Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

2025 Volume 5, Issue 1: 15–24
DOI: https://doi.org/10.48185/jitc.v5i1.1047

Deep Learning Techniques for Detecting BOTNET Attacks in IOT Environments: A Review

AREMU B. L.

Department of Computer Science, Faculty of Natural and Applied Sciences, Al-Hikmah University, Ilorin, Nigeria

Received: 10.07.2024 • Accepted: 24.08.2025 • Published: 14.09.2025 • Final Version: 12.10.2025

Abstract: With the exponential growth of the Internet of Things (IoT) and its increasing integration into various domains, security threats have become a significant concern. One of the most menacing threats in the IoT landscape is botnet attacks, which can cause extensive damage and compromise the privacy and integrity of data via commands and control mechanisms. Traditional security measures are often insufficient in detecting these sophisticated attacks. This review explores the application of deep learning techniques for botnet detection in IoT environments. By analyzing the strengths and limitations of various deep learning models, the aim is to provide insights into their effectiveness and potential for securing IoT ecosystems. Thus, this study will provide better understanding of how deep learning-based models can be built using some novel approaches.

Keywords: Deep Learning, BOTNET Attacks, IoT, Machine Learning, DDoS

1. Introduction

The Internet of Things (IoT) refers to a collaborative network comprising interconnected devices that can autonomously make decisions without human intervention. Saheed, Abiodun, Misra, Holone, Palacios (2022). Advancements in technologies such as automatic identification, sensors, tracking, wireless communications, embedded computing, distributed services, and 5G networks have facilitated the integration of sophisticated objects into our daily lives through the Internet. This convergence of the Internet and intelligent communicative objects has positioned the IoT as a pivotal player in the ICT industry for the foreseeable future.

In the IoT, a "thing" encompasses a vast array of entities, including individuals equipped with blood pressure monitoring implants, sensor-equipped vehicles that alert drivers about low tire pressure, tagged farm animals, or any object capable of data transfer through an IP address over a network. According to Cisco, approximately 50 billion devices were connected to the Internet in the year 2020 (Cisco Annual Internet Report, 2018-2023). Despite its potential to revolutionize various aspects of society and industry, the IoT's widespread adoption requires robust security measures to address increased accessibility and potential risks. The IoT's success hinges on reducing energy consumption, given that low battery capacities significantly impact network performance and quality of service (QoS). The scope of IoT devices is extensive, encompassing healthcare devices, wearables, industrial robots, smart televisions, and remotely monitored smart city infrastructures. The IoT holds promising applications; however, a considerable portion of the population, approxi-

* Corresponding Author: moruff.oyelakin@cuab.edu.ng

mately 87 percent, remains unfamiliar with the term "IoT".

The most common attacks that heavily jeopardize IoT devices are botnet attacks. A botnet is defined as a group of internet-connected devices running more than one bot (Ahmed et al., 2019). However, they are used to execute Distributed Denial-of-service (DDoS) attacks and steal data. Furthermore, they are also used to allow access to data, a major privacy issue in the IoT environment. The reason for this attack is that IoT is composed of heterogeneous environments and resource constraints such as low memory and computational power (Bojarajulu et al., 2023). The constraints promote security-related problems which are critical and need to be adequately scrutinized. Hence, deep learning techniques are deemed the suitable way to deal with botnet attacks in an IoT environment. A review is needed to assess whether deep learning techniques are deemed the suitable way to deal with botnet attacks in an IoT environment.

According to Oyelakin et al. (2020), there are increased malware attacks in networks, and significant machine learning techniques have been used to address the problem. There is a need for an implementation of a detection system that will address any significant challenge in the future. Regardless of the existing detection systems, they do not have the capacity to address the issue due to the variations that are used for the penetration. Overall, the detection systems are classified into two significant aspects, anomaly-based and misused systems. Based on the detection architecture, such deep learning techniques can be categorized into networked-based and host-based detection techniques (Soe et al., 2020). The implementation of IoT is already done, and the technology is becoming efficient. However, what awaits is the security concerns, and when not addressed in time, will heavily affect the existing population.

According to the Cisco Annual Internet Report (2023), there will be high growth of mobile data traffic, making it necessary to understand the role of deep learning techniques. Unfortunately, most IoT devices continue to be attacked with escalated cybersecurity threats. Oyelakin et al (2020) also pointed out that threats landscape in the cyber space keeps widening on daily basis. This implies there is constant growth in the rate of cyber criminals. The most suitable way is to focus on long-lasting and cost-effective solutions that would address any future issues. Deep learning techniques such as misuse-based detection are not only relevant in addressing botnet attacks but also offer a better solution to the existing attack signatures. Basically, the techniques are effective depending on to what level they are implemented. Therefore, it is essential to highlight that with the effective consideration of the techniques, it will be easy to achieve better results.

Additionally, Hussain et al. (2020) in their study found that deep learning techniques can be used as a detection mechanism for botnet attacks. It also detects their capability and is able to create a false-positive alarm for effective management. Another problem is the use of outdated datasets through IoT devices, which creates a better foundation for cybercriminals. It means the solution may not necessarily lie with the traditional management approach but the machine learning ones; besides, there is a need to integrate the IoT attack records, which will make it easy to implement deep learning technique and detection model for IoT attacks (Saheed et al., 2022). Therefore, deep learning techniques are deemed the suitable way to deal with botnet attacks in an IoT environment.

By analyzing the strengths and limitations of various deep learning models, the aim is to provide insights on how best to build improved machine learning techniques for detecting botnet attacks.

1.1. Statement of the Problem

In the ever-evolving landscape of cybersecurity, the proliferation of Internet of Things (IoT) devices has brought about new challenges in detecting and mitigating botnet attacks. Deep learning

techniques have emerged as a promising approach to fortify IoT environments against such threats. This review employs a structured approach to comprehensively assess the current literature on deep learning applications for botnet attack detection in IoT environments. Extensive searches of peer-reviewed journals, conference proceedings, and reputable online databases are conducted to identify relevant studies. Inclusion criteria encompassing research papers that utilized deep learning algorithms for IoT botnet detection and the selected studies are critically analyzed to extract valuable insights.

Existing research on IoT security and intrusion detection techniques are reviewed, highlighting the shortcomings of current approaches and the need for innovative solutions that address the unique challenges of IoT networks.

1.2. Aim and Objectives

The aim of this study is to review deep learning techniques for detecting botnet attacks in IoT environments.

The specific objectives of this study are to:

i. source for relevant literature on deep leaning techniques for detecting botnet attacks in IoT environments from notable repositories and

ii. carry out a review of some of the existing literature on the use of deep leaning techniques for detecting botnet attacks in IoT environments.

1.3. Significance of the Study

This review has significant benefits for various stakeholders in the field of IoT security and network management. Below are some of the major stakeholders who will benefit from the outcome of this research, and the benefits they will derive:

i. General internet users: As IoT devices become more secure against botnet attacks due to the implementation of advanced deep learning techniques, internet users will have increased confidence in using these devices without worrying about potential security breaches.;

ii. Security experts and professionals: Security professionals responsible for securing IoT systems in various organizations will benefit from this research by gaining knowledge about the most effective deep learning techniques for botnet detection. This can assist them in devising better strategies to safeguard their IoT infrastructures and quickly respond to potential attacks;

iii. Security researchers: Researchers in the field of security will benefit from this review as it can serve as a foundation for future studies and advancements in botnet attack detection using deep learning.

2. Literature Review

Machine learning is a field within computer science with the objective of empowering computers to acquire knowledge autonomously, and without explicit programming it. The roots of machine learning can be traced back to the artificial intelligence movement of the 1950s. It focuses on practical goals and real-world applications, especially in prediction and optimization (Bi, Goodman, Kaminsky & Lessler, 2019). The core idea in Machine Learning is to allow computers to recognize

patterns, make decisions, and gain insights from experience, just like how humans learn from their experiences.

According to DeLancey, Simms, Mahdianpari, Brisco, Mahoney & Kariyeva (2019), there are generally two categories of Machine Learning: Shallow learning and deep learning. In deep learning, many successive layered representations of data are used, such as hundreds of convolutions/filters. However, in shallow learning one or two layered representations of the data are typically used. Deep learning has significant potential in addressing various tasks, including but not limited to image recognition, natural language processing, speech recognition, surpassing human Go playing, and autonomous driving.

Deep learning refers to a class of artificial intelligence methods based on neural networks with multiple layers. Key advantages of deep learning include the ability to automatically extract complex features and patterns from raw data and detect anomalies and outliers. Studies have shown deep learning models match or outperform traditional machine learning in detecting network intrusions and malware (Yin et al., 2017). However, deep learning has not been extensively applied to detecting threats in IoT environments.

The transition from shallow learning to the era of deep learning was driven by several key factors, including advances in computational power, the availability of large-scale datasets, and the development of innovative neural network architectures (Wei, Chu, Sun, Xu, Deng, Chen & Lei 2019). Below are some of the advantages of deep learning techniques over shallow learning:

i. Increase in Computational Power: Deep learning models are more computationally intensive than shallow learning models due to their complex architectures with multiple layers of neurons. With the advent of powerful and affordable GPUs (Graphics Processing Units) and other hardware accelerators, the computational power required to train and run deep learning models became more accessible and feasible.

ii. Emergence of Big Data: The proliferation of the internet, digital devices, and sensor technologies led to the generation and accumulation of massive amounts of data. Deep learning algorithms thrive on large-scale datasets, and having access to vast amounts of labeled data became crucial for training deep neural networks effectively.

iii. Breakthroughs in Neural Network Architectures: Researchers made significant advancements in designing effective neural network architectures that could handle deeper layers while mitigating the problem of vanishing gradients. Key breakthroughs include the development of Convolutional Neural Networks (CNNs) for image processing and Recurrent Neural Networks (RNNs) for sequential data, such as natural language.

iv. Success in Image and Speech Recognition: Deep learning demonstrated remarkable performance improvements in image recognition and speech recognition tasks, surpassing the capabilities of traditional machine learning algorithms. The successful application of deep learning in these areas attracted significant attention and funding, further propelling its development.

v. Introduction of Deep Learning Frameworks: The creation of user-friendly and efficient deep learning frameworks, such as TensorFlow and PyTorch, provided researchers and developers with tools to experiment, implement, and deploy deep learning models more effectively and efficiently.

vi. Exploration of Deep Neural Networks' Representational Power: Researchers began to realize the impressive representational power of deep neural networks, allowing them to learn intricate

patterns and hierarchies in the data. This ability to learn hierarchical representations made deep learning models more adept at handling complex and high-dimensional data, such as images and natural language.

Deep learning, a subset of artificial intelligence, has showcased remarkable potential in diverse fields. Figure 1. Tamoghna Ghosh & Shravan Kumar Belagal Math, 2023. Its ability to automatically learn intricate patterns and representations from complex data makes it an ideal candidate for addressing the challenges of IoT security. In the context of botnet detection, deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN) have shown promising results.

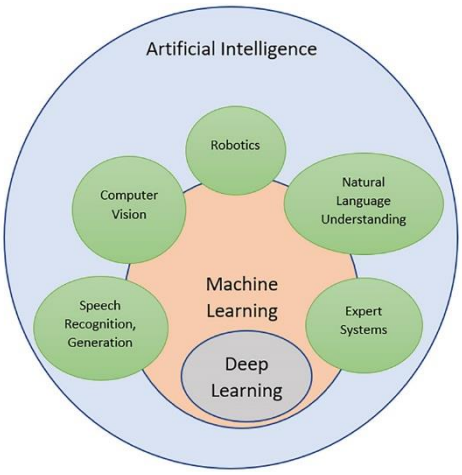

Figure 1: Subsets of Artificial Intelligence. Tamoghna Ghosh & Shravan Kumar Belagal Math (2023)

The Internet of Things (IoT) denotes an extensive and interconnected network of computer devices, such as sensors, that engage in swift data exchange. Gazis, A. (2021). Additionally, this seamless interconnection between devices is established through Machine-to-Machine communication (M2M), which provides a standardized method for diverse machines engaged in various tasks to communicate and exchange information on a global level rapidly.

A botnet is a network of compromised devices controlled by a malicious entity, the "botmaster," which enables attackers to send commands to compromised devices to launch various cyberattacks (Antonakakis et al., 2017). In IoT environments, botnets can exploit device vulnerabilities to conduct denial-of-service attacks, steal private data, or use devices without the owners' knowledge, such as for crypto mining. Attackers can also hide botnet traffic within legitimate IoT protocols to evade detection. Defending against botnets poses a formidable challenge, as they can rapidly evolve and leverage new vulnerabilities.

2.1. Related Work

The constant introduction of diverse devices has led to significant growth, which in turn has brought forth new concerns regarding privacy and security. With the increasing number of Internet-connected devices and the emergence of IoT technologies, computer networks face a surge of sophisticated intrusions. Saheed, Abiodun, Misra, Holone & Colomo-Palacios (2022). To tackle this issue, companies are investing more in research to enhance attack detection. They are comparing different intelligent methods for testing and verification to identify the most accurate ones. The adoption of IoT has also risen across various sectors, including healthcare, gaining popularity among technology researchers and developers. Nevertheless, the pressing challenge of IoT lies in its privacy and security

vulnerabilities, stemming from energy constraints and the scalability limitations of IoT devices. Consequently, finding solutions to improve IoT's security and privacy issues remains a crucial problem in the field of computer security. This paper therefore presented a proposal for an intrusion detection system (IDS) based on machine learning (ML-IDS) to identify attacks on IoT networks. The main focus of this research revolves around applying supervised machine learning algorithms for IoT-based intrusion detection. The researchers concluded that this approach can be enhanced in the future by incorporating deep learning models.

In another research paper by Chen, Sheu, Kuo, & Van Cuong (2020), the researchers presented an innovative approach to counter Distributed Denial of Service (DDoS) attacks within IoT gateways using a multi-layer machine learning-based detection system. Their system effectively identifies various types of DDoS attacks, such as sensor data flood, ICMP flood, SYN flood, and UDP flood, by converting their distinguishing features into numerical representations. By simulating real-world conditions, they conducted DDoS attacks from eight smart poles, resembling an actual IoT environment. The results demonstrated the high accuracy of our multi-layer DDoS detection system in accurately differentiating between normal and attack packets originating from IoT devices. The proposed method achieves a remarkable F1-score exceeding 97%. Their multi-layer DDoS detection system not only identified DDoS attacks but also effectively thwarted the malicious devices. It is important to note that this solution has certain limitations, including the artificial feature marking, rendering the trained model non-transferable to new domains. However, they anticipated potential enhancements through the integration of alternative unsupervised learning approaches in future research endeavors.

Furthermore, a study by Pajouh, Javidan, Khayami, Dehghantanha, & Choo (2016) introduced a novel framework consisting of a two-layer dimension reduction and classification model. The primary aim was to identify unauthorized activities within IoT backbone networks, with a specific focus on detecting infrequent attacks (e.g., U2R and R2L) that possess significant threat potential. Their newly devised model surpassed the performance of comparable existing models, displaying superior detection rates for both uncommon and typical attacks. By incorporating a blend of unsupervised (PCA) and supervised (LDA) feature extraction techniques, their approach achieved accurate discrimination between distinct attack categories and normal behaviors, facilitated by the inclusion of advanced classification algorithms.

Pajouh et al. wanted to delve in the future into the application of non-parametric strategies like dimension reduction modules and fuzzy clustering, in pursuit of enhancing classification accuracy against U2R, R2L, and other attack types. Additionally, there was an intriguing avenue for further research which involved extending the proposed model's capabilities to identify intrusions across diverse layers of the IoT architecture, including the application and support layers, as well as various protocols operating within the network layer.

In their study, Anthi, Williams and Burnap (2018) aimed to create Pulse, an innovative and adaptable Intrusion Detection System (IDS) tailored for IoT environments. Their proposed model operated in real-time, utilizing both signature-based and anomaly-based detection methods within a network context. The development occurred in two distinct phases. In the initial phase, an IoT smart-home testbed was constructed, and benign network activities were closely monitored to establish a baseline of normal behavior for each connected device. The subsequent phase involved subjecting the same network to various attacks and malicious activities, such as network scanning, while continuously recording network traffic. These two phases yielded two datasets: one containing benign network traffic and the other encompassing malicious activity. Subsequent to data collection, a Machine

Learning (ML) model was constructed to form the core of the proposed IDS. To train this model, supervised ML algorithms were employed. The resulting model could detect network traffic anomalies, even in instances of previously unseen attacks. Moreover, it had the capacity to learn and improve its accuracy over time, enhancing its ability to identify attacks. A supplementary component of the system comprised a rule-based algorithm, consisting of diverse rules that complemented the outcomes produced by the ML model. It was expected that this integration would enhance the overall predictive accuracy.

While their preliminary outcomes were promising, there remained several aspects and parameters requiring further consideration for the comprehensive development of Pulse. Initial steps included grouping similar devices together through clustering, thereby deriving a standard traffic behavior for each device cluster. This approach was envisioned to enhance the accuracy of anomaly detection and malicious node identification. Additionally, they wanted to conduct an expanded range of attacks, for more comprehensive testing. Furthermore, the inclusion of additional features, such as Payload and Ingoing/Outgoing ratio, in ML training should be explored. Finally, the rule-based algorithm alluded to in the generic architecture of Pulse. This needed to be developed and integrated in the future.

Another research conducted by Diro and Chilamkurti (2018) was aimed at adopting the deep learning approach to cybersecurity for detecting attacks in social internet of things. The performance of this deep model was compared against the traditional machine learning approach, Furthermore, distributed attack detection was evaluated against their centralized detection system. The experiments proved that their distributed attack detection system was superior to centralized detection systems using deep learning model. It was also demonstrated that the deep model was more effective in attack detection than its shallow counter parts. Furthermore, their deep learning model proved its superiority over conventional machine learning techniques like softmax in the task of classifying network data as normal or attack on previously unseen test data. Moving forward, their future endeavours would encompass a comparative assessment of distributed deep learning IDS using an alternative dataset, in conjunction with various traditional machine learning algorithms such as SVM, decision trees, and diverse neural networks. Finally, they intend to explore in the future the potential of network payload data in intrusion detection, recognizing its potential to unveil essential patterns for differentiation.

In another research paper, Hodo, Bellekens, Hamilton, Dubouilh, Iorkyase, Tachtatzis and Atkinson (2016) presented a neural network-based approach for intrusion detection on IoT network to identify DDoS and DOS attacks. Their detection was based on the classification of normal and threat patterns. They validated their ANN model against a simulated IoT network. This model demonstrated over 99% accuracy. It was able to identify successfully different types of attacks and showed good performances in terms of true and false positive rates. For future developments, Hodo et al. wanted to introduce more attacks to test the reliability of their method against attacks and improve the accuracy of the framework. Furthermore, they would investigate other deeper neural networks such as the recurrent and convolutional neural network approach.

Javaid, Niyaz, Sun & Alam (2016) proposed a deep learning-based approach for developing an efficient and flexible Network Intrusion Detection System (NIDS). They used Self-taught Learning (STL), which is a deep learning-based technique, on NSL-KDD - a benchmark dataset for network intrusion. In the near future, they planned to use deep learning technique to implement a real-time NIDS for actual networks. Another high-impact research area they planned to explore in this area is on-the-go feature learning on raw network traffic headers instead of derived features.

According to Hezam, Mostafa, Ramli, Mahdin & Khalaf (2021), the impacts of Distributed-Denial-of-Service (DDoS) attacks were undoubtedly significant and were continuously growing, especially

with the proliferation of Internet-of-Things (IoT) devices. Despite numerous efforts to detect and mitigate such attacks, the threat remains persistent and more substantial than ever. DDoS attacks involve flooding a targeted computer or resource with fake requests, overwhelming the system and obstructing genuine requests from being fulfilled. These attacks are often orchestrated through botnets, with new variants becoming increasingly sophisticated and hard to counter.

To address this challenge, the researchers explored various approaches, including middle-box and Artificial Intelligence (AI) solutions utilizing machine learning (ML) techniques. In this paper, the authors proposed a deep learning (DL) approach using three specific DL algorithms: recurrent neural network (RNN), convolutional neural network (CNN), and Long short-term memory (LSTM)-RNN. Their goal was to defend against DDoS attacks specifically targeting IoT networks. The performance of the three algorithms was compared in terms of accuracy, precision, recall, and f-measure. The results demonstrate that the RNN achieved the highest accuracy at 89.75% among the three algorithms, followed by the LSTM-RNN and the CNN.

3. Methodology

In this review paper, many searches were conducted using a wide range of search strings. The following search phrase were used: (“deep learning techniques”), (“deep learning techniques for detecting botnet attacks” OR “deep learning techniques for detecting botnet attacks in IoT environments”), (“Network Intrusion Detection”), (“IoT”), (“Distributed Denial of Service” OR “DOS/DDOS”) and (“Intrusion Detection System”). The above search phrases were considered so as to obtain a good number of relevant studies in research repositories for the review being carried out.

The following platforms were used to for conducting researches: Google Scholar, Researchgate, Academia.edu, IEEE Explore, ACM Conference, Science Direct, Google search engine, etc.

4. Findings & Discussions

From the above reviews, there has been significant research in the various areas of machine learning for detecting botnet attacks in IoT environments. However, the use of deep learning techniques has not been explored well enough. There is still a need for more research to develop effective and efficient deep learning models that can detect botnet attacks in real-time and with higher accuracy.

In addition, as IoT devices often collect sensitive data, privacy concerns are paramount. Investigating privacy-preserving mechanisms within deep learning models, such as Federated Learning or Differential Privacy, can safeguard user data while maintaining the efficacy of botnet detection. Specifically, there is a need for research that addresses the following needs:

- Developing deep learning models that can detect botnet attacks in real-time and with higher accuracy.
- Developing deep learning models that can detect botnet attacks in heterogeneous IoT environments.
- Developing deep learning models that can detect new and unknown botnet attacks.

5. Conclusion

This study has carried out review of works that use various machine learning techniques for detecting botnet attacks and other forms of intrusion. This study has done that extensively so as to provide further insights into how to protect IoT devices.

References

[1] Ahmed, Z., Danish, S. M., Qureshi, H. K., & Lestas, M. (2019, September). Protecting iots from mirai botnet attacks using blockchains. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). IEEE.

[2] Almalki, L., Alnahdi, A., & Albalawi, T. (June 14, 2023). Role-Driven Clustering of Stakeholders: A Study of IoT Security Improvement. *Sensors 2023*, 23(12), 5578. https://doi.org/10.3390/s23125578.

[3] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Mao, C. (2017). Understanding the Mirai Botnet. In *26th USENIX Security Symposium* (pp. 1093-1110). Vancouver, BC, Canada: USENIX Association.

[4] Bojarajulu, B., Tanwar, S., & Singh, T. P. (2023). Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model. *Computers & Security*, *126*, 103064.

[5] Catillo, M., Pecchia, A., Villano, U. (Jan 7, 2023). A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection. *Applied Sciences*, 2023, 13(2), 837; https://doi.org/10.3390/app13020837.

[6] Chen, Y. W., Sheu, J. P., Kuo, Y. C., & Van Cuong, N. (2020, June). Design and implementation of IoT DDoS attacks detection system based on machine learning. In 2020 European Conference on Networks and Communications (EuCNC) (pp. 122-127). IEEE.

[7] Cisco Annual Internet Report. (2018-2023). *White paper, Cisco Public*. (pp. 2).

[8] Deeks, M. A Review on Botnet Attacks. Preprints 2023, 2023070366. https://doi.org/10.20944/preprints202307.0366.v1.

[9] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.

[10] Diro, A., Chilamkurti, N., Nguyen, V.-D., & Heyne, W. (2021). A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. *Sensors*, 21(24), 8320. http://dx.doi.org/10.3390/s21248320.

[11] Gazis, A. (2021). What is IoT? The Internet of Things explained. Academia Letters, Article 1003. https://doi.org/10.20935/AL1003.

[12] Haq, M.A. (Feb 27, 2023). DBoTPM: A Deep Neural Network-Based Botnet Prediction Model. *Electronics 2023*, 12(5), 1159. https://doi.org/10.3390/electronics12051159.

[13] Hezam, A. A., Mostafa, S. A., Ramli, A. A., Mahdin, H., & Khalaf, B. A. (2021, August). Deep learning approach for detecting botnet attacks in IoT environment of multiple and heterogeneous sensors. In *International Conference on Advances in Cyber Security* (pp. 317-328). Singapore: Springer Singapore.

[14] Hezama, A. A., Mostafa, S. A., Baharumb, Z., Alanda, A., & Salikon, M. Z. (2021) Combining Deep Learning Models for Enhancing the Detection of Botnet Attacks in Multiple Sensors Internet of Things Networks. *International Journal on Informatics Visualization.* 5(4), 380-387.

[15] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

[16] Hussain, F., Abbas, S. G., Fayyaz, U. U., Shah, G. A., Toqeer, A., & Ali, A. (2020, November). Towards a universal features set for IoT botnet attacks detection. In *2020 IEEE 23rd International Multitopic Conference (INMIC)* (pp. 1-6). IEEE.

[17] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26).
[18] Oyelakin A. M., Alimi M. O. & Abdulrauf T. (2020). Performance analysis of selected machine learning algorithms for the classification of phishing URLs. *Journal of Computer Science and Control Systems*, *13*(2), 16-19.
[19] Oyelakin, A. M., & Jimoh, R. G. (2021). A Survey of Feature Extraction and Feature Selection Techniques Used in Machine Learning-Based Botnet Detection Schemes. *VAWKUM Transactions on Computer Sciences,* 9(11), 01-07.
[20] Pajouh, H. H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K. K. R. (2019). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing, 7(2), 314-323.
[21] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409. https://www.sciencedirect.com/science/article/pii/S1110016822001570.
[22] Saheed, Y. K., Usman, A. A., Sukat, F. D., & Abdulrahman, M. (Apr 11, 2023). A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the Internet of Things network. *Frontiers in Computer Science,* 5. https://doi.org/10.3389/fcomp.2023.997159.
[23] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Machine learning-based IoT-botnet attack detection with sequential architecture. *Sensors*, *20*(16), 4372.
[24] Tamoghna Ghosh & Shravan Kumar Belagal Math (2023). *Practical Mathematics for AI and Deep Learning (pp. 31)*. India: BPB Publications.
[25] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954-21961. https://doi.org/10.1109/ACCESS.2017.2762418.