Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 254 (2025) 68–77

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Digital Sovereignty (ICDS)

Enhancing IoT Resilience: Machine Learning Techniques for Autonomous Anomaly Detection and Threat Mitigation

Shashika Lokuliyana
Department of Computer System Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
shashika.l@sliit.lk

Deemantha Siriwardana
Department of Computer System Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
deemantha.s@sliit.lk

Kalupahanage A.G.A
Department of Computer System Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
it2100802@my.sliit.lk

Bulathsinhala D.N
Department of Computer System Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
it21013614@my.sliit.lk

Herath H.M.S.D
Department of Computer System Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
it21054990@my.sliit.lk

Herath H.M.T.M
Department of Computer System Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
it21001734@my.sliit.lk

Abstract

The explosive growth of the Internet of Things (IoT) has had a substantial impact on daily life and businesses, allowing for real-time monitoring and decision-making. However, increased connectivity also brings higher security risks, such as botnet attacks and the need for stronger user authentication. This research explores how machine learning can enhance Internet of Things security by identifying abnormal activity, utilizing behavioral biometrics to secure cloud-based dashboards, and detecting botnet threats early. Researchers tested numerous machine learning methods, including K-Nearest Neighbors (KNN), Decision Trees, Logistic Regression, and XGBoost on publicly available datasets. The Decision Tree model earned an impressive accuracy rate of 0.73 for anomaly identification, proving its supremacy in dealing with complex security risks, while the XGBoost model demonstrated strong performance with a 92% accuracy rate for detecting TCP SYN flood attacks. Research findings show the effectiveness of these strategies in enhancing the security and reliability of IoT devices. This study provides significant insights into the use of machine learning to protect IoT devices while also addressing crucial concerns such as power consumption and privacy.

© 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of the ICDS 2024 (General chairs and program committee Chairs)

Keywords: Internet of Things, machine learning, anomaly detection, botnet detection, behavioral biometrics, IoT security

1877-0509 © 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of the ICDS 2024 (General chairs and program committee Chairs)
10.1016/j.procs.2025.02.065

1. Introduction

The Internet of Things (IoT) has transformed how we interact with our environment, allowing smart homes to manage lighting and temperature, as well as industrial systems to improve production efficiency. IoT devices, with sensors and internet connections, allow for immediate monitoring and regulation in various areas such as healthcare, transportation, and agriculture. Nevertheless, the extensive connectivity and data-gathering capabilities that make IoT powerful also bring about significant security and privacy challenges.

With the rise of IoT devices, it has become more important to secure the data they produce and send. These devices frequently function on the outskirts of networks, gathering and transmitting confidential data on the internet. It is essential to protect the confidentiality, integrity, and availability of the data they manage, which may include personal health records and critical industrial metrics[2]. Regrettably, Many IoT devices are vulnerable to cyberattacks due to their limited processing capabilities, lack of robust security features, and operation in open networks.

Botnet attacks are a major risk to IoT systems [3]. A botnet consists of a collection of devices infected with malicious software, controlled by a hacker, capable of executing Distributed Denial of Service (DDoS) attacks, stealing data, and performing other harmful activities[4]. IoT devices are frequently targeted in cyber-attacks due to their lack of proper security and widespread availability [5]. The quick growth of IoT technology has given cybercriminals additional opportunities to exploit these weaknesses, resulting in a rise in botnet-related incidents [6].

Recent advancements in IoT security have focused on developing various detection mechanisms, including signature-based and anomaly-based methods, to counter emerging threats. Traditional approaches to cybersecurity often struggle to effectively address the complexity and ever-changing nature of modern cyberattacks on IoT devices. Signature-based methods depend on known threat patterns, rendering them ineffective against new and emerging attacks. On the other hand, anomaly-based methods frequently experience high false-positive rates due to IoT's diverse and dynamic environments. Additionally, conventional security solutions often cannot scale to manage the vast amounts of data generated by IoT devices and lack the adaptability necessary to keep pace with evolving attack techniques. This study aims to tackle these limitations by utilizing the XGBoost algorithm, which offers speed and accuracy for real-time detection of specific threats, such as TCP SYN flood attacks. Ultimately, this approach seeks to create a more resilient security framework for IoT infrastructure.

This proposed system stands out in its comprehensive approach to IoT security, as it not only detects anomalies, botnet activity, and DDoS attacks but also includes a robust mechanism for secure user authentication [36]. While many existing solutions focus solely on threat detection, our system addresses the full spectrum of security needs by ensuring that only authenticated users can access and interact with IoT devices. By integrating advanced authentication protocols alongside real-time threat detection, our system provides a layered security approach that strengthens IoT networks against unauthorized access and data breaches [37]. This comprehensive strategy accurately identifies potential threats and reduces risks associated with user impersonation and unauthorized access, thereby safeguarding the confidentiality, integrity, and availability of sensitive IoT data. [38].

To combat these risks, more and more researchers are relying on machine learning (ML) to boost IoT security [7]. Machine learning empowers systems to analyze data and recognize patterns that may suggest malicious behavior. For example, machine learning models can be taught to identify abnormal patterns in network data that might indicate the existence of a botnet or other cybersecurity incidents [8]. These models could constantly learn and adjust to emerging threats, offering an additional level of protection for IoT networks.

As IoT devices are increasingly adopted in sectors like healthcare, smart homes, and industrial automation, the need for robust cybersecurity measures has become more urgent. [10]. The TCP SYN flood attack poses a significant danger as a form of DDoS attack that focuses on disrupting the connection establishment process of devices on the internet [11]. These attacks have the potential to disturb IoT devices, resulting in service interruptions and notable financial damage [12]. Conventional security systems frequently have difficulty keeping pace with rapidly changing attacks, highlighting the value of ML techniques [13]. This study suggests using the XGBoost algorithm for

identifying TCP SYN flood attacks. XGBoost is a powerful machine-learning tool recognized for its quickness and precision, which makes it perfect for instantly identifying threats [14]. The model undergoes training and testing.

2. Literature review

The swift adoption of Internet of Things (IoT) devices has greatly improved areas like smart homes and industrial automation. However, it has also brought about significant security issues. Identifying abnormal behaviors, defending against botnet attacks, and guaranteeing safe user verification are the main obstacles. Researchers are more and more turning to machine learning (ML) methods to improve security in IoT in order to deal with these problems.

Recent studies have leveraged machine learning to enhance IDS capabilities in IoT [29]. For instance, a machine learning-based IDS for IoT networks demonstrates the effectiveness of sophisticated models in detecting diverse attack types. An ensemble model optimized with the Gray Wolf Optimizer combines multiple classifiers to improve accuracy and computational efficiency in complex IoT environments [30]. Further, hybrid approaches using metaheuristic optimization, such as Firefly and C5.0 algorithms, have shown potential in securing critical infrastructure by achieving high detection accuracy with minimal false positives [31]. These approaches underscore the effectiveness of advanced IDS models in enhancing IoT security, particularly in optimizing accuracy, reducing false alarms, and addressing IoT ecosystem needs.

The growing use of IoT devices has created an urgent need for effective intrusion detection systems (IDS) to protect against diverse and evolving threats. Recent advances in IoT anomaly detection emphasize machine learning and deep learning models for their ability to recognize complex traffic patterns, though challenges remain in handling device diversity, adapting to new threats, and achieving real-time detection in limited-resource settings [32]. Similarly, Khan et al. (2023) proposes a hybrid deep learning model for IDS, focusing on emergency management and combining different architectures to boost accuracy and resilience. This model addresses issues such as class imbalance and processing efficiency, yet the study calls for further refinement to support real-time, low-overhead operation [2]. Both studies underscore the promise of advanced models for IoT security while highlighting areas where further research is needed for real-world application [33].

A. Anomaly Detection in IoT Networks

With the increase in IoT devices, it is crucial to identify abnormalities in the large volumes of data they produce. Conventional rule-based methods are frequently insufficient because of the ever-changing and varied characteristics of IoT environments. On the other hand, advanced machine learning techniques provide better and quicker identification of security risks and system issues. Scholars have concentrated on creating frameworks that use edge computing for detecting anomalies in real-time [12], and on designing models that are lightweight and efficient for operating on devices with limited resources [13]. These methods aid in developing a stronger IoT security structure [14].

B. Botnet Attacks Detection in IoT

Botnet attacks are a major danger to IoT systems as they involve using compromised networks of devices to carry out widespread attacks. Many IoT devices are at high risk due to their open and limited-processing characteristics [3]. Machine learning methods such as K-Nearest Neighbors (KNN), Decision Trees, and Logistic Regression have displayed potential in spotting these attacks through the identification of abnormal patterns in network traffic [4]. Yet, there are still obstacles to overcome, including enhancing the models' ability to work effectively with various IoT devices and resolving the contradictions found in current studies.

C. **User Authentication Based on Behavioral Biometrics**

Conventional methods of authentication using passwords are no longer effective in defending against advanced cyberattacks. Behavioral biometrics is a potential substitute that examines distinct patterns in user interactions with their devices, such as mouse movements and keystroke dynamics [14]. These challenging and ever-

changing characteristics can improve security in IoT applications on the cloud, offering consistent and less disruptive authentication [15]. Incorporating these systems into network security frameworks provides an extra level of defense, especially from unauthorized internal entry.

D. **Detecting TCP SYN Flood Attacks**

TCP SYN flood attacks take advantage of the connection initiation process between devices, flooding servers and leading to service denial. IoT devices are at high risk because of their restricted resources and extensive use, which makes them vulnerable targets [11]. The detection of these attacks greatly relies on machine learning, particularly the XGBoost algorithm. XGBoost proves to be efficient for analyzing network traffic patterns and differentiating between regular and harmful behaviors [14], making it a suitable choice for instantaneous intrusion detection in IoT settings [15]. Training the model on thorough datasets such as UNSW_NB15 [7] enables it to accurately recognize and address these risks, guaranteeing the dependability and accessibility of IoT systems [8].

There are several technical shortcomings in current intrusion detection systems (IDS) for IoT networks, indicating a need for better solutions. Traditional methods, including signature-based and anomaly-based detection, often struggle with complex and evolving threats. Signature-based approaches tend to overlook new attacks, while anomaly-based models frequently produce high rates of false positives. Additionally, class imbalance in IoT datasets frequently results in biased models that may overlook critical, less common attack types. Many current solutions also lack scalability for real-time detection in resource-constrained devices and do not address secure user authentication, increasing vulnerability to unauthorized access.

3. Methodology

This study focuses on enhancing IoT security by targeting three main areas: identifying anomalies in IoT endpoint devices, detecting IoT botnet attacks, and improving user authentication with behavioral biometrics. The datasets utilized, developed models, preprocessing methods, and proposed systems are detailed in the subsequent sections

A. Datasets

1. IoT-23 Dataset: The IoT-23 dataset was used to detect anomalies in IoT networks [35]. This dataset comprises network traffic data from smart home devices, such as Amazon Echo, Philips HUE, and Somfy Door Lock. It contains both benign and malicious traffic, providing a comprehensive basis for training and testing anomaly detection models.

2. N-BaIoT Dataset: The N-BaIoT dataset was utilized for evaluating the efficacy of machine learning models in identifying botnet attacks [10]. This dataset includes traffic data from IoT devices infected with well-known malware such as Bashlite and Mirai.

3. Behavioral Biometric Dataset: Data was collected from users interacting with a cloud-based dashboard, including mouse movements and keystroke dynamics. This data was used to create behavioral profiles for user authentication [14].

Average Dwell Time (D_{avg}): The average Time s key is pressed:

$$D_{avg} = \frac{\sum_{k=1}^{m} t_{k,down} - t_{k,up}}{M}$$

Where $tk,down$ and tk,up are the times when key k is pressed down and released, respectively, and m Is the number of keystrokes.

Mean Flight Time (F_{mean}): the average time between releasing one key and pressing the next

$$F_{mean} = \frac{\sum_{k=1}^{m-1} t_{k+1\,down} - t_{k\,up}}{m-1}$$

Fig. 1. Keystroke Features

Mean Velocity (V_{mean}): the average speed of the mouse movement over a session, calculated as

$$v_{mean} = \frac{\sum_{i=1}^{n-1} \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}{n-1}$$

where (X_i, y_i) are the cursor coordinates at the i-th timestamp, and n is the number of recorded points.

Average Acceleration (A_{avg}): Calculated by differentiating the velocity between points:

$$A_{avg} = \frac{\sum_{i=1}^{n-2} |v_{i+1} - v_i|}{n-2}$$

Fig. 2. Mouse Dynamics Features

4. The UNSW-NB15 Dataset was used by the authors and was developed by the Australian Centre for Cyber Security (ACCS). This dataset includes a combination of normal and malicious network traffic, featuring SYN flood attacks. It has been divided into a training set and a test set for analysis. For this study, the Authors focused on the training set, which contains 175,341 records and 49 features, including various network flow characteristics.

B. Data Preprocessing

To address class imbalance in the dataset, several strategies were implemented to ensure balanced model performance. The dataset was split into 80% for training and 20% for testing, maximizing learning from the data while retaining sufficient evaluation samples. Resampling techniques, including SMOTE for oversampling minority classes and under sampling majority classes, were applied to balance the dataset and reduce bias. Additionally, class weights were adjusted during model training, giving higher importance to minority classes to enhance sensitivity toward underrepresented categories. Evaluation metrics beyond accuracy, such as F1 score, precision-recall curves, and AUC-PR, were used to gain a comprehensive view of the model's performance on imbalanced data.

Advanced algorithms like balanced random forests and boosting techniques, which handle imbalance more effectively, were incorporated, with stratified cross-validation ensuring each fold maintained the class distribution. Post-processing techniques, including threshold tuning, were also applied to increase recall for the minority class, improving detection of underrepresented instances. These combined approaches create a robust framework for accurate predictions across all classes, effectively mitigating the effects of class imbalance in the dataset.

IoT-23 Dataset : Loading and Sampling: Each of the 23 individual datasets was loaded into separate data frames using the Pandas library. A sample of 100,000 rows was extracted from each dataset to ensure manageability [12]. Combining Datasets: The sampled data frames were combined into a single dataset, "iot23_combined.csv," which preserved the diversity of network traffic while making the data more manageable for analysis [13]. Normalization: Features were normalized to ensure equal contribution in models like KNearest Neighbors (KNN), with values scaled between 0 and 1 [14] (Tables 1 and 2).

N-BaIoT Dataset : Handling Missing Data: Missing values in the dataset were imputed using the mean technique [10]. Class Imbalance: I made sure to remember the following text: "The Synthetic Minority Over-Sampling Technique (SMOTE) was used to tackle class imbalance.", particularly the underrepresentation of botnet traffic, by generating synthetic samples of the minority class [11].

Behavioral Biometric Data : Feature Extraction: Key metrics, such as mouse speed, acceleration, and keystroke timing, were extracted from the raw data to create feature vectors for the machine learning model [15].

UNSW-NB15 Dataset : In this process, Authors first performed feature selection by identifying and selecting features that are most relevant to detecting TCP SYN flood attacks, such as TCP flags, packet sizes, and flow duration [7]. Next, the target variable, which indicates whether a network record is benign or malicious, was encoded into

binary form, with 0 representing benign and 1 representing malicious activity [8]. Finally, Authors standardized the features to make sure they are all on the same scale., which helps improve the performance and accuracy of the XGBoost model during training [9].

C. Machine Learning Models

Anomaly Detection Model: Decision Tree-This model builds a tree structure by partitioning the data based on features that provide the most information gain, classifying network traffic as normal or anomalous [12]. Naive Bayes-Based on Bayes' theorem, this model calculates the probability of each class (normal or anomalous) given the feature values and classifies the traffic accordingly [14].

Botnet Detection Model: K-Nearest Neighbors (KNN): This model classifies data points based on the closest examples in the feature space, which is particularly useful after applying SMOTE to balance the dataset [4]. Decision Tree and Logistic Regression: These models were also employed to detect botnet activity, with SMOTE enhancing their performance by addressing class imbalance [6].

User Authentication Model: Behavioral Biometrics: The system uses a machine learning model to classify login attempts based on the user's mouse and keystroke dynamics. This model was integrated into the backend of the cloud dashboard's login system [16].

D. Proposed Systems

Anomaly Detection System: A traffic capture unit collects data from IoT devices, which is then sent to a compute unit (either a cloud or local computer) [12]. The compute unit applies the decision tree and Naive Bayes models to classify the data as normal or anomalous [14]. If an anomaly is detected, the system can trigger actions such as dropping packets or alerting users [15].

Botnet Detection System: The preprocessed N-BaIoT dataset, balanced with SMOTE, is used to train the machine learning models [11]. These models are then tested on their ability to detect botnet activity [12]. The system can predict whether network traffic is benign or part of a botnet [10].

User Authentication System: Behavioral data is collected during login attempts and processed by the machine learning model [15]. The system then decides whether to grant or deny access based on the user's interaction patterns [16]. The integration ensures that security measures do not impact the usability or performance of the dashboard [14].

TCP SYN Flood detection system: The XGBoost model, a decision-tree-based ensemble machine learning algorithm, was utilized in this study due to its efficiency, flexibility, and strong performance in a gradient boosting framework [9]. For optimal results, the Authors configured XGBoost with a learning rate of 0.1, a maximum tree depth of 6, 100 estimators, and a subsample ratio of 0.8 [8]. These parameters were carefully optimized through grid search and cross-validation techniques to achieve the best possible model performance [7]. The model was trained using the preprocessed dataset, and its performance was evaluated using key metrics such as accuracy, precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) [9]. Cross-validation was employed to ensure the robustness and reliability of the evaluation results [11].

Table 1. Variables and Definition for ZEEK files

Column	Description
ts	This is the time of the first packet
uid	A unique identifier of the connection
id	The connection's 4-tuple of endpoint addresses/ports
proto	The transport layer protocol of the connection
service	An identification of an application protocol
duration	How long the connection lasted
orig_bytes	The number of payload bytes the originator sent
resp_bytes	The number of payload bytes the responder sent
conn_state	Possible connection state values
local_orig	If the connection is originated locally, this will be T
local_resp	If the connection is responded locally, this will be T
missed_bytes	Indicates the number of bytes missed in content gaps
history	Records the state history of connections as a string
orig_pkts	Number of packets that the originator sent
orig_ip_bytes	Number of IP level bytes that the originator sent
resp_pkts	Number of packets that the responder sent
resp_ip_bytes	Number of IP level bytes that the responder sent
tunnel_parents	uid values for any encapsulating parent connections
orig_l2_addr	Link-layer address of the originator

Table 2. Counts of Attack Types for File IOT23

Label	Count
PartOfAHorizontalPortScan	825939
Okiru	262690
Benign	197809
DDoS	138777
Attack	3915
C&C-HeartBeat	349
C&C-FileDownload	43
C&C-Torii	30
FileDownload	13
C&C-HeartBeat-FileDownload	8
C&C-Mirai	1

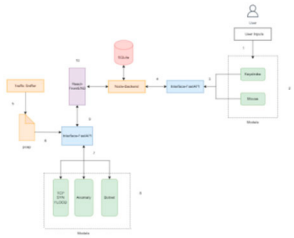

Fig. 3. Overall system diagram

The system (Fig. 3) begins with Step 1, where the user provides input through the User Input module, which collects data from keystrokes and mouse dynamics (Figures 1 and 2). The Keystroke and Mouse models analyze this behavioral input to verify the user's identity, ensuring secure authentication before granting access to the frontend interface.

Once authenticated, the system proceeds to monitor network traffic. The Traffic Sniffer captures network traffic data and stores it in pcap files, which are sent to the Interface-FastAPI module for processing. This interface directs the data to the three detection models: TCP SYN Flood Detection, Anomaly Detection, and Botnet Detection. Each model independently analyzes the traffic data to predict potential threats.

Finally, the processed data and prediction results from these models are displayed on the React-Frontend, providing real-time insights into the traffic status and alerting users to any suspicious activities detected within the network. This architecture() ensures both user authentication and continuous monitoring of network traffic to maintain IoT security.

4. Results and discussion

The efficiency of different machine learning models in identifying anomalies, detecting botnet attacks, and ensuring user authentication security in IoT networks was thoroughly assessed. During anomaly detection with the IoT-23 dataset, the Decision Tree model stood out as the best performer with an accuracy of 0.73, surpassing the Naive Bayes model, which only reached 0.30. The Decision Tree's capacity to detect intricate patterns in IoT network traffic, along with its fast processing time of around 3 seconds, makes it ideal for real-time anomaly detection. This study's findings support previous research, confirming the effectiveness of Decision Tree models in handling complex data relationships, particularly in settings with varied and changing network conditions.

Table 3. Comparison of Model Performance

System	Model	Dataset	Accuracy Score
Anomaly Detection	Decision Tree	IoT-23	73%
	Naive Bayes	IoT-23	30%
Botnet Detection	Decision Tree	N-BaIoT	99.997%
	KNN	N-BaIoT	99.996%
	Logistic Regression	N-BaIoT	84.581%
TCP SYN Flood Detection	XGBoost	UNSW_NB15	92%
User authentication and behavioral biometrics	XGBoost	Custom Dataset	92%

The evaluation of the Decision Tree, K-nearest neighbours (KNN), and Logistic Regression models for botnet detection using the N-BaIoT dataset revealed significant differences in performance (Table 3). The Decision Tree model demonstrated near-perfect efficacy with an accuracy of 99.997%, while the KNN model achieved comparably

high accuracy at 99.996%, albeit with slightly higher misclassification rates. Conversely, the Logistic Regression model exhibited a markedly lower accuracy of 84.581%, reflecting its limitations in accurately classifying specific traffic categories, particularly benign instances. These findings underscore the superior precision and reliability of advanced models like Decision Tree and KNN for addressing the complexities of botnet detection in IoT environments(Figures: 4-7).

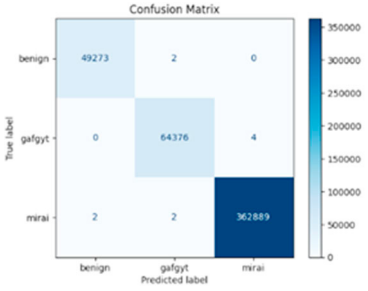

Fig. 4. Botnet Confusion Matrix

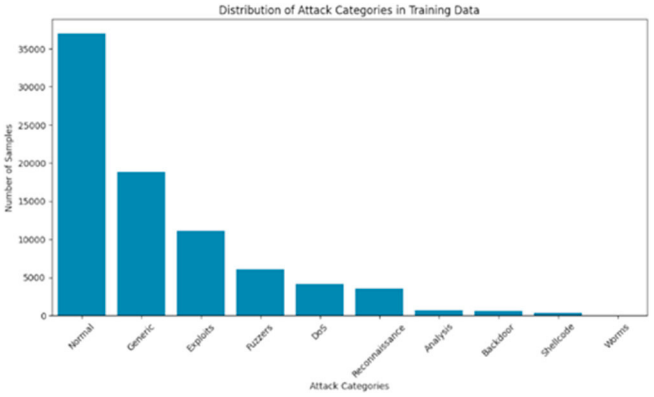

Fig. 5. Distribution of attacks matrix

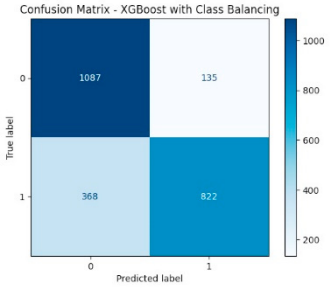

Fig. 6 Behavioral biometrics authentication confusion Metrix

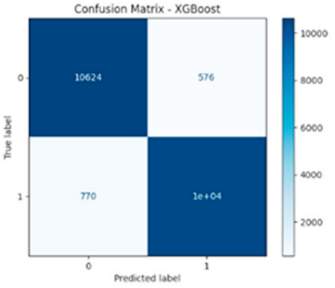

Fig. 7 DOS Attack Matrix

The study highlights the effectiveness of a behavioral biometric system for user authentication, achieving 92% accuracy and maintaining performance despite user behavior variations. It outperforms traditional methods in security and convenience, making it ideal for cloud-based IoT systems. XGBoost proved effective for real-time detection of TCP SYN flood attacks in IoT environments but requires optimization to address computational demands on low-resource devices. Machine learning models like Decision Tree and KNN also excelled in botnet detection, underscoring the potential of AI in securing IoT networks. However, limitations include the dataset's representativeness, reliance on artificial data, and controlled testing environments. Future work should focus on diverse datasets, novel models, and resource-efficient solutions to enhance real-world applicability.

5. Conclusion

The Cloudflare DDoS Threat Report for Q4 2023 reveals a sharp increase in Distributed Denial of Service (DDoS) attacks, especially targeting telecommunications, gaming, and financial services, with the United States, Germany, and Singapore being the most affected countries. The report highlights the growing sophistication of these attacks, including multi-vector and high-volume assaults exceeding 100 Gbps, which disrupt network infrastructure and service availability [34].

The research on resilient IoT infrastructures addresses these issues by using machine learning-based intrusion detection to identify complex attack patterns, such as DDoS, TCP SYN flood, and botnet activity. This approach supports digital sovereignty (DS) by enabling nations and organizations to protect their critical infrastructure autonomously, reducing reliance on foreign cybersecurity providers. By incorporating local authentication through behavioral biometrics and using local storage solutions, our framework minimizes external dependencies and enhances DS by keeping sensitive data under local control [34].

This study aimed to improve IoT security by investigating anomaly detection, botnet attack detection, user authentication, and TCP SYN flood attack detection. The research indicated that machine learning models such as Decision Tree, Naive Bayes, K-Nearest Neighbors (KNN), and XGBoost can improve the security and reliability of IoT systems. Notable results show that Decision Tree and Naive Bayes models are effective in identifying anomalies in IoT networks, but more studies are required to incorporate live monitoring and enhance the robustness of IoT systems. Decision Tree and KNN models performed better than simpler models in detecting botnet attacks [1], [2], but further efforts are needed to ensure their generalization across various IoT devices and attack types [3], [4]. The potential of a user authentication system using behavioral biometrics was demonstrated, but further enhancements are required to adjust to evolving user behavior and enhance accuracy. The research also emphasized the capability of XGBoost in accurately identifying TCP SYN flood attacks [30], [31], which adds to the overall goal of protecting IoT networks from advanced cyber threats. In general, the study highlights the importance of continuous improvement and development of machine learning methods to adapt to the changing nature of cyber threats and enhance the security of IoT devices in the digital environment.

Disclaimer

During the preparation of this work, the author utilized AI-assisted tools such as (please specify tools used, e.g., ChatGPT, Perplexity, Grammarly, or others) to enhance English language accuracy, including spelling, grammar, and punctuation. The content generated or corrected by these tools was thoroughly reviewed, revised, and edited by the author to ensure accuracy and originality. The author accepts full responsibility for the originality of the final content of this publication

References

[1] S. Pokhrel, R. Abbas, and B. Aryal, “IoT Security: Botnet Detection in IoT Using Machine Learning,” in Proceedings of the International Conference on Information Technology, 2019, pp. 1-6.

[2] M. Aamir and S. M. A. Zaidi, “Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning,” IEEE Access, vol. 7, pp. 127276-127285, 2019.

[3] H. Bahsi, S. Nomm, and F. B. La Torre, “Detection of IoT Botnet using Machine Learning and Deep Learning,” Journal of Communications and Information Networks, vol. 4, no. 3, pp. 1-7, 2019.

[4] 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, Article ID 4515642, pp. 1-14, Oct. 2022.

[5] Sattari, F. et al. “A Hybrid Deep Learning Approach for Bottleneck Detection in IoT,” IEEE Access, vol. 10, pp. 77039–77053, 2022. doi:10.1109/access.2022.3188635.

[6] Hussain, F. et al. “A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks,” IEEE Access, vol. 9, pp. 163412–163430, 2021. doi:10.1109/access.2021.3131014.

[7] Alharbi, A., and Alsubhi, K. “Botnet Detection Approach Using GraphBased Machine Learning,” IEEE Access, vol. 9, pp. 99166–99180,2021. doi:10.1109/access.2021.3094183.

[8] Stephens, B. et al. “Detecting Internet of Things Bots: A Comparative Study,” IEEE Access, vol. 9, pp. 160391–160401, 2021. doi:10.1109/access.2021.3130714.

[9] Panda, M., Mousa, A.A. and Hassanien, A.E. “Developing an Efficient Feature Engineering and Machine Learning Model forDetectingIoTBotnet Cyber Attacks,” IEEE Access, vol. 9, pp. 91038–91052, 2021. doi:10.1109/access.2021.3092054.

[10] Almuqren, L. et al. “Hybrid Metaheuristics With Machine Learning Based Botnet Detection in Cloud Assisted Internet of Things Environment,” IEEE Access, vol. 11, pp. 115668–115676, 2023. doi:10.1109/access.2023.3322369.

[11] Ali, M. et al. “Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment,” IEEE Access, vol. 12, pp. 40682– 40699, 2024. doi:10.1109/access.2024.3376400.

[[12] S.A. Ali et al., "Leveraging machine learning for real-time anomaly detection and self-repair in IoT devices," in *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, 202[Online].Available:doi:10.1109/iccsai59793.2023.10421539.

[13] R.S. Gaines, W. Lisowski, S.J. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," RAND Corporation, Santa Monica, CA, USA, 1980.

[14] A.A.E. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," *IEEE Trans. Dependable Secur. Comput.*, vol. 4, pp. 165–179, 2007.

[15] A.A.E. Ahmed and I. Traore, "Anomaly Intrusion Detection Based on Biometrics," in *Proc. Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, West Point, NY, USA, 15–17 June 2005, pp. 452–453.

[16] N. Gunathilake, A. Padikaraarachchi, S. Koralagoda, M. Jayasundara, P. Paliyawadana, C. Manawadu, and U. Rajapaksha, "Enhancing the Security of Online Banking Systems via Keystroke Dynamics," in *Proc. The 8th International Conference on Computer Science & Education (ICCSE 2013)*, 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6553973

[17] R.S. Gaines, W. Lisowski, S.J. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," RAND Corporation, Santa Monica, CA, USA, 1980.

[18] A.A.E. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," *IEEE Trans. Dependable Secur. Comput.*, vol. 4, pp. 165–179, 2007.

[19] A.A.E. Ahmed and I. Traore, "Anomaly Intrusion Detection Based on Biometrics," in *Proc. Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, West Point, NY, USA, 15–17 June 2005, pp. 452–453.

[20] Myridakis, D., Myridakis, P. and Kakarountas, A. (2020) 'Intrusion detection and botnet prevention circuit for IOT devices', 2020 5th SouthEast Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) [Preprint]. doi:10.1109/seeda-cecnsm49515.2020.9221789

[21] F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[22] B. I. Hairab, M. Said Elsayed, A. D. Jurcut and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," in IEEE Access, vol. 10, pp. 98427-98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[23] I. Cvitić, D. Perakovic, B. B. Gupta and K. -K. R. Choo, "BoostingBased DDoS Detection in Internet of Things Systems," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2109-2123, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3090909.

[24] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai and V. Grout, "Detection and Classification of DDoS Flooding Attacks on Software-Defined

[25] Networks: A Case Study for the Application of Machine Learning," in

[26] IEEE Access, vol. 9, pp. 122495-122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[27] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," in

[28] W. I. Khedr, A. E. Gouda and E. R. Mohamed, "FMDADM: A MultiLayer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," in IEEE Access, vol. 11, pp. 28934-28954, 2023, doi: 10.1109/ACCESS.2023.3260256.

[29] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends," Sensors, vol. 24, no. 6, p. 1968, 2024.

[30] I. U. Khan, M. Y. Ayub, A. Abdollahi, and A. Dutta, "A hybrid deep learning model-based intrusion detection system for emergency planning using IoT-network," in 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Cosenza, Italy, 2023, pp. 1-5, doi: 10.1109/ICT-DM58371.2023.10286954.

[31] M. Z. M. Arafat, S. A. Hussain, M. T. Islam, and A. M. A. Latif, "A machine learning-based intrusion detection for detecting internet of things network attacks," Journal of Electrical Systems and Information Technology, vol. 9, no. 1, p. 8, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110016822001570.

[32] A. Alqadhib, T. AlZubi, and O. A. Khalaf, "A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the Internet of Things," International Journal of Information Security,2023.[Online].Available: https://link.springer.com/article/10.1007/s10207-023-00803-x.

[33] S. N. Amrawee, M. Z. A. Bhuiyan, and M. H. Jo, "Metaheuristic Firefly and C5.0 algorithms based intrusion detection for critical infrastructures,"in2024IEEETransactionsonIndustrialInformatics, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10193917.

[34] Cloudflare, "DDoS threat report 2023 Q4," Cloudflare Blog, Nov. 2023. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q4/.

[35] Labbe, M., Khalil, I., Hafeez, A., & Jamal, M. A. J. "IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic." Canadian Institute for Cybersecurity, University of New Brunswick, 2020. [Online]. Available: https://www.unb.ca/cic/datasets/iot-23.html

[36] Moustafa, N., & Slay, J. "UNSW-NB15: A Comprehensive Dataset for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)." Centre for Cyber Security Research, Australian Centre for Cyber Security (ACCS), University of New South Wales, 2015. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/

[37] https://www.elsevier.com/about/policies-and-standards/generative-ai-policies-for-journals#3-for-editors