International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Cyber Attack Breaches Prediction Using ML

Indrasena Reddy[1], Yalavala Sambasiva Rao[2], Udata Venkatasai[3], S. Geetha[4], T. Kumanan[5]

[1, 2, 3]Student, Computer Science and Engineering, Dr MGR Educational and Research Institute
[4]HOD, Computer Science and Engineering, Dr MGR Educational and Research Institute
[5]Professor, Computer Science and Engineering, Dr MGR Educational and Research Institute

Abstract

Cyber attacks have become a major threat to digital security, compromising sensitive information and disrupting critical systems. As these threats continue to evolve, the need for proactive defense mechanisms is greater than ever. This study explores the use of machine learning to predict potential cyber attack breaches, enabling early detection and prevention. By analyzing network traffic patterns, our approach helps identify suspicious activities before they escalate into full- scale breaches. To enhance practical usability, the model is designed for real-time deployment, allowing seamless integration with cybersecurity systems for continuous monitoring and rapid response. This research demonstrates the potential of AI-driven solutions in strengthening cybersecurity, paving the way for more advanced threat detection and prevention strategies in the future.

Keywords: Cybersecurity, Machine Learning, Threat Detection, Anomaly Detection

I. INTRODUCTION

In today's technology-driven world, cyber attacks have become a growing concern, affecting individuals, businesses, and even governments. As digital systems and online services expand, so do the risks associated with cyber threats. Hackers and malicious actors continuously find new ways to exploit vulnerabilities, leading to data breaches, financial losses, and system disruptions. The increasing frequency and sophistication of these attacks highlight the need for more advanced and proactive security measures..

Traditional cybersecurity approaches, such as firewalls, antivirus software, and rule-based intrusion detection systems, have long been used to protect digital assets. However, these methods are often reactive, relying on predefined rules and signatures to detect known threats. This makes them less effective against new, evolving, or previously unseen cyber threats. As cybercriminals develop more advanced attack techniques, conventional security measures struggle to keep pace, leaving systems vulnerable to breaches.

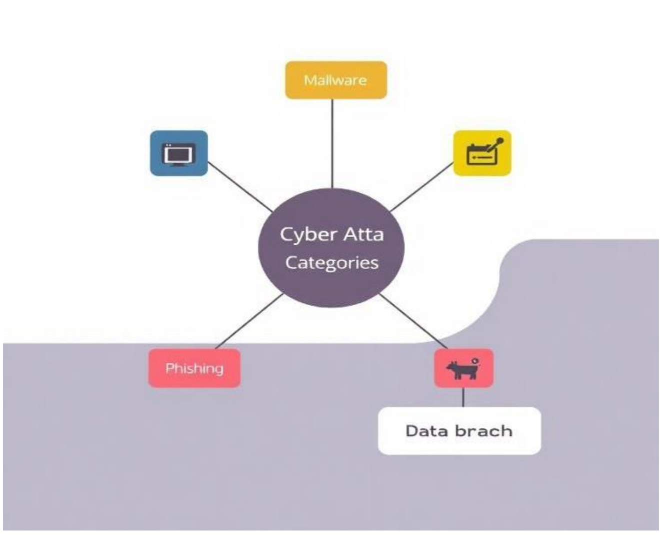
To address these challenges, machine learning has emerged as a powerful tool in cybersecurity. Unlike traditional methods, machine learning models can analyze large volumes of network traffic, identify patterns, and detect anomalies in real-time. By continuously learning from data, these models can adapt to new attack strategies, improving the ability to predict and prevent cyber breaches before they occur. This proactive approach helps organizations strengthen their security posture and respond to threats more effectively.

Cyber attack prediction involves analyzing network activity and classifying it as either normal or potentially malicious. Machine learning models process various network parameters, such as connection types, data transfer rates, and access behaviors, to identify unusual activities that may indicate an attack. When integrated into cybersecurity systems, these models can provide real-time alerts, enabling security teams to take immediate action and mitigate potential threats before they cause significant harm.Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

One of the key advantages of machine learning in cyber attack prediction is its ability to handle vast and complex datasets. Modern cyber threats generate massive amounts of data, making manual monitoring and traditional rule-based systems inefficient. Machine learning algorithms, however, can efficiently process and extract valuable insights from this data, improving threat detection accuracy and reducing false alarms. This capability is crucial in safeguarding sensitive information and ensuring the stability of digital infrastructure.

One of the key advantages of machine learning in cyber attack prediction is its ability to handle vast and complex datasets. Modern cyber threats generate massive amounts of data, making manual monitoring and traditional rule-based systems inefficient. Machine learning algorithms, however, can efficiently process and extract valuable insights from this data, improving threat detection accuracy and reducing false alarms. This capability is crucial in safeguarding sensitive information and ensuring the stability of digital infrastructure.

Additionally, machine learning-based cybersecurity solutions can be deployed as APIs, allowing seamless integration with existing security frameworks. This enables organizations to enhance their threat detection capabilities without completely overhauling their current security infrastructure. By leveraging AI-driven security systems, businesses can proactively monitor their networks, detect potential breaches, and take preventive measures before attackers can exploit vulnerabilities.



The growing reliance on cloud computing, the Internet of Things (IoT), and remote work environments further emphasizes the need for advanced cyber attack prediction mechanisms. With more devices and users connected to the internet, the attack surface continues to expand, increasing the risk of cyber threats. Implementing AI-powered security solutions can help organizations protect their digital assets and ensure the privacy and safety of their users.

II. OBJECTIVE

The goal of this project is to create a machine learning model that can predict cyber attacks by analyzing network traffic, improve its accuracy through feature engineering and data preprocessing, evaluate its effectiveness using key metrics, and deploy it as an API for real-time threat monitoring. Ultimately, this will contribute to better cybersecurity and help protect systems from potential breaches.

III. RELATED WORK

These are the related works done by the other researchers Xiaoming Li, Xianfu Wang, and Zhiyuan Ma's [1] study discusses the application of machine learning models, particularly Random Forest and Gradient Boosting Machines (GBM), in predicting cyber attack breaches. The study highlights that the Random Forest classifier performs well with an accuracy of 97%, while Gradient Boosting offers better precision in detecting low-frequency attacks. The research suggests that ensemble methods, such as Random Forest, outperformed traditional classifiers like Support Vector Machines (SVM) and Logistic Regression.

Anand V, N. Karthikeyan, and K. S. Rajasekar's [2] research provides an in-depth comparison of anomaly detection techniques for cyber attack prediction. Their work demonstrated the superior performance of LSTM-based models in identifying patterns in sequential network traffic data. The study further emphasized that LSTM outperforms conventional machine learning models like Decision Trees (DT) and Naive Bayes in detecting sophisticated attack patterns.

Rashid et al. [4] highlighted the importance of integrating deep learning architectures for cyber attack prediction, proposing a Convolutional Neural Network (CNN)-based framework. This research found that deep learning models, especially CNNs, provided better results than traditional machine learning models, including Random Forest and Logistic Regression, by identifying hidden patterns in high-dimensional security logs.

Pablo J. et al. [5] proposed the use of a hybrid genetic algorithm to optimize the performance of traditional classifiers like SVM and Random Forest in predicting cyber attack breaches. The proposed method included feature selection using the genetic algorithm to minimize overfitting, thereby improving the classifiers' robustness and accuracy. The hybrid model demonstrated an improvement in prediction accuracy by 8% compared to standard methods.

Vivek Sharma and Ravindra R. [6] compared various ensemble learning techniques for cyber attack detection. Their study found that models like Gradient Boosting and AdaBoost significantly outperformed single models like Decision Trees in terms of recall and F1 score. However, they also noted that the performance of ensemble methods highly depends on the quality of the feature engineering process.

Singh et al. [7] proposed an integrated machine learning pipeline to detect cyber attacks from network traffic data. The pipeline used feature extraction, feature selection, and classification stages to predict attack types with a focus on high-dimensional data. Random Forest and K-Nearest Neighbor (KNN) classifiers showed the best results, with an F1 score of 0.88 and 0.84, respectively.

Tiwari and Suresh [8] conducted a study on the detection of DDoS (Distributed Denial of Service) attacks using machine learning. The study found that while SVM performed adequately, ensemble techniques like Random Forest achieved higher precision and recall values, outperforming SVM in real-time detection systems for DDoS.

Chaudhary et al. [9] proposed an approach based on deep reinforcement learning (DRL) for predicting cyber attacks. By employing a multi-agent system, their model adapts to new attack types and improves prediction over time. The study suggested that DRL's adaptability could handle the evolving nature of cyber threats better than traditional machine learning models.

J. Soni et al. [10] discussed the use of neural networks, particularly Long Short-Term Memory (LSTM), for detecting cyber attack breaches in sequential data. Their results showed that LSTM models outperformed other algorithms like SVM, Naive Bayes, and Decision Trees by correctly identifying complex attack patterns in real-time network traffic analysis.Do not confuse “imply” and “infer”.

Kumar and Bhattacharya [11] proposed an approach for intrusion detection based on Hybrid Learning Models. By combining unsupervised learning techniques such as k-means clustering with supervised models like Decision Trees, they achieved better accuracy and F1 scores for anomaly-based attack detection in industrial systems.

Liang et al. [12] explored the use of adversarial machine learning in predicting cyber attacks. Their work focused on using adversarial training methods to improve the robustness of models like SVM, Random Forest, and Neural Networks, showing that adversarial attacks could expose weaknesses in traditional models, which adversarial methods could overcome.

A study by S. Verma and K. Kumar [13] evaluated the effectiveness of convolutional neural networks (CNNs) for cyber attack detection in IoT networks. The study revealed that CNNs performed exceptionally well in identifying malicious activities in highly noisy IoT environments, outperforming traditional models like Logistic Regression and SVM.

Chakraborty et al. [14] developed a framework based on ensemble learning techniques to predict cyber breaches. Their model combined classifiers like Random Forest, AdaBoost, and XGBoost, and was tested on large-scale cybersecurity datasets. The ensemble method significantly improved detection accuracy and reduced false positives in breach prediction.

Saxena et al. [15] utilized support vector machines (SVM) and decision trees for predicting cyber attack breaches in cloud computing environments. The paper highlights that SVM, when combined with feature selection methods like Principal Component Analysis (PCA), was the most effective in detecting anomalous behavior in cloud-based systems

IV. METHODOLOGY

We require a Significant quantity of data To predict cyber attack breaches, we gather extensive data from past network and system incidents, apply data protection techniques like Principal Component Analysis (PCA), and use a Random Forest Classifier to detect potential threats.

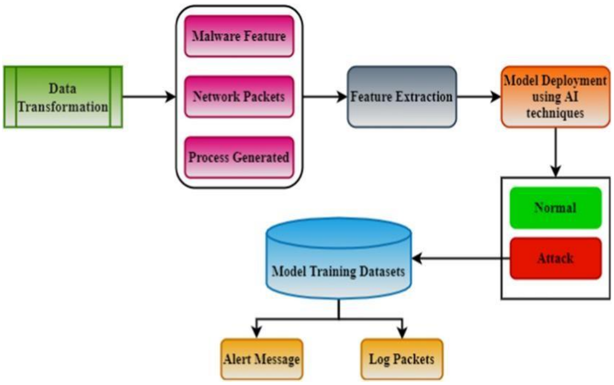


Figure 1 process flow

A. *CICIDS2017 Dataset*

Our dataset for cyber attack breaches prediction contains records of past network activities, including both normal and malicious traffic. Each record includes various network features such as port numbers, packet counts, flow duration, and other key indicators that help identify potential cyber threats. The dataset is labeled, meaning each entry is marked as either a normal activity or an attack, helping the machine learning model learn patterns and distinguish between safe and harmful activities. Since real-world data is often imbalanced, where attack cases are fewer than normal ones, techniques like SMOTE (Synthetic Minority Over-sampling Technique) may be used to balance the dataset, ensuring better model performance.

B. *Preprocessing and visualization*

During preprocessing for cyber attack breaches prediction, we start by cleaning the dataset by removing duplicates and handling missing values to ensure data consistency. We then perform feature selection to retain the most relevant attributes for attack detection. Categorical variables are encoded into numerical formats, and numerical features are normalized or standardized to improve model performance. Additionally, data balancing techniques like SMOTE are applied if the dataset is imbalanced to ensure fair learning. Finally, the dataset is split into training and testing sets for model evaluation.

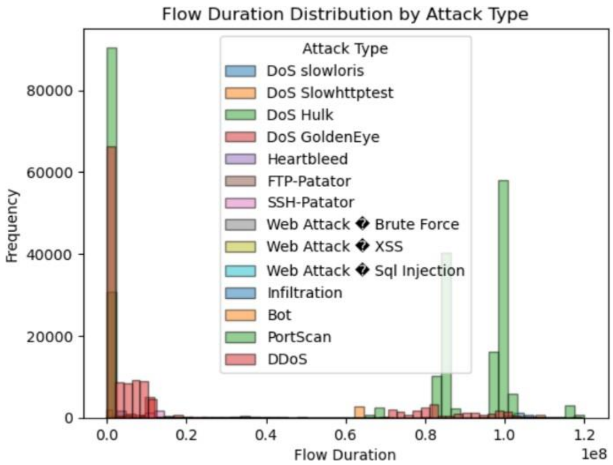


Figure 2 flow duration

The code first removes all benign (normal) network traffic from the dataset, leaving only malicious attack data. It then identifies all unique attack types and iterates through each one, creating a histogram to visualize the distribution of flow durations for each type of cyberattack. The alpha=0.5 parameter makes the bars semi-transparent, allowing overlapping distributions to be seen more clearly, while edgecolor='black' ensures each bar is outlined for better distinction. The final plot provides insights into how different cyberattacks behave in terms of duration, helping in understanding patterns and identifying anomalies in network traffic.

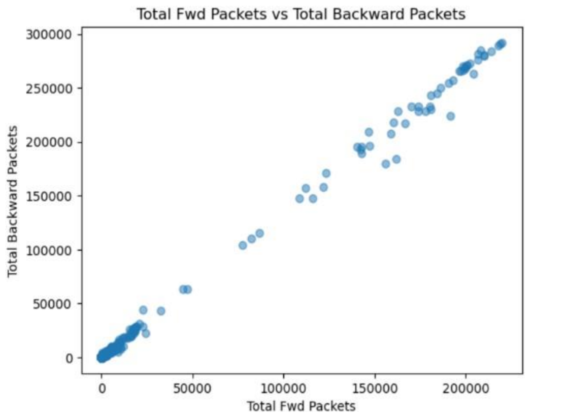


Figure 3 FWD packets vs Backward packets

This scatter plot helps analyze network traffic patterns by comparing the number of packets sent forward (from the source) and backward (from the destination). The strong positive correlation suggests that most network connections involve a nearly proportional exchange of packets, which is expected in normal communications. However, deviations from this trend could indicate anomalies, such as cyberattacks, where an unusually high or low number of packets in one direction may suggest malicious activity, such as Distributed Denial-of-Service (DDoS) attacks, port scanning, or other network intrusions. This visualization aids in identifying such irregular patterns for cybersecurity analysis.

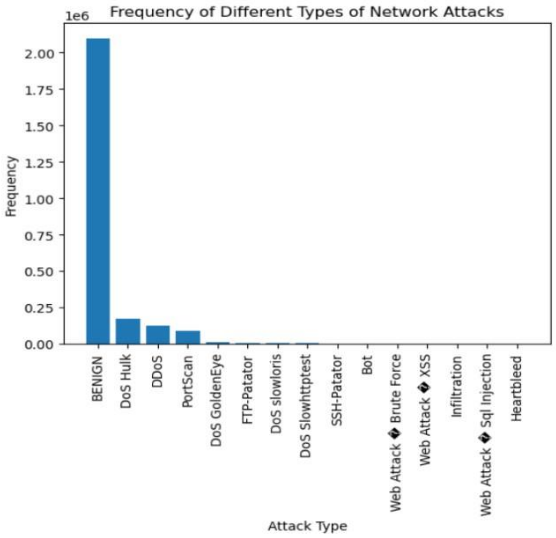


Figure 4 types of attacks

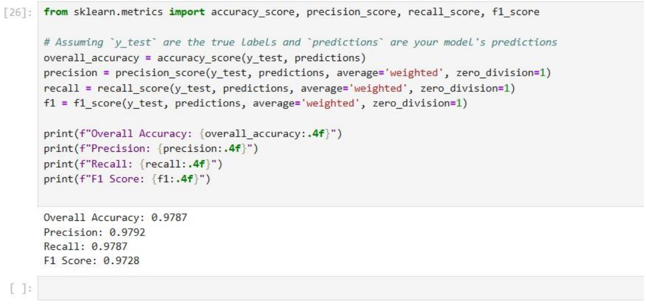
The bar chart shows that normal (BENIGN) traffic is by far the most common, followed by several Denial-of-Service (DoS) attacks like Hulk, DDOS, PortScan, GoldenEye, Slowloris, and Slowhttptest, indicating a need for strong defenses against these common disruptions. It also reveals brute-force login attempts targeting FTP and SSH services, as well as web application attacks such as Brute Force, XSS, and SQL Injection, highlighting the importance of web application security measures. The detection of the Heartbleed vulnerability suggests this specific exploit was targeted at some point. While these attack types provide insight into potential security threats.

C. *Model trained*

Random Forest is a supervised learning algorithm commonly used for classification problems. It works by creating multiple decision trees and then using a majority vote from these trees to classify data. For datasets with continuous values, Random Forest can easily handle them, making it a versatile tool for different types of data. While it is often used for classification tasks, Random Forest can also be applied to regression problems where the goal is to predict numerical values. The model combines the predictions from individual trees, represented as

$g(x) = f0(x) + f1(x) + f2(x) + ...$ to make a final decision or prediction.

V. RESULT

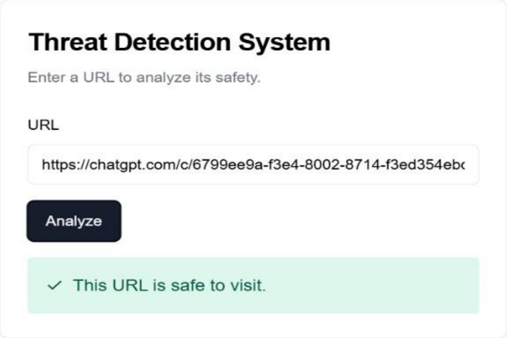


```
[26]: from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score

      # Assuming `y_test` are the true labels and `predictions` are your model's predictions
      overall_accuracy = accuracy_score(y_test, predictions)
      precision = precision_score(y_test, predictions, average='weighted', zero_division=1)
      recall = recall_score(y_test, predictions, average='weighted', zero_division=1)
      f1 = f1_score(y_test, predictions, average='weighted', zero_division=1)

      print(f"Overall Accuracy: {overall_accuracy:.4f}")
      print(f"Precision: {precision:.4f}")
      print(f"Recall: {recall:.4f}")
      print(f"F1 Score: {f1:.4f}")

      Overall Accuracy: 0.9787
      Precision: 0.9792
      Recall: 0.9787
      F1 Score: 0.9728

[ ]:
```

Figure 5 Result

The model's performance metrics reveal that it is highly effective in predicting the correct class. The overall accuracy of 97.87% means the model correctly classified almost 98% of the instances in the test set, but this metric alone might not tell the full story, especially if the dataset has an imbalance between classes. Precision of 97.92% shows that when the model predicted a positive class, it was almost 98% accurate, which is crucial when false positives can be costly, such as in situations where incorrect positive predictions could lead to unnecessary actions. Recall of 97.87% indicates that the model was able to correctly identify nearly 98% of the actual positive cases, which is important when missing a positive case (false negative) would be problematic. The F1 score of 97.28% provides a balanced view of the model’s performance, combining both precision and recall. However, while these results suggest strong performance, it's essential to consider the context of the problem, such as possible data biases or the costs of different types of errors, as high accuracy doesn’t always mean a perfect model.

Overall Accuracy: 0.9787
Precision: 0.9792
Recall: 0.9787
F1 Score: 0.9728



Threat Detection System

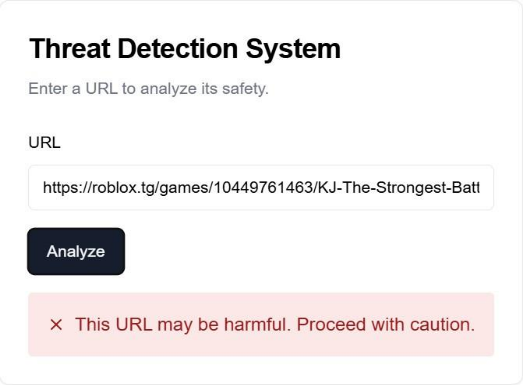
Enter a URL to analyze its safety.

URL

https://chatgpt.com/c/6799ee9a-f3e4-8002-8714-f3ed354eb

✓ This URL is safe to visit.

Our Threat Detection System helps keep users safe online by quickly checking whether a website is safe before they visit it. Users simply enter a URL, and the system takes care of the rest. It works by checking the URL against known lists of harmful websites, analyzing its structure and characteristics, and using advanced machine learning models to spot signs of phishing, malware, and other online threats. Once the analysis is done, the system provides clear feedback. If the website is safe, users will see a reassuring "This URL is safe to visit" message with a green checkmark. This gives users the confidence to browse the web without worrying about cyber threats. The system is designed to be flexible, so it can be improved in the future by adding new threat data and updating its machine learning models to keep up with new security risks.



Threat Detection System

Enter a URL to analyze its safety.

URL

https://roblox.tg/games/10449761463/KJ-The-Strongest-Batt

× This URL may be harmful. Proceed with caution.

Our Threat Detection System helps keep users safe online by quickly checking whether a website is safe before they visit it. Users simply enter a URL, and the system takes care of the rest. It works by checking the URL against known lists of harmful websites, analyzing its structure and characteristics, and using advanced machine learning models to spot signs of phishing, malware, and other online threats. Once the analysis is done, the system provides clear feedback. If the website is safe, users will see a reassuring "This URL is safe to visit" message with a green checkmark. If the URL is deemed harmful, users will see a warning message: "This URL is harmful. Proceed with caution," so they can make informed decisions. The system is designed to be flexible, so it can be improved in the future by adding new threat data and updating its machine learning models to keep up with new security risks.

REFERENCES

[1] Rani, P., Nag, A. K., & Shahriyar, R. (2024). A Data- Driven Classification Framework for Cybersecurity Breaches. IT Professional, 26(2), 39-48.

[2] Bakar, A. A., & Zolkipli, M. F. (2023). Cyber Security Threats and Predictions: A Survey. International Journal of Advances in Engineering and Management (IJAEM), 5(2)

[3] RAO, M. P. N., & DEVISETTY, M. L. D. N. V. Cyber

Hacking Breaches Prediction and Detection Using Machine Learning.

[4] Pujitha, K., Nandini, G., Sree, K. T., Nandini, B., & Radhika, D. (2023, May). Cyber hacking breaches prediction and detection using machine learning. In 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN) (pp. 1-6). IEEE.

[5] AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on

future cyber-attacks and related cybersecurity measures. momentum, 3(14), 15.

[6] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.

[7] Zhang, H., Zhou, Y., Liu, S., & Jiang, Y. (2019). A hybrid deep learningbased model for cyberattack detection in the industrial internet of things. IEEE Access, 7, 185160-185173.

[8] Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A.

A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security, 31(3), 357-374.

[9] Aminanto, M. E., & Kim, K. (2017). Deep learning in intrusion detection system: An overview. Journal of Computer Sciences and Applications,5(4), 140-146.

[10]Sahu, M., & Tomar, S. (2021). Cybersecurity and machine learning: Recent applications and trends. Cybersecurity, 4(1), 1-22

[11]Chen, L., Wang, W., & Zhang, J. (2020). A machine learning-based framework for cybersecurity threat detection. Journal of Computer Security, 28(3), 457-473.

[12]Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[13]Raza, S., & Zeeshan, S. (2018). Anomaly detection in network traffic using machine learning algorithms. Journal of Cybersecurity, 4(2), 102-110.

[14]Tang, L., Li, J., & Xu, Z. (2021). A hybrid machine learning model for cyberattack prediction in industrial control systems. IEEE Transactions on Industrial Informatics, 17(9), 6311-6320.

[15]Nwankpa, C., & Ijomah, W. (2022). Predicting cyber threats in the cloud computing environment using machine learning. International Journal of Cloud Computing and Services Science, 11(1), 44-58.