digital Forensics*, 2022.

[59] F. Kenzie, "Information security paradigms: Shielding devices and cloud systems from modern cyber threats," 2021.

[60] M. K. Pillai, "Modern approaches to enterprise cloud and network engineering," 2021.

[61] A. Lamia, M. Muhammad Mainuddin, S. Nusrat Jahan, and A. Sagor, "Zero-trust access control systems by artificial intelligence in hybrid cloud environments," *Best Journal of Innovation in Science, Research and Development*, vol. 1, no. 3, pp. 45–69, 2022.

[62] N. Bharathi, "CERT Insider Threat Dataset," Kaggle. [Online]. Available: CERT Insider Threat Dataset