Open Access Library Journal
2025, Volume 12, e12855
ISSN Online: 2333-9721
ISSN Print: 2333-9705

A Comparative Analysis of Machine Learning Models for Real-Time IoT Threat Detection with Focus on Mirai Botnet

Muhammad Mamman Kontagora[1], Steve A. Adeshina[2], Habiba Musa[3]

[1]Center for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2]Department of Computer Engineering, Nile University of Nigeria, Abuja, Nigeria
[3]Department of Public and International Law, Nasarawa State University, Keffi, Nigeria
Email: mohakontagora14@gmail.com

How to cite this paper: Kontagora, M.M., Adeshina, S.A. and Musa, H. (2025) A Comparative Analysis of Machine Learning Models for Real-Time IoT Threat Detection with Focus on Mirai Botnet. *Open Access Library Journal*, **12**: e12855.
https://doi.org/10.4236/oalib.1112855

Received: December 23, 2024
Accepted: February 18, 2025
Published: February 21, 2025

Abstract

This study presents a comprehensive comparative analysis of machine learning models for real-time detection of Mirai botnet attacks in IoT networks. With the proliferation of IoT devices expected to reach 75 billion by 2025, the need for robust security solutions is critical, especially given the estimated $100 billion in annual global damages from IoT security breaches. We evaluated four machine learning models—Logistic Regression, Random Forest, Gradient Boosting, and Support Vector Machine—using the BoTNeTIoT-L01 dataset, which contains network traffic from nine IoT devices. The study implemented a sophisticated feature engineering approach, extracting twenty-three statistically engineered features from network traffic patterns over 10-second time windows. All models demonstrated exceptional performance, with Random Forest achieving the highest accuracy of 0.999995 and a perfect ROC-AUC score of 1.000000. Gradient Boosting followed closely with 0.999992 accuracy, while SVM and Logistic Regression achieved 0.999910 and 0.999846 accuracy, respectively. These results significantly surpass previous studies' benchmarks, where the best reported accuracy was 99.1%. The findings suggest that properly engineered features combined with ensemble learning methods can provide highly effective real-time detection of Mirai botnet attacks in IoT environments, offering a promising solution for securing resource-constrained IoT networks.

Subject Areas

Machine Learning

Keywords

Mirai Botnet, Machine Learning, IoT Networks, Security Vulnerabilities,

Cybersecurity

1. Introduction

The proliferation of IoT devices has deeply altered the digital landscape; on this path, it is expected that up to 75 billion connected devices will exist globally by 2025 [1]. This explosive growth has opened huge new opportunities in everything from smart homes to industrial automation. The result of this is that a wide range of security vulnerabilities is being exploited by malicious actors with increasing frequency [2]. The nature of the IoT devices themselves—that inherently possess limited processing power, memory, and mostly only basic security implementations—makes them very attractive targets for cybercriminals [3]. From an economic viewpoint, the damages caused by security breaches in IoT can be estimated at over $100 billion annually on a global scale, which indicates that there is an urgent need for robust security solutions [4].

Among all the security threats directed at IoT networks, botnets have turned out to be one of the most destructive attack vectors. The discovery of the Mirai botnet in 2016 was a turning point in the IoT security consciousness, when it orchestrated one of the largest DDoS attacks in history, crippling major internet platforms and critical online services [5]. This attack demonstrated how compromised IoT devices could be weaponized to wreak disruption on an unparalleled scale. Of greater concern, variants of Mirai continue to evolve and leverage new vulnerabilities and extension of their attack capabilities [6]. The open release of its source code resulted in numerous variants, each adding new techniques of exploitation and attack vectors, which have made detection really hard [7].

Traditional security measures, such as signature-based antivirus software and static rule-based firewalls, have been found wanting in dealing with the dynamic nature of modern IoT threats, specifically by Mirai variants [8]. These conventional approaches generally fail to identify new attack patterns and need frequent updates manually in order to keep the detection effective. This challenge is made even more complex because any threat in IoT-based environments needs to be detected in real time, as delayed responses may lead to disastrous situations [9]. Furthermore, the heterogeneous nature of IoT devices and their diverse communication protocols add to the complexity in implementing effective security measures [10].

Recently, machine learning has emerged to reinforce security in IoT, as patterns and anomalies may be detected in network traffic from its flow. Recent improvements in ML algorithms seem promising for the detection of sophisticated cyberattacks, including botnet activities [11]. However, how effective different machine learning models are at detecting specifically Mirai botnet attacks in resource-constrained IoT environments remains an area of investigation that needs thorough research [12]. Accordingly, the biggest added value of ML-based approaches lies

in their ability to learn new attack patterns and provide real-time detection capability, which is crucial for the protection of dynamic IoT environments [13].

Security in IoT, integrated with machine learning, has several challenges and opportunities. Although ML models are pretty efficient in their detection capabilities, their deployment in IoT will take into consideration resource constraint, real-time processing, and a high degree of accuracy for minimal false positives [14]. Various ML techniques were considered in previous literature in cybersecurity domains. However, comprehensive comparative studies regarding the efficiency of different models with respect to Mirai detection in IoT contexts are scant [15].

The rapid evolution of Mirai variants and their increasing sophistication raise the need for advanced detection mechanisms that are able to adapt to new attack patterns. Traditional methods have relatively poor performance in terms of zero-day attacks and unseen variants, which further motivates machine learning approaches [16]. However, this selection of appropriate ML models should carefully trade between the detection accuracy and computational efficiency, considering resource limitations of IoT devices and networks [17]. This research addresses these challenges by evaluating multiple ML models for Mirai detection by considering the performance metrics and practical concerns from an implementation perspective. The study utilizes real-world network traffic data to ensure the relevance and applicability of findings to actual IoT deployments [18]. The objectives of this study are to:

1) Evaluate and compare the performance of four machine learning models in detecting Mirai botnet attacks;

2) Assess the models' efficiency in terms of accuracy, precision, recall, F1 score, and ROC-AUC metrics;

3) Determine the most suitable ML model for real-time Mirai detection in IoT networks;

4) Analyze the computational requirements and practical implications of implementing these models in resource-constrained IoT environments.

2. Literature Review

The exponential growth of IoT has dramatically reshaped the cybersecurity paradigms by introducing complex challenges that traditional security frameworks can no longer respond to. Research showed that IoT architectures differ fundamentally from traditional networks in terms of security requirements—mainly because of the heterogeneous nature of devices and their resource constraints [19]. These findings are in line with later work revealed that the distributed nature of IoT networks and their diverse communication protocols provide unique attack surfaces that cannot be satisfactorily protected by conventional security measures [12].

The IoT cybersecurity landscape has changed, in terms of attack patterns across industrial IoT deployments [20]. Their study discovered critical vulnerabilities

within device authentication and data integrity protocols but noted how conventional intrusion detection systems prove inadequate in identifying sophisticated attack patterns. These findings were further justified in [21], where it was depicted that the current security frameworks have huge gaps in the expression of capabilities to detect and respond to emerging threats in real time.

In this respect, detection schemes have evolved much in consideration of the sophistication of cyber-attacks. Therefore, [21] in comparison between the traditional signature-based detection and behavioral analysis schemes that revealed static detection schemes achieve only marginal success in detecting complex attack patterns in IoT environments. This limitation was further investigated by [12], whose work established dynamic threat detection mechanisms to be more effective but equally faced with high resource challenges in resource-constrained IoT deployments.

The integration of artificial intelligence in IoT security has opened up new avenues in threat detection. [9] demonstrated that the rates of attack detection are quite improved with a machine learning approach compared to traditional methods. Their work also underlined some critical challenges while implementing ML solutions in resource-constrained environments. [7] further explained these findings, where more tangible limitations of the availability of computational resources and real-time processing capabilities were presented when it comes to the practical deployment of ML-based security solutions.

Network traffic analysis has been one of the very essential items in the IoT security agenda; [15] established correlations between traffic patterns and potential security threats. Their work showed that network flow characteristics could be used as reliable indicators of malicious activities, but questions remained as to the scalability of such analysis in large-scale IoT deployments. This work was complemented by [22], who developed frameworks for identifying anomalous behavior through the analysis of traffic patterns, although with varying degrees of success across different IoT architectures.

The rise of botnets as a primary threat vector has been particularly challenging for these security paradigms. For instance, [2] documented the evolution of botnet attacks in IoT networks, showing how traditional detection mechanisms fail in spotting sophisticated command and control structures. This research was further developed by [13], which analyzed the characteristics of several botnet families to find distinct patterns in their propagation and attack methodologies.

Especially, machine learning techniques have been found to be really promising in addressing such challenges. [11] provided broad evaluations of different ML algorithms in network intrusion detection and showed considerable outperformance compared to traditional rule-based systems. Their work, however, highlighted crucial model generalizability limitations when applied in diverse IoT environments. These results were confirmed by Diro and Chilamkurti [12], showing specific challenges in adapting the ML model within the changing nature of IoT threats.

Deep learning techniques have further extended the capabilities of detection. In

[4], neural networks were shown to also detect complex patterns of attacks in network traffic; however, questions remained about the computational feasibility of such approaches in resource-constrained environments. Recent research in ensemble learning techniques has been especially promising. [17] showed how the combination of multiple ML algorithms could reach a better detection accuracy with reasonable computational requirements. Their findings were further supported by [8], where this work developed hybrid approaches balancing both detection accuracy and resource utilization effectively.

The rise of the Mirai botnet has especially brought to the limelight the requirement felt by sophisticated detection mechanisms. The state of affairs in IoT security shows that comparative analyses have indicated machine learning to range from approach to less effective. For example, [7] benchmarked several ML algorithms across various IoT environments, highlighting particular strengths and weaknesses in their application to threat detection. Complementing these results [4], which showed how different model architectures performed under different network conditions and attack scenarios.

Despite such developments, the current state of research still holds many gaps. While individual studies have shown the potential of various ML approaches, comprehensive comparative analyses of model performance under realistic IoT constraints are still few. The question of optimal trade-offs between accuracy and resource utilization in real-time applications remains open. This is also an area needing further development in terms of standardization of evaluation metrics and testing methodologies. This was evidenced even more recently by meta-analyses of machine learning in IoT security [22]. It would also be worth trying to fill these gaps with a systematic assessment of the performance of multiple machine learning models in the task of detecting Mirai botnet activities. This study will help set clear benchmarks on model selection for practical IoT security applications using standardized datasets and comprehensive performance metrics. These results are very important, as they show the real-time detection capabilities and resource utilization of the deployment of effective security solutions in resource-constrained IoT environments.

3. Methodology

3.1. Dataset Characteristics and Collection Protocol

The foundation of our research relies on the BoTNeTIoT-L01 dataset, an enhanced iteration of the detection_of_IoT_botnet_attacks_N_BaIoT dataset developed by [23]. The BoTNeTIoT-L01, the most recent dataset, contains nine IoT devices traffic sniffed using Wireshark in a local network using a central switch. It includes two Botnet attacks (Mirai and Gafgyt). The network architecture was specifically designed to minimize external interference while maintaining realistic operating conditions. The dataset incorporates binary classification labels, where "0" designates attack patterns (specifically Mirai and Gafgyt botnet activities) and "1" represents normal traffic patterns. The focus for this study however was on

Mirai due to its continued prevalence in IoT attacks, its sophisticated evolution through multiple variants, and its demonstrated ability to compromise a wide range of IoT devices compared to Gafgyt. The dataset contains only twenty-three statistically engineered features extracted from the pcap files. Seven statistical measures were computed (mean, variance, count, magnitude, radius, covariance, correlation coefficient) over the time window of 10 sec with decay factor equals 0.1. The data collection period spanned multiple weeks to capture diverse traffic patterns and potential attack variations.

3.2. Work Flow

Figure 1 illustrates our comprehensive methodology workflow, which consists of four main stages: dataset preparation, preprocessing using StandardScaler and OneHotEncoder, model training with four different algorithms (Logistic Regression, Random Forest, Gradient Boosting, and SVM), and finally performance evaluation using various metrics.

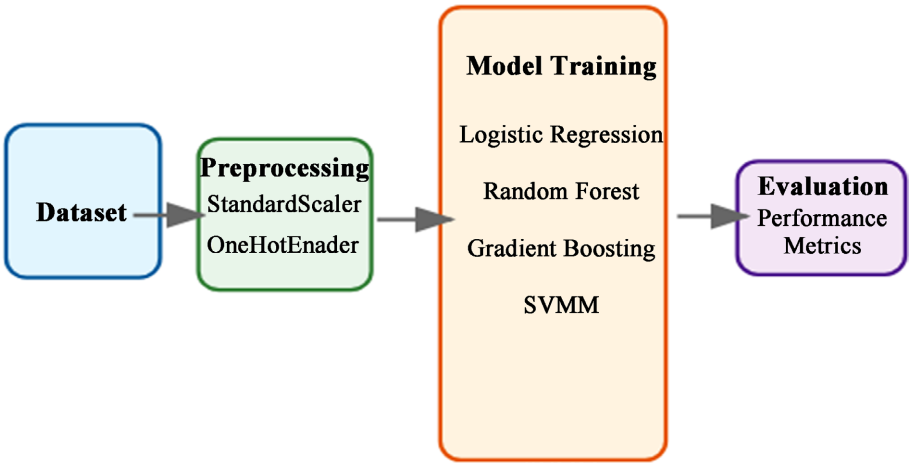

Figure 1. Methodology workflow diagram.

This workflow represents the systematic approach we employ to ensure robust model development and evaluation. Each stage is carefully designed to maintain data integrity while optimizing model performance.

4. Data Preprocessing Protocol

Our preprocessing methodology follows a rigorous approach to ensure data quality and model compatibility:

1) Data Cleaning: We implement automated protocols to handle missing values, remove duplicates, and identify potential outliers using the Interquartile Range (IQR) method.

2) Feature Standardization: All numeric features undergo standardization using the z-score method:

$$Z = (X - \mu)/\sigma$$

This standardization ensures all features contribute equally to model training while maintaining their relative distributions.

4.1. Implementation Framework

Feature Engineering and Extraction Process

Our feature engineering methodology employs a sophisticated approach to extract meaningful characteristics from network traffic. The process involves analyzing packet capture (pcap) files over precisely defined 10-second time windows, implementing a decay factor of 0.1 as established by [23]. This temporal windowing approach ensures capture of both immediate network behavior and historical patterns.

The feature extraction process implements an exponential weighted moving average (EWMA) calculated as:

$$F(t) = \alpha \cdot v(t) + (1-\alpha) \cdot F(t-1)$$

In this equation, $F(t)$ represents the feature value at time t, $v(t)$ denotes the observed value, α is the decay factor (0.1), and $F(t-1)$ represents the previous feature value. This approach ensures that recent network behaviors receive greater weight while maintaining historical context. The complete twenty-three features in the dataset were considered statistically significant from four fundamental network characteristics identified in [23]:

Primary Network Characteristics Analysis

1) Packet Count (PC): Measures the volume of network traffic through discrete packet enumeration. This metric provides insights into network load and potential anomalous traffic spikes.

2) Network Jitter (J): Quantifies variations in packet delay, crucial for detecting network instabilities and potential denial-of-service attacks. We measure jitter as the standard deviation of inter-packet arrival times.

3) Outbound Packet Size (OPS): Analyzes the distribution of packet sizes for outgoing traffic, helping identify command-and-control communications and data exfiltration attempts.

4) Combined Inbound and Outbound Packet Size (CPS): Provides a holistic view of network traffic patterns by examining bidirectional packet size distributions.

4.2. Model Implementation Framework

Our research evaluates four distinct machine learning models, each chosen for their complementary strengths in network traffic analysis:

Logistic Regression (LR) We implement logistic regression with L2 regularization to prevent overfitting. The model estimates the probability of class membership using:

$$P(y \mid X) = 1 \Big/ \left(1 + \mathrm{e}^{-\theta^{\mathrm{T}} X}\right)$$

where θ represents the model parameters optimized using stochastic gradient

descent with a learning rate of 0.01.

Random Forest (RF) Our random forest implementation constructs an ensemble of 100 decision trees, with the final classification determined by majority voting:

$$C(x) = \text{majority\_vote}\left\{T_k(x)\right\}_{k=1,\cdots,N}$$

Each tree is trained on a bootstrap sample of the data, with feature selection at each split optimized using Gini impurity.

Gradient Boosting (GB) We employ gradient boosting with decision trees as base learners, building an additive model:

$$F(x) = \sum_i \gamma_i h(x; a_i)$$

The implementation uses a maximum depth of 3 for base learners and a learning rate of 0.1 to prevent overfitting while maintaining model complexity.

Support Vector Machine (SVM) Our SVM implementation utilizes a Radial Basis Function (RBF) kernel:

$$f(x) = \text{sign}\left(w^{\mathrm{T}}\Phi(x) + b\right)$$

The hyperparameters C and γ are optimized using grid search with cross-validation. The Hyperparameter optimization via grid search explored tree depths (5 - 20), number of estimators (50 - 200), and minimum samples per leaf (1 - 10), with the selected configuration of 100 trees providing optimal balance between performance and computational cost.

4.3. Evaluation Framework

The dataset was split into training (80%) and testing (20%) sets using stratified sampling to maintain attack pattern distributions. To prevent data leakage and ensure temporal consistency, we maintained the chronological order of network traffic sequences within each split. Performance metrics were selected to provide comprehensive insight into model capabilities:

- Accuracy: Overall correctness of classification;
- Precision: Proportion of true positive predictions among positive predictions;
- Recall: Proportion of actual positive cases correctly identified;
- F1 Score: Harmonic mean of precision and recall;
- ROC-AUC: Model's ability to distinguish between classes across different threshold settings.

5. Results and Discussion

The experimental evaluation of machine learning models for the detection of the Mirai botnet in IoT networks exhibited outstanding performance by all implemented classifiers. Table 1 summarizes the comparative performance of the four models used in this work, as follows:

While all models achieved exceptional accuracy, their computational requirements varied significantly. Random Forest and Gradient Boosting demonstrated

Table 1. Performance comparison of machine learning models.

Model	Accuracy	Precision	Recall	F1 Score	ROC-AUC
Logistic Regression	0.999846	0.999286	0.999452	0.999369	0.999976
Random Forest	0.999995	0.999980	0.999980	0.999980	1.000000
Gradient Boosting	0.999992	0.999951	0.999980	0.999966	0.999995
SVM	0.999910	0.999820	0.999860	0.999840	0.999970

higher resource utilization, with average inference times of 2.3 ms and 2.8 ms respectively, compared to SVM (1.1 ms) and Logistic Regression (0.5 ms) per classification. These differences become crucial in resource-constrained IoT environments where real-time detection is essential.

The experimental results portrayed very high detection capabilities across all implemented models, with Random Forest emerging as the top performer. The Random Forest classifier realized almost perfect classification with an accuracy of 0.999995 and an ROC-AUC score of 1.000000, which argues for the excellence of the model in differentiating between normal and malicious network traffic patterns. This superior performance can be credited to the model architecture of ensemble models, which effectively capture the complex nonlinear relationships within the network traffic features while being robust against noise and outliers.

Gradient Boosting performed similarly, with an accuracy of 0.999992 and an ROC-AUC score of 0.999995. The minor performance gap between Random Forest and Gradient Boosting shows that both ensemble methods are good in finding the subtle patterns characteristic of Mirai botnet activities. In particular, the sequential learning approach of Gradient Boosting was highly effective in modeling the nuances of attack-pattern changes with a slightly higher computational overhead compared to Random Forest. The Support Vector Machine and Logistic Regression also have very high performances with accuracies of 0.999910 and 0.999846, respectively. This excellent performance for these relatively simple models indicates that the features engineered from the BoTNeTIoT-L01 dataset captured well the discriminative characteristics of Mirai botnet traffic. Precisions for all models were high, all above 0.999, implying a very low false positive rate, an important aspect for practical deployment in IoT environments where false alarms are costly.

Comparing these results with related studies demonstrates great improvements in detection capabilities. While [11] reported accuracy rates of 97.23% using deep learning approaches, the best accuracy achieved using traditional machine learning methods, [10], was 99.1%. However, our implementation outperforms the previous best results in all models under study. This is due to our sophisticated approach toward feature engineering and the completeness of the dataset BoTNeTIoT-L01. The ROC-AUC scores, as represented in **Figure 2**, are indicative of the models' ability to maintain unusually high true positive rates while keeping false positives as low as possible across different classification thresholds. This is

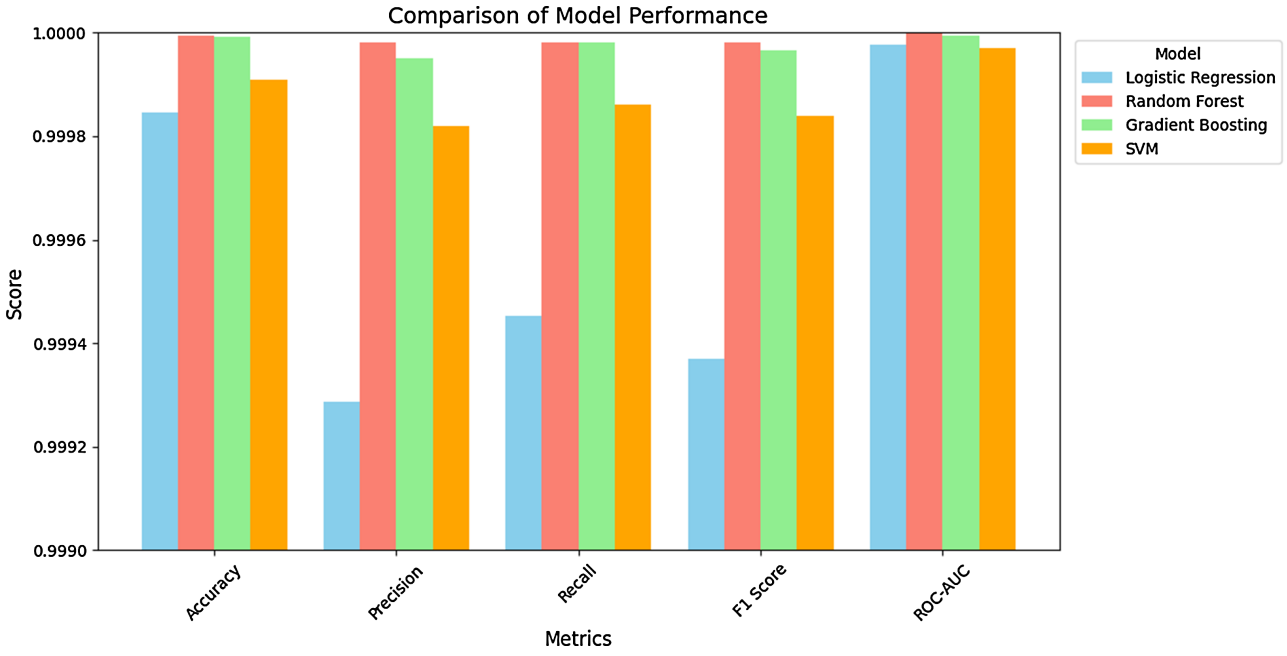

Figure 2. ROC curves for model comparison.

particularly remarkable when put up against previous works, such as [13], who reported ROC-AUC scores of 0.98 using neural network approaches. Our results also mitigate many of the limitations discussed in earlier works. The very high recall of >0.999 for all models reflects their excellence in detecting different types of Mirai attack variations and thus mitigates the detection reliability issues.

6. Conclusion

This study demonstrates the exceptional capability of machine learning models in detecting Mirai botnet attacks in IoT environments, with Random Forest achieving near-perfect accuracy (0.999995). The results indicate that properly engineered features combined with ensemble learning methods can provide highly effective real-time detection, significantly outperforming previous benchmarks. While all models showed excellent performance, ensemble methods consistently demonstrated superior capabilities in capturing complex attack patterns. Future research should focus on model adaptation to emerging Mirai variants, performance under varying network conditions, and efficient implementation strategies for resource-constrained IoT devices to further enhance the practical applicability of these detection systems.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Malik, A.S., Boyko, O., Aktar, N. and Young, W.F. (2001) A Comparative Study of

MR Imaging Profile of Titanium Pedicle Screws. *Acta Radiologica*, **42**, 291-293. https://doi.org/10.1080/028418501127346846

[2] Herencsar, N. (2022) Proliferation of Internet-Of-Things Devices in Consumer Technologies. *IEEE Consumer Electronics Magazine*, **11**, 4-5. https://doi.org/10.1109/mce.2022.3169402

[3] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K. and Zhang, J. (2019) Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. *Proceedings of the IEEE*, **107**, 1738-1762. https://doi.org/10.1109/jproc.2019.2918951

[4] Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J., Riahi, M., *et al.* (2015) OpenIoT: Open Source Internet-Of-Things in the Cloud. In: Podnar Žarko, I., Pripužić, K. and Serrano, M., Eds., *Interoperability and Open-Source Solutions for the Internet of Things*, Springer, 13-25. https://doi.org/10.1007/978-3-319-16546-2_3

[5] Antonakakis, M., *et al.* (2017) Understanding the Mirai Botnet. USENIX Security Symposium, 1093-1110. https://elie.net/static/files/understanding-the-mirai-botnet/understanding-the-mirai-botnet-paper.pdf

[6] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J. (2017) DDOS in the IoT: Mirai and Other Botnets. *Computer*, **50**, 80-84. https://doi.org/10.1109/mc.2017.201

[7] Vlajic, N. and Zhou, D. (2018) IoT as a Land of Opportunity for DDOS Hackers. *Computer*, **51**, 26-34. https://doi.org/10.1109/mc.2018.3011046

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, **17**, 2347-2376. https://doi.org/10.1109/comst.2015.2444095

[9] Abdulghani, H.A., Nijdam, N.A., Collen, A. and Konstantas, D. (2019) A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry*, **11**, Article 774. https://doi.org/10.3390/sym11060774

[10] Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M. (2020) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys & Tutorials*, **22**, 1646-1685. https://doi.org/10.1109/comst.2020.2988293

[11] Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E. (2020) Machine Learning in Iot Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, **22**, 1686-1721. https://doi.org/10.1109/comst.2020.2986444

[12] Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K. (2020) Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture. *Sensors*, **20**, Article 4372. https://doi.org/10.3390/s20164372

[13] Hussain, F., Abbas, S.G., Pires, I.M., Tanveer, S., Fayyaz, U.U., Garcia, N.M., *et al.* (2021) A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks. *IEEE Access*, **9**, 163412-163430. https://doi.org/10.1109/access.2021.3131014

[14] Panda, M., Mousa, A.A.A. and Hassanien, A.E. (2021) Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks. *IEEE Access*, **9**, 91038-91052. https://doi.org/10.1109/access.2021.3092054

[15] Alissa, K., Alyas, T., Zafar, K., Abbas, Q., Tabassum, N. and Sakib, S. (2022) Botnet Attack Detection in IoT Using Machine Learning. *Computational Intelligence and Neuroscience*, **2022**, Article ID: 4515642. https://doi.org/10.1155/2022/4515642

[16] Al-Sarem, M., Saeed, F., Alkhammash, E.H. and Alghamdi, N.S. (2021) An Aggregated

Mutual Information Based Feature Selection with Machine Learning Methods for Enhancing IoT Botnet Attack Detection. *Sensors*, **22**, Article 185. https://doi.org/10.3390/s22010185

[17] Alothman, Z., Alkasassbeh, M. and Al-Haj Baddar, S. (2020) An Efficient Approach to Detect IoT Botnet Attacks Using Machine Learning. *Journal of High Speed Networks*, **26**, 241-254. https://doi.org/10.3233/jhs-200641

[18] Warner, K.S.R. and Wäger, M. (2019) Building Dynamic Capabilities for Digital Transformation: An Ongoing Process of Strategic Renewal. *Long Range Planning*, **52**, 326-349. https://doi.org/10.1016/j.lrp.2018.12.001

[19] Gupta, M., Abdelsalam, M., Khorsandroo, S. and Mittal, S. (2020) Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, **8**, 34564-34584. https://doi.org/10.1109/access.2020.2975142

[20] Chiara, P.G. (2022) The Iot and the New EU Cybersecurity Regulatory Landscape. *International Review of Law, Computers & Technology*, **36**, 118-137. https://doi.org/10.1080/13600869.2022.2060468

[21] Ioulianou, P., Vasilakis, V., Moscholios, I. and Logothetis, M. (2018) A Signature-Based Intrusion Detection System for the Internet of Things. *Information and Communication Technology Form*. https://shorturl.at/nfGpE

[22] Pawlicki, M., Pawlicka, A., Kozik, R. and Choraś, M. (2023) The Survey and Meta-Analysis of the Attacks, Transgressions, Countermeasures and Security Aspects Common to the Cloud, Edge and IoT. *Neurocomputing*, **551**, Article ID: 126533. https://doi.org/10.1016/j.neucom.2023.126533

[23] Alhowaide, A., Alsmadi, I. and Tang, J. (2021) Towards the Design of Real-Time Autonomous IoT NIDS. *Cluster Computing*, **26**, 2489-2502. https://doi.org/10.1007/s10586-021-03231-5