A Review of an Artificial Intelligence-Driven Autonomous System for Botnet Detection and Mitigation in Internet of Things Network

Cheah Wei Yan1, a) and Nur Erlida Ruslan1, 2, b)

1*Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Malaysia.*

2*Centre of Image and Vision Computing, CoE of Artificial Intelligence,* *Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Malaysia*

*b) Corresponding author: nurerlida@mmu.edu.my*

*a) 1201203703@student.mmu.edu.my*

**Abstract.** The rapid expansion of Internet of Things (IoT) networks has significantly enhanced connectivity across various sectors. Nevertheless, such expansion has also created serious security loopholes that have exposed the IoT devices to botnet attacks. The attacks take advantage of the vulnerability of the devices and perform malicious actions that include Distributed Denial-of-Service (DDoS) attacks, data breaches, and unauthorized control of the systems. To combat such rising threats, this review paper discusses the current methodologies and suggests an independent, real-time botnet detection and mitigation framework based on the advanced machine learning algorithms, such as Random Forest (RF) and Neural Networks (NN). The key aim of the study is to examine and assess existing methods of botnet detection, define their limitations, and propose a more efficient one that would improve the detection accuracy and resolve the main issues of dataset imbalance, the constant growth of IoT networks, and the need to provide scalable security responses. The suggested solution combines the real-time anomaly detection and proactive mitigation strategies to enhance IoT security, shorten response times, and limit the impact on the network. The review can fill the gap between theoretical development and practical application by providing a detailed review of the latest botnet defence systems and proposing a flexible, adaptive model of protecting IoT ecosystems against the latest cyber threats. The work is an essential reference model to improving cybersecurity precautions against the fast-developing threats, which guarantee undetermined and smart IoT network security.

# INTRODUCTION

While the rise of IoT has helped smart homes and healthcare, it has also made IoT networks more at risk of cyberattacks, mainly those that rely on botnets. Devices that have been compromised by malicious actors can cause DDoS attacks, take important data, and destroy important systems. Using only signature detection is usually not enough to stop the changing threats in IoT devices. As a result, AI and ML now play a key role in spotting and handling botnets by analysing vast amounts of data and finding patterns linked to attacks. CNNs and other deep learning methods are capable of learning to detect anomalies in IoT networks by themselves, as shown by Moorthya et al., [1].In addition, researchers Wazzan et al., [2] ,have found that when systems use both supervised and unsupervised approaches, they are better able to respond to new IoT attacks. The use of feature engineering and artificial data generation is also growing, with Pokhrel et al., [3], addressing data imbalance by applying KNN and MLP models. There are still difficulties in building detection systems for IoT devices that are both small and work well across many devices. Being able to catch new botnet threats quickly and adapt to them will be important in future research, with deep learning and mixed approaches expected to help a lot in securing IoT [4].

## IoT Networks and Botnet Security Challenges

IoT makes it possible for household appliances, vehicles, wearable gadgets, and industrial machines to communicate and run over the Internet, encouraging progress in healthcare, manufacturing, agriculture, and planning cities [4]. For instance, homes with smart technology can adjust lights, maintain the right temperature, and secure the house, while industries use IoT to make predictions that avoid losing time due to breakdowns. Nevertheless, with more use of IoT, challenges with security are rising. Since IoT devices are not very powerful, they struggle to use strong security tools, and the large variety and complexity of these networks make it tough to protect them all the same [5]. As a result, there are significant risks, since personal health data, financial details, and messages may be sent through IoT devices. Weakly secured endpoints are becoming a common target for cybercriminals, who use them to move laterally, take data, and control the system. Botnets, which consist of taken-over IoT devices that are remotely controlled, are among the biggest threats. Most of the time, these devices do not get security updates, still use default passwords, and are simple for attackers to use to install malware. In 2016, when the Mirai botnet DDoS was launched, it showed how significant disruptions can happen because of such weaknesses [5]. Botnets may also be used to spread malware and steal login details from IoT devices, making phishing, ransomware, and identity theft possible [1]. Since IoT devices are found in many places and are not always secure, attackers can easily target them, and this can result in machines not working, financial costs, and damage to the company’s reputation. As IoT grows, it is important to have strong security at each device, keep updates regular, and use security products that can be scaled to address botnet risks.

## Artificial Intelligence in Security of IoT

AI and ML help a great deal to secure IoT networks, mainly by discovering and stopping issues caused by botnets [5]. Like people, AI systems look at lots of data, notice patterns, and decide on their own, while ML is a branch of AI that allows models to figure out answers on their own, using the information they are given [6]. They are essential for cybersecurity since they assist in managing the fast and large data volumes people cannot deal with by themselves. By detecting patterns and making choices, AI in Intrusion Detection Systems (IDS) monitors the network traffic and looks through it to identify the presence of botnets by identifying any unusual behavior or abrupt increase in traffic [7]. Even when it is difficult to differentiate between botnet and normal traffic in the network, ML technology can detect botnets in a network where there are many IoT devices. Also, it can be applied to detect new security threats, such as unusual traffic, given that it may detect botnets that elude typical security scans. Streaming ML frameworks are most of the time employed to identify anomalies in real-time as data is constantly moving through the trained models. They help to make responses quicker, isolate threats as they occur, and reduce the proliferation of any breach of security. Nevertheless, it is necessary to consider which type of model is the most accurate, with the least latency and computers resources demand. Deep learning is especially effective when processing large volumes of data to detect complex and constantly evolving attack strategies [8]. AI and ML allow security solutions to remain adaptive and identify emerging attacks by managing the increasing IoT devices.

## Mitigation for Botnets in IoT Networks

To secure IoT networks against botnets, proactive tools and immediate response are essential, as well as the use of AI in monitoring and detecting the indicators of botnet presence [9]. These systems are helpful in disconnecting with infected devices, preventing malicious traffic, or alerting administrators to respond promptly. With Software-Defined Networking (SDN), botnets can be combated because they offer a more flexible and programmable network which can be controlled and updated in real time [10]. SDN enables the administrator to easily isolate compromised devices and redirect traffic thus the network is more secure than a static network configuration. As we evolve botnets, we should continue to evolve our mitigation. AI systems should be able to learn new data and change their detection and response strategies. The combination of AI and SDN provides IoT networks with powerful and adaptable security against any emerging forms of cyber threat.

## Evaluation Matrix

To evaluate the proposed botnet detection models, several evaluation measures are used, such as accuracy, precision, recall, F1 score, and the confusion matrix. These metrics give a full understanding of the models’ ability to differentiate between IoT traffic as either benign or malicious.

1. Accuracy: Accuracy is defined as a total number of instances that are classified correctly as benign or malicious, divided by a total number of instances. It is calculated as shown in Equation (1).

(1)

1. TP: True Positives (correctly classified malicious traffic).
2. TN: True Negatives (correctly classified benign traffic).
3. FP: False Positives (benign traffic misclassified as malicious).
4. FN: False Negatives (malicious traffic misclassified as benign).
5. Precision: Precision or the positive predictive value measures the proportion of actual positives among all the positive predictions made. It focuses on minimizing false positives and is defined as shown in Equation (2).

(2)

1. Recall: Recall is a measure of a model to identify all actual positive instances out of all the model’s predicted positives. It calculates the proportion of true positives correctly identified out of all actual positive cases and is defined as shown in Equation (3).

(3)

1. F1-Score: The F1-Score is the harmonic mean of precision and recall and is a useful measure when there is a major difference between false positive and false negative results. It is calculated as shown in Equation (4).

(4)

# AI Techniques for IoT Botnet Security

## Methodology and Techniques for Botnet Detection

ML is popular in botnet detection as it can identify patterns in the traffic of large networks. Algorithms vary in their strengths and weaknesses based on how complex the data is, what resources are available, and what the system needs. Decision Trees and K-Means are helpful for basic detection jobs and in real time, yet they can have trouble with changing or noisy data. Random Forests, SVMs, and Neural Networks, which are more advanced, work better in difficult or nonlinear situations, but they are more challenging to use and need more resources. Table 1 outlines the main features of widely used algorithms, giving an overview of how effective they are, their weaknesses, and the resources they need for IoT botnet detection.

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLE 1.** Machine learning algorithm | | | |
| **Algorithm** | **Advantages** | **Limitation** | **Computational Cost** |
| Decision Tree (DT) | Simple to understand, easy to implement, interpretable rules | Prone to overfitting, less effective with noisy data | Low |
| Random Forest (RF) | Robust to overfitting, handles high-dimensional data well | Less interpretable, slower than a single tree | Medium |
| Support Vector Machine (SVM) | Effective in high-dimensional spaces, good at handling small sample sizes | Not suitable for large datasets, sensitive to parameter tuning | High |
| Artificial Neural Network (ANN/MLP) | Capable of modelling complex nonlinear relationships | Requires large datasets, sensitive to overfitting and hyperparameters | Medium to High |
| Convolutional Neural Network (CNN) | Excellent at pattern recognition and spatial/temporal analysis | Requires more data and training time, not suitable for low-resource devices | High |
| K-Means Clustering | Simple, scalable, unsupervised, does not require labelled data | Needs predefined number of clusters, sensitive to outliers | Low to Medium |

It is now widely accepted that AI is an important tool in proactive detection and countermeasures against botnet attacks on the IoT systems. Recent literature has reviewed different methods that integrate SDN, intrusion detection systems, and honeypots to provide agile, adaptive, and scalable defenses against threats. Afterward, the document introduces significant AI-driven countermeasures, recorded in the reviewed research, summarizing their effectiveness, limitation, and processing needs shown in Table 2.

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLE 2.** Botnet mitigation method | | | |
| **Methodology** | **Advantages** | **Limitation** | **Computational Cost** |
| CatBoost with SDN | Fast prediction speed, efficient with SDN control logic | Requires SDN infrastructure; less interpretable than simpler models | Medium |
| CNN-based DepBot in SDN | Learns complex DDoS patterns; enables dynamic mitigation via OpenFlow | High model complexity; needs large training data and resources | High |
| ML-Integrated SDN-IDS | Adaptive rule updates; real-time intrusion response | Relies on accurate IDS alerts; IDS tuning required | Medium to High |
| ML-based Honeynet | Distributed detection; scalable via cloud coordination | Delayed reaction due to central analysis; dependent on honeypot quality | Medium |
| Naive Bayes + PCA in SDN | Lightweight and interpretable; reduces data dimensionality via PCA | May underperform with complex attack patterns; sensitive to data noise | Low to Medium |

# Result and Discussion

Table 3 outlines how different ML models perform when used for detecting bots in the CTU-13 dataset. DT are easy to use and quick, having an accuracy of 85%. By combining DTs, RF can achieve a f1-score level of 95%. SVMs are not as effective at 78% accuracy because their data is not linear. Although ANN and CNN models are accurate 99.94% and 100%, using them requires more computing power. This method provides 94% accuracy and is helpful when identifying new attacks without having known examples. Still, despite deep learning being the most precise, DT and RF are helpful because they are quick and easy to understand.

**TABLE 3.** Botnet mitigation method

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Author(s)** | **Year** | **Dataset** | **Algorithm** | **Accuracy** | **Challenges** | **Remarks** |
| Ibrahim et al., [7] | 2020 | CTU-13 | K-Means Clustering | 94% | Needs strong feature engineering; cannot label traffic directly. | Unsupervised; good for unknown threats or anomaly detection. |
| Velasco-Mata et al., [11] | 2021 | CTU-13 | Decision Tree (DT) | 85% (F1-Score) | Needs optimal feature selection for efficient classification. | Interpretable and efficient, good for lightweight systems. |
| S. Padhiar et al., [12] | 2020 | CTU-13 | Random Forest (RF) | 95% | Requires continuous adaptation to evolving botnet behaviours. | Strong ensemble model with high generalization. |
| A. Alharbi et al., [13] | 2023 | CTU-13 | Artificial Neural Network (ANN) | 99.94% | High false positives; needs up-to-date training data. | Excellent accuracy but requires large, current datasets. |
| M.W. Nadeem et al., [14] | 2021 | CTU-13 | Convolutional Neural Network (CNN) | 100% | High computational cost and tuning complexity. | Top accuracy; ideal for high-resource environments. |

With ML, SDN-based mitigation systems rapidly identify and deal with traffic from botnets. While CatBoost works well against UDP flooding, it has difficulties handling more advanced types of attacks. It stops DDoS floods but is unable to protect against spoofed or multi-vector attacks. Using SDN IDS alerts with SIEM helps to find threats more easily, but it may delay the response time. Honeynets do not stop attacks right away as they are used for analysis, leaving the main systems unprotected for a short time. While Naive Bayes with PCA can work quickly, it has difficulties with complex or encrypted traffic. To sum up as shown in Table 4, these methods try to strike a balance between speed and accuracy, though they may struggle with handling advanced or varied attacks from bots.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TABLE 4.** Botnet mitigation method | | | | | |
| **Author(s)** | **Year** | **Mitigation Method + Model/Approach** | **Mitigation Strategy** | **Testbed / Dataset** | **Challenges Noted** |
| Wani et al., [9] | 2020 | Naive Bayes + PCA-based SDN Flow Filter | Blocks malicious TCP/IP flows at switch level based on lightweight PCA-transformed NB classification | SDN controller analyzing header-level traffic | Ineffective for encrypted/deep payloads; limited feature visibility |
| S. R, A. Raj et al., [10] | 2021 | CatBoost-based DDoS Flow Mitigator via SDN Controller | Blocks high-rate traffic at ingress switches using SDN flow rules triggered by CatBoost classification | Mininet + RYU + Custom UDP Botnet | Static rule logic; limited to 2 features; effective only for UDP flooding |
| B. Al-Duwairi et al., [15] | 2023 | CNN-based DepBot integrated into SDN Controller | Dynamically pushes flow rules to mitigate botnet-based DDoS using real-time CNN predictions | Real SDN testbed + custom dataset | Only works on flooding DDoS; lacks spoofing resistance; limited testbed scope |
| Al-Duwairi et al. [16] | 2020 | ML-Integrated SDN-IDS with SIEM Coordination | Parses IDS alerts in SIEM and modifies SDN flow rules to isolate/drop malicious flows | SDN + Splunk SIEM integration | Coordination overhead; mitigation delay due to SIEM parsing and flow updates |
| Banerjee et al. [17] | 2021 | ML-Guided SDN Honeynet for Botnet Isolation | Reroutes attack flows to honeypot zones; isolates malicious behavior using ML classification | Simulated SDN with trap zones | Reactive-only; depends on attackers interacting with the honeynet |

# CONCLUSION

As IoT networks keep expanding, they become more prone to botnet attacks, making it important to have smart defenses that can detect and stop these attacks in real time [18]. The review highlights that AI, especially machine learning and deep learning, is key to improving the security of IoT devices. While CNN and ANN models can do well at spotting objects, they require a lot of computing power. Simple models like decision trees and random forests are both effective and efficient, and K-Means clustering has the potential to discover unknown threats using data that is not pre-labelled. Moreover, using AI and SDN together makes it easier to adjust and expand defense methods. Still, there are obstacles, such as uneven data amounts, different types of devices, and new kinds of danger. In the future, AI should be made lightweight, easy to understand, and able to adapt to the different requirements of IoT systems, protecting IoT environments from botnet attacks and helping develop strong, smart networks.

# References

1. R. S. S. Moorthy, and N. Nathiya, “Botnet Detection Using Artificial Intelligence,” Procedia Computer Science **218**, 1405–1413 (2023).
2. M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, “Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research,” Applied Sciences **11**(12), 5713 (2021).
3. S. Pokhrel, R. Abbas, and B. Aryal, “IoT Security: Botnet detection in IoT using Machine learning,” arXiv.Org, (2021).
4. S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, “Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey,” IEEE Access **9**, 94668–94690 (2021).
5. C. Kaushik, D. VarunTeja, M. S. Krishna, and S. Jaavali, “DDoS Attack Detection and Mitigation Using Mininet and RYU Controller in SDN Environment,” in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, (IEEE, Kamand, India, 2024), pp. 1–7.
6. A. K. Abed, and A. Anupam, “Review of security issues in Internet of Things and artificial intelligence‐driven solutions,” Security and Privacy **6**(3), e285 (2023).
7. Ibrahim Wan Nur Hidayah, Selamat Ali, Anuar Syahid, and Krejcar Ondrej, “Clustering Botnet Behavior Using K-Means with Uncertain Data,” in *Frontiers in Artificial Intelligence and Applications*, (IOS Press, 2019).
8. A. K. Kumar, S. Rathnamala, T. Vijayashanthi, M. Prabhananthakumar, A. Panthakkan, S. Atalla, and W. Mansoor, “Enhanced Hybrid Deep Learning Approach for Botnet Attacks Detection in IoT Environment,” in *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, (IEEE, Dubai, United Arab Emirates, 2024), pp. 1–6.
9. A. Wani, and S. Revathi, “Ransomware protection in IoT using software defined networking,” IJECE **10**(3), 3166 (2020).
10. S. R, A. Raj, K. Saivenu, M. I. Ahmed, S. B, and A. Kanavalli, “Detection and mitigation of botnet based DDoS attacks using catboost machine learning algorithm in SDN environment,” IJATEE **8**(76), 445–461 (2021).
11. A. Delplace, S. Hermoso, and K. Anandita, “Cyber Attack Detection thanks to Machine Learning Algorithms,” arXiv.Org, (2020).
12. S. Padhiar, and R. Patel, “Performance evaluation of botnet detection using machine learning techniques,” IJECE **13**(6), 6827 (2023).
13. A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, “Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things,” Electronics **10**(11), 1341 (2021).
14. M.W. Nadeem, H.G. Goh, Y. Aun, and V. Ponnusamy, “Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques,” IEEE Access **11**, 49153–49171 (2023).
15. 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,” IJECE **10**(2), 2182 (2020).
16. M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, “Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques,” Sensors **24**(11), 3571 (2024).
17. S. Banerjee, and P.S. Chakraborty, “To Detect the Distributed Denial-of-Service Attacks in SDN using Machine Learning Algorithms,” in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, (IEEE, Greater Noida, India, 2021), pp. 966–971.
18. A. Hussain, U. Farooq, and I. Rabbi, "Facilitating digital experience sharing among vehicles through utilisation of pre-existing communication infrastructure," Journal of Informatics and Web Engineeringf 4(2), 262–274 (2025). https://doi.org/10.33093/jiwe.2025.4.2.17