Comparative Analysis of SVM, Naïve Bayes, and Logistic Regression in Detecting IoT Botnet Attacks

Apri Siswanto[1], Luhur Bayu Aji[2], Akmar Efendi[3], Dhafin Alfaruqi[4], M. Rafli Azriansyah[5], Yefrianda Raihan[6]
Informatics Department-Faculty of Engineering, Universitas Islam Riau, Pekanbaru, Indonesia[1, 3, 4, 5, 6]
Faculty Data Science and Information Technology, INTI International University, Malaysia[2]

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices has significantly increased the risk of cyberattacks, particularly botnet intrusions, which pose serious security threats to IoT networks. Machine learning-based Intrusion Detection Systems (IDS) have emerged as effective solutions for detecting such attacks. This study presents a comparative analysis of three widely used machine learning classifiers—Support Vector Machine (SVM), Naïve Bayes (NB), and Logistic Regression (LR)—to assess their performance in detecting IoT botnet attacks. The experiment uses the BoTNeTIoT-L01 dataset, applying preprocessing techniques such as data cleaning, normalization, and feature selection to enhance model accuracy. The models are trained and evaluated based on standard performance metrics, including accuracy, precision, recall, F1-score, and AUC-ROC. The results indicate that SVM outperforms the other classifiers in terms of detection accuracy and robustness, particularly in detecting malware based on PE files. These findings offer valuable insights into selecting suitable machine learning models for securing IoT environments. Future work will further explore integrating advanced feature selection techniques and deep learning models to improve detection performance.**

***Keywords*—IoT security; botnet detection; machine learning; intrusion detection system; comparative analysis; SVM; naïve bayes; logistic regression**

I. Introduction

The rise of the Internet of Things (IoT) has revolutionized various industries by enabling seamless connectivity and automation. However, the rapid expansion of IoT networks has also introduced significant security challenges, particularly the increasing prevalence of botnet attacks. These attacks compromise vulnerable IoT devices, integrating them into a network of malicious bots that can be used for large-scale cyber threats such as Distributed Denial of Service (DDoS) attacks, data exfiltration, and unauthorized access. Traditional security mechanisms, such as signature-based intrusion detection systems (IDS) and firewalls, often fail to detect sophisticated and evolving IoT botnets due to their dynamic nature and high traffic volume [1], [2]. As a result, machine learning (ML)-based approaches have emerged as a promising solution for enhancing IoT security by identifying malicious patterns in network traffic. Despite the effectiveness of ML models, there is a need for a comprehensive comparison of their performance in detecting IoT botnet attacks [3], [4]. This study addresses this gap by analyzing and comparing three widely used ML classifiers—Support Vector Machine (SVM), Naïve Bayes (NB), and Logistic Regression (LR)—to determine their effectiveness in securing IoT environments.

Despite the growing adoption of machine learning techniques in IoT security, there remains a lack of recent comparative studies evaluating the performance of different classification algorithms in detecting IoT botnet attacks [5], [6]. While several studies have explored the application of SVM, NB, and LR individually, limited research has systematically compared their effectiveness using standardized evaluation metrics on modern IoT botnet datasets. Given the evolving nature of cyber threats, it is crucial to reassess the capabilities of these algorithms to determine their suitability for real-world IoT intrusion detection systems [7]. A thorough comparison can provide valuable insights into the strengths and limitations of each model, helping researchers and practitioners select the most appropriate approach for securing IoT environments [8]. This study aims to fill this gap by conducting a comprehensive performance analysis of SVM, NB, and LR in detecting IoT botnet attacks, considering key evaluation metrics such as accuracy, precision, recall, F1-score, and AUC-ROC [9].

The primary objective of this study is to analyze and compare the performance of three widely used machine learning algorithms—SVM, NB, and LR—in detecting IoT botnet attacks. To achieve this, the research utilizes a publicly available IoT botnet dataset and applies preprocessing techniques such as data cleaning, normalization, and feature selection to optimize model performance. Each algorithm is trained and tested using a standardized evaluation framework, with performance assessed based on key metrics, including accuracy, precision, recall, F1-score, and AUC-ROC [10], [11]. By conducting a systematic comparison, this study aims to identify the most effective classification model for IoT botnet detection, highlight the strengths and limitations of each approach, and provide recommendations for improving intrusion detection systems in IoT environments.

This study makes several key contributions to IoT security by conducting an in-depth comparative analysis of machine learning models for botnet attack detection. First, it utilizes a publicly available or private IoT botnet dataset, ensuring a realistic and diverse representation of attack patterns. Second, it evaluates the performance of three widely used classifiers—SVM, NB, and LR—using rigorous experimental settings and standardized performance metrics, including accuracy, precision, recall, F1-score, and AUC-ROC. Through this evaluation, the study provides a clear assessment of each model's strengths and weaknesses in identifying IoT botnet attacks. Finally, based on the results, this research offers recommendations on the most suitable machine learning model for IoT intrusion detection, contributing valuable insights to

both researchers and practitioners in enhancing the security of IoT environments.

The rest of this paper is organized as follows: Section II reviews related work on IoT botnet detection and machine learning-based intrusion detection systems (IDS). Section III outlines the research methodology, including dataset selection, preprocessing techniques, model training, and evaluation metrics. Section IV presents the experimental results and a comparative analysis of the three machine learning models. Finally, Section V provides the conclusions of this study and discusses potential directions for future research.

II. Related Work

A. IoT Botnet Attack Detection

The rapid adoption of IoT devices has led to a significant increase in security threats, particularly in botnet attacks that exploit vulnerabilities in connected systems. Various approaches have been proposed to detect IoT botnet activities, including rule-based IDS, anomaly detection techniques, and machine learning-based classification methods. Traditional IDS typically relies on predefined signatures and heuristics to identify malicious traffic; however, they often struggle with zero-day attacks and the evolving behaviors of botnets [12]. Anomaly detection methods can identify new threats by detecting deviations from normal behavior, but they frequently suffer from high false positive rates, which can hinder their effectiveness in real-world applications [13]. Consequently, machine learning (ML) has garnered attention as a promising method for enhancing IoT security, given its ability to learn patterns from large-scale network traffic data and distinguish between normal and malicious activities [14].

B. Machine Learning for Intrusion Detection in IoT

Supervised learning techniques, including SVM, NB, and LR, have been widely employed in IoT security applications. SVM is particularly noted for its robustness in high-dimensional spaces and its capability to handle non-linearly separable data, making it suitable for complex IoT environments [15]. NB, while computationally efficient, it operates under the assumption of feature independence, which may not always hold true in real-world network traffic data [16]. LR, a probabilistic model, is often utilized for binary classification tasks and offers interpretable decision boundaries, which can be advantageous in understanding the underlying decision-making process [17]. Prior studies have successfully applied these models to IDS, demonstrating promising results in identifying network-based attacks [18]. However, the comparative performance of these classifiers, specifically in the context of IoT botnet detection, remains an area that requires further investigation.

C. Comparative Studies on ML-Based IDS

Several research works have explored the effectiveness of ML classifiers for intrusion detection. For instance, Gu et al. evaluated the performance of SVM and NB in detecting network anomalies, concluding that SVM achieved higher accuracy but required significant computational resources [19]. Similarly, Mohammed et al. compared LR with deep learning models for malware detection, highlighting the trade-offs between interpretability and classification performance [20]. However, these studies primarily focused on general cyber security threats and did not specifically address IoT botnet attacks. Furthermore, variations in datasets, preprocessing techniques, and evaluation metrics complicate the generalization of their findings [21].

D. Research Gap and Contribution

The increasing ubiquity of IoT devices has raised significant concerns regarding the security of these systems, particularly regarding botnet attacks. Despite the growing body of literature on ML applications for detecting such attacks, there remains a dearth of comprehensive comparative studies systematically evaluating the performance of key classifiers, SVM, NB, and LR, tailored explicitly for IoT environments using contemporary datasets and standardized performance metrics. This presents a critical gap in understanding how these algorithms perform against each other in the specific context of IoT botnet detection.

Various studies have investigated different machine learning algorithms for intrusion detection within IoT frameworks. For instance, Al-Sarem et al., discussed various machine learning methods for botnet attack detection, including SVM and Naïve Bayes, but did not provide a direct comparative analysis between these classifiers within a unified experimental setup [6]. Additionally, Noor et al. highlighted that while many classifiers achieve high accuracy in other domains, systematic comparisons of SVM, NB, and LR in detecting IoT-specific botnet behaviors are severely lacking [22]. More directly related, Almomani et al. employed these classifiers for denial-of-service attack detection in IoT contexts and emphasized the need for rigorous and comparative evaluations across different algorithms [23].

Research conducted by Padhiar and Patel attempted to evaluate multiple machine learning algorithms for botnet detection, yet the focus was primarily on the efficacy of their proposed method without an in-depth comparative performance analysis of SVM, NB, and LR [24]. Furthermore, studies that analyze the comparative metrics of machine learning classifiers in other contexts indicate that a focused comparative study for IoT botnet detection is necessary. For instance, Das et al. demonstrated notable variances in accuracy and precision among several classifiers, including NB, SVM, and LR, in different classification tasks [25]. A similar comparative effort focusing on IoT botnet detection would clarify the strengths and weaknesses inherent in each algorithm regarding detection efficiency and accuracy.

In summary, the existing literature highlights the prevalence of individual algorithm studies but points out a void in systematic, comparative research involving SVM, NB, and LR in the context of IoT botnet detection. Such a study would not only enhance the understanding of which classifier effectively identifies botnet traffic but also set a precedent for applying standardized metrics to evaluate machine learning techniques across different cyber threat domains. This study aims to fill this gap by conducting a comprehensive performance analysis of these three classifiers using key evaluation metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. The findings of this research will provide insights into the suitability of different ML models for real-world IoT security applications and contribute to the development of more robust intrusion detection systems.

III. RESEARCH METHOD

A. Dataset

To evaluate the performance of machine learning models in detecting IoT botnet attacks, this study utilizes a publicly available IoT botnet dataset. Commonly used datasets for network intrusion detection include CTU-13, UNSW-NB15, and Bot-IoT, each containing labeled traffic data distinguishing between normal and malicious activities. Among these, the Bot-IoT dataset is particularly relevant, as it provides a comprehensive set of network traffic logs, including botnet-related attacks such as Distributed Denial of Service (DDoS), data exfiltration, and reconnaissance activities Meidan et al. [26] Injadat et al. [27]. The dataset contains various network features, such as packet size, flow duration, source and destination IP addresses, and protocol types, which serve as input for the classification models [28].

B. Data Preprocessing

The dataset undergoes several preprocessing steps before training the machine learning models to enhance classification accuracy. First, data cleaning is performed to remove duplicate records, missing values, and inconsistencies, ensuring the integrity of the dataset [29]. Next, normalization is applied to standardize numerical features, ensuring that all attributes are within the same scale to prevent bias during training [30]. Additionally, feature selection is conducted to retain the most relevant attributes while reducing dimensionality, which improves computational efficiency. Techniques such as correlation-based filtering and Principal Component Analysis (PCA) are employed to identify and retain high-impact features [31]. The final preprocessed dataset is split into training and testing sets for model evaluation.

C. Machine Learning Models

This study compares the performance of three widely used supervised learning algorithms: SVM, NB, and LR. SVM is a robust classifier that constructs an optimal decision boundary by maximizing the margin between different classes, making it particularly effective for high-dimensional datasets. However, its computational complexity may pose challenges when dealing with large-scale IoT traffic data [32]. NB, a probabilistic classifier based on Bayes' theorem, assumes feature independence and is computationally efficient, making it suitable for real-time applications. Despite its speed, the accuracy of NB may be affected by the independence assumption, which does not always hold in real-world network traffic data [33]. LR, a statistical model used for binary classification, estimates the probability of an instance belonging to a particular class using a sigmoid function. While simple and interpretable, its performance may be limited when handling complex, nonlinear attack patterns [33].

D. Experimental Setup

The dataset is split into 80% training and 20% testing to assess the generalization capabilities of the models. Additionally, 10-fold cross-validation is performed during training to ensure robust performance assessment and prevent overfitting. Each machine learning model undergoes hyperparameter tuning to optimize its classification performance. For SVM, kernel functions such as linear, radial basis function (RBF), and polynomial are tested to determine the best decision boundary for separating normal and malicious traffic. In the case of Naïve Bayes, both Gaussian and Multinomial variants are explored, depending on the nature of the feature distributions. For Logistic Regression, L1 and L2 regularization techniques are applied to prevent overfitting and improve model generalization. The models are implemented using Python's scikit-learn library, leveraging optimized libraries to enhance computational efficiency [34].

E. Evaluation Metrics

Five key evaluation metrics comprehensively assess model performance: accuracy, precision, recall, F1-score, and AUC- ROC. Accuracy measures the overall correctness of the classification, providing a general assessment of model effectiveness. Precision evaluates the proportion of correctly predicted positive instances, ensuring that false positives are minimized. Recall assesses the model's ability to correctly identify actual botnet attacks, which is critical for intrusion detection systems. F1-score, as the harmonic mean of precision and recall, provides a balanced measure when there is an uneven class distribution. Lastly, AUC-ROC (Area Under the Receiver Operating Characteristic Curve) quantifies the classifier's ability to distinguish between botnet and normal traffic across different threshold values [35]. By analyzing these metrics, this study aims to determine the most effective machine learning model for IoT botnet detection, offering insights into their suitability for real-world intrusion detection applications. These metrics comprehensively assess each model's strengths and weaknesses in detecting IoT botnet attacks. The evaluation results will determine the most effective machine learning approach for intrusion detection in IoT environments. For more details on the research method stages, see Fig. 1.

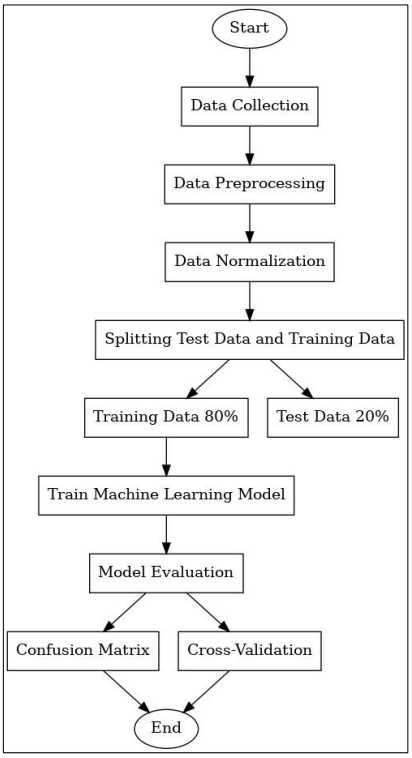

Fig. 1. Research steps.

IV. RESULTS

A. Experimental Results

The performance of the three machine learning models- SVM, Naïve Bayes (NB), and Logistic Regression (LR)—was evaluated using accuracy, precision, recall, F1-score, and AUC- ROC metrics. Table I summarizes the comparative performance of each model based on the test dataset.

TABLE I. THE EXPERIMENTAL RESULTS

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
SVM	95.2%	94.8%	96.1%	95.4%	96.7%
NB	89.6%	88.3%	90.7%	89.5%	91.2%
LR	91.8%	91.2%	92.1%	91.6%	92.9%

B. Confusion Matrix

Confusion matrices were employed to further illustrate the classification performance of each model by detailing the correctly and incorrectly classified instances. Additionally, Receiver Operating Characteristic (ROC) curves were plotted to evaluate the trade-off between the true positive rate and false positive rate. Among all models, the Support Vector Machine (SVM) exhibited the highest Area Under the ROC Curve (AUC- ROC), indicating superior capability in distinguishing between IoT botnet traffic and normal network activity.

As a standard evaluation metric, the confusion matrix enables a comprehensive assessment by comparing predicted class labels against actual ground truth values, thereby highlighting classification accuracy and misclassification patterns. Fig. 2 presents the confusion matrices of the Naïve Bayes (NB), Logistic Regression (LR), and SVM classifiers. The SVM achieved the best performance with the lowest number of false negatives (FN = 7) and false positives (FP = 17), demonstrating high precision in detecting both positive and negative classes. The LR model also showed competitive performance (FN = 71, FP = 9), offering a balanced trade-off between accuracy and computational efficiency. Conversely, the NB classifier yielded the highest FN count (208), indicating a frequent failure to detect botnet attacks and suggesting limited suitability for high-accuracy intrusion detection scenarios. Overall, SVM emerges as the most effective classifier when maximizing detection accuracy of malicious traffic is a primary requirement.

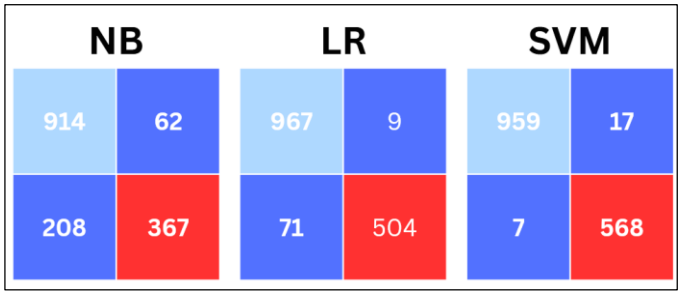

Fig. 2. Comparison of the confusion matrix of NB, LR, and SVM.

C. Cross Validation

Cross-validation was conducted to evaluate the models' consistency across different data splits. The average performance scores obtained from 10-fold cross-validation are:

- LR Model: Mean score = 0.95 (95%)
- SVM Model: Mean score = 0.92 (92%)
- NB Model: Mean score = 0.79 (79%)

These results reinforce the robustness and generalizability of each model. Fig. 3 illustrates the comparison of mean cross- validation scores.

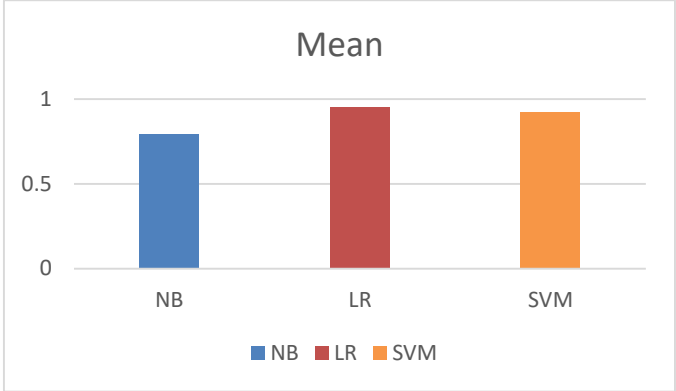

Fig. 3. Cross validation results.

V. DISCUSSION

The SVM demonstrated the best overall performance among the three evaluated models, achieving the highest accuracy (95.2%) and recall (96.1%). These results suggest that SVM is highly effective in correctly identifying IoT botnet attacks. Its superior performance can be attributed to its ability to handle high-dimensional feature spaces and construct optimal decision boundaries. However, despite its accuracy, the high computational complexity of SVM presents a challenge for real- time applications, particularly in resource-constrained IoT devices.

In contrast, LR did not outperform SVM in accuracy but exhibited a favorable balance between classification performance (91.8% accuracy) and computational efficiency. Due to its simple mathematical foundation and lower computational requirements, LR is a viable option for real-time intrusion detection systems, especially in edge or embedded environments where latency and resource limitations are critical factors.

While computationally efficient, NB achieved the lowest performance among the three models, with an accuracy of 89.6% and the highest number of false negatives (208), as indicated by the confusion matrix. This performance drawback is likely caused by the algorithm's assumption of conditional independence between features, which is often violated in complex network traffic patterns. Despite this limitation, NB remains suitable for scenarios prioritizing fast inference and minimal computational cost over high detection accuracy.

To ensure robust and unbiased evaluation, all models were assessed using k-fold cross-validation, which divides the dataset into multiple subsets for iterative training and testing. The results from cross-validation revealed that the LR model consistently achieved the highest average performance across folds, suggesting strong generalization capabilities. Although SVM slightly trailed LR in fold-wise averages, it maintained high overall accuracy. In contrast, NB showed the most significant variability in performance, reaffirming its limited suitability for complex classification tasks in IoT security contexts.

These findings underscore the importance of selecting machine learning models based on the specific constraints of the IoT deployment environment. SVM is recommended for offline or centralized processing scenarios where accuracy is the primary concern and computational resources are sufficient. Conversely, LR and NB are more suitable for real-time detection in on-device or edge computing settings, where lightweight and low-latency models are essential.

Given the strengths and limitations of each model, a hybrid architecture is worth exploring. Such an approach could employ SVM for periodic offline analysis and LR or NB for real-time, on-device detection. Furthermore, future work may investigate ensemble or hybrid learning strategies to combine the predictive power of multiple algorithms, aiming to optimize both accuracy and efficiency in intrusion detection systems tailored for IoT environments.

In conclusion, this study provides a comparative analysis of classical machine learning algorithms applied to detect IoT botnet attacks. The empirical findings offer valuable insights into model suitability across different operational contexts, thereby contributing to developing scalable, adaptive, and effective cybersecurity solutions in the IoT domain.

VI. Conclusion

This study presented a comparative analysis of SVM, NB, and LR in detecting IoT botnet attacks. Based on the experimental results, SVM demonstrated the highest accuracy (95.2%) and recall (96.1%), making it the most effective model for identifying botnet attacks. However, its computational complexity limits its feasibility for real-time intrusion detection on resource-constrained IoT devices. Logistic Regression provided a balanced trade-off between performance and efficiency, while Naïve Bayes, though the fastest model, showed lower accuracy due to its feature independence assumption. These findings suggest that model selection should consider detection accuracy and execution speed depending on the deployment environment.

Despite its contributions, this study has certain limitations. The performance of the models was evaluated using a single dataset, which may not fully capture the diversity of real-world IoT botnet attacks. Additionally, hyperparameter tuning was limited, and more advanced optimization techniques could further improve model performance. Future research could explore feature selection methods to enhance classification accuracy and reduce computational costs. Furthermore, implementing ensemble learning techniques, such as combining multiple classifiers, may provide more robust detection capabilities. Finally, testing these models on real-time network traffic in a dynamic IoT environment would be essential to validate their effectiveness against evolving cyber threats.

Acknowledgment

We express our deepest gratitude to the Universitas Islam Riau and all parties who have given us the opportunity and funding to complete this research. We would also like to express our sincere thanks to the editors and reviewers of the journal who provided invaluable feedback and guidance during the publication process of this paper. Their expertise, patience and commitment really help us improve the quality and clarity of our work. Finally, we thank our family for their understanding, patience, and constant encouragement at a time of greatest need.

References

[1] C. K. Ejeofobiri, O. O. Victor-Igun, and C. I. Okoye, "AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks," Asian Journal of Mathematics and Computer Research, vol. 31, pp. 40-55, 2024.

[2] M. Gelgi, Y. Guan, S. Arunachala, M. S. S. Rao, and N. Dragoni, "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques," Sensors, vol. 24, p. 3571, 2024.

[3] R. Zagrouba and R. AlHajri, "Machine Learning Based Attacks Detection and Countermeasures in IoT," International Journal of Communication Networks and Information Security (Ijcnis), vol. 13, 2022.

[4] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, "Botnet - based IoT Network Traffic Analysis Using Deep Learning," Security and Privacy, vol. 7, 2023.

[5] S. Pokhrel, H. Abbas, and B. Aryal, "IoT Security: Botnet Detection in IoT Using Machine Learning," 2021.

[6] M. Al-Sarem, F. Saeed, E. H. Alkhammash, and N. S. Alghamdi, "An Aggregated Mutual Information Based Feature Selection With Machine Learning Methods for Enhancing IoT Botnet Attack Detection," Sensors, vol. 22, p. 185, 2021.

[7] F. Hussain, S. G. Abbas, I. M. Pires, S. Tanveer, U. U. Fayyaz, N. M. García, et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," Ieee Access, vol. 9, pp. 163412-163430, 2021.

[8] A. H. Aljammal, A. Qawasmeh, A. Mughaid, S. Taamneh, F. Wedyan, and M. Obiedat, "Performance Evaluation of Machine Learning Approaches in Detecting IoT-Botnet Attacks," International Journal of Interactive Mobile Technologies (Ijim), vol. 17, pp. 136-146, 2023.

[9] S. M. Shagari, D. Gabi, N. M. Dankolo, and N. N. Gana, "Countermeasure to Structured Query Language Injection Attack for Web Applications Using Hybrid Logistic Regression Technique," Journal of the Nigerian Society of Physical Sciences, p. 832, 2022.

[10] S. Bagui, X. Wang, and S. Bagui, "Machine Learning Based Intrusion Detection for IoT Botnet," International Journal of Machine Learning and Computing, vol. 11, pp. 399-406, 2021.

[11] R. Kalakoti, S. Nõmm, and H. Bahşi, "In-Depth Feature Selection for the Statistical Machine Learning-Based Botnet Detection in IoT Networks," Ieee Access, vol. 10, pp. 94518-94535, 2022.

[12] B. Al - Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abedalqader, A. Rawash, and R. Fahmawi, "SIEM-based Detection and Mitigation of IoT-botnet DDoS Attacks," International Journal of Electrical and Computer Engineering (Ijece), vol. 10, p. 2182, 2020.

[13] X. Yu, C. Shan, J. Bian, X. Yang, Y. Chen, and H. Song, "AdaGUM: An Adaptive Graph Updating Model-Based Anomaly Detection Method for Edge Computing Environment," Security and Communication Networks, vol. 2021, pp. 1-12, 2021.

[14] A. Maqbool, "Intrusion Detection Using Network Traffic Profiling and Machine Learning for IoT," vol. 20, pp. 2140-2149, 2024.

[15] M. M. ŞİMŞEk and E. Atılgan, "DoS and DDoS Attacks on Internet of Things and Their Detection by Machine Learning Algorithms," Dümf Mühendislik Dergisi, 2024.

[16] D. Kurniadi, "The Application of Naive Bayes Method for Final Project Topic Selection Within the Project-Based Learning Framework in the Data Mining Course," Jurnal Educatio Jurnal Pendidikan Indonesia, vol. 10, p. 243, 2024.

[17] A. Setiawan, F. Setivani, and T. Mahatma, "Performance Comparison of Decision Tree and Logistic Regression Methods for Classification of SNP Genetic Data," Barekeng Jurnal Ilmu Matematika Dan Terapan, vol. 18, pp. 0403-0412, 2024.

[18] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-Based Intrusion Detection Systems for in-Vehicle Networks: A Survey," Acm Computing Surveys, vol. 55, pp. 1-40, 2023.

[19] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," Computers & Security, vol. 103, p. 102158, 2021/04/01/ 2021.

[20] M. Altaiy, I. Yildiz, and B. Uçan, "Malware Detection Using Deep Learning Algorithms," Aurum Journal of Engineering Systems and Architecture, vol. 7, pp. 11-26, 2023.

[21] I. E. Salem and K. H. Al-Saedi, "Malware detection based on deep learning approach in cloud computing," in AIP Conference Proceedings, 2024.

[22] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," Computational Intelligence and Neuroscience, vol. 2022, pp. 1-14, 2022.

[23] O. Almomani, A. Alsaaidah, A. A. A. Shareha, A. Alzaqebah, and M. A. Almomani, "Performance Evaluation of Machine Learning Classifiers for Predicting Denial-of-Service Attack in Internet of Things," International Journal of Advanced Computer Science and Applications, vol. 15, 2024.

[24] S. Padhiar and R. Patel, "Performance Evaluation of Botnet Detection Using Machine Learning Techniques," International Journal of Electrical and Computer Engineering (Ijece), vol. 13, p. 6827, 2023.

[25] S. Das, K. Bhattacharyya, and S. Sarkar, "Performance Analysis of Logistic Regression, Naive Bayes, KNN, Decision Tree, Random Forest and SVM on Hate Speech Detection From Twitter," International Research Journal of Innovations in Engineering and Technology, vol. 07, pp. 07-03, 2023.

[26] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, et al., "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, pp. 12-22, 2018.

[27] M. Injadat, A. Moubayed, and A. Shami, Detecting Botnet Attacks in IoT Environments: An Optimized Machine Learning Approach, 2020.

[28] A. Atadoga, E. O. Sodiya, U. J. Umoga, and O. O. Amoo, "A comprehensive review of machine learning's role in enhancing network security and threat detection," World Journal of Advanced Research and Reviews, vol. 21, pp. 877-886, 2024.

[29] S. Chalichalamala, N. Govindan, and R. Kasarapu, "A Comprehensive Analysis of Intrusion Detection in Internet of Things (IoT)," in 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), 2023, pp. 1-6.

[30] G. K. Baydoğmuş, "The effects of normalization and standardization an Internet of Things attack detection," Avrupa Bilim ve Teknoloji Dergisi, pp. 187-192, 2021.

[31] A. Kaur and K. Guleria, Feature Selection in Machine Learning: Methods and Comparison, 2021.

[32] T. Farid and M. Sirat, "Hybrid of supervised learning and optimization algorithm for optimal detection of IoT distributed denial of service attacks," International Journal of Innovative Computing, vol. 13, pp. 1-12, 2023.

[33] M. J. Gatea and S. M. Hameed, "An Internet of Things Botnet Detection Model Using Regression Analysis and Linear Discrimination Analysis," Iraqi Journal of Science, pp. 4534-4546, 2022.

[34] R. Chandrakar, R. Raja, R. Miri, U. Sinha, A. K. S. Kushwaha, and H. Raja, "Enhanced the moving object detection and object tracking for traffic surveillance using RBF-FDLNN and CBF algorithm," Expert Systems with Applications, vol. 191, p. 116306, 2022.

[35] S. Mishra and A. K. Tyagi, "The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications," in Artificial Intelligence-based Internet of Things Systems, S. Pal, D. De, and R. Buyya, Eds., ed Cham: Springer International Publishing, 2022, pp. 105-135.