Botnet Detection in IoT Networks: A Review of Deep Learning Techniques and Performance Metrics

Jahanvi Dubey
M.Tech Scholar
Department of Computer Science & Technology
Oriental Institute of Science and Technology
Bhopal, India

Deepshikha Patel
Head of Department
Department of Computer Science & Technology
Oriental Institute of Science and Technology
Bhopal, India

Abstract: The exponential growth of Internet of Things (IoT) networks has transformed industries and daily life but has also exposed significant security vulnerabilities, making IoT devices highly susceptible to botnet attacks. This study examines the application of deep learning techniques to effectively detect and mitigate botnet threats in IoT environments. Models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), and hybrid architectures have proven effective in analyzing complex network traffic and identifying malicious behaviors. The study evaluates the performance of these models, including hierarchical frameworks and hybrid approaches, across benchmark datasets like BoT-IoT and N-BaIoT. It also explores enhancements like feature extraction, quantization techniques, and adaptive learning strategies. While these methods show high accuracy and efficiency, challenges such as resource limitations, evolving attack strategies, and the lack of standardized datasets persist. This study emphasizes the need for innovative and scalable solutions, highlighting the potential of advanced techniques to strengthen IoT security and ensure robust botnet detection systems for evolving cyber threats.

Keywords: IoT Networks, Botnet Detection, Deep Learning, CNN, RNN, LSTM, Hybrid Models, Intrusion Detection, Network Security, Time-Series Analysis.

I.INTRODUCTION

The Internet of Things is an ensemble of objects capable of connecting and interacting with one another. This is how they can communicate with one another and exchange data without human interference. Examples include IoT-based devices: smart home appliances, wearables, industrial sensors, and medical equipment, each embedded with sensors, software, and communication technologies [1]. The IoT networks architecture can be categorized into three layers: perception or data acquisition through sensors, network or transmission using protocols such as MQTT or HTTP, and application, which involves data processing and end-user services. Despite such a network that offers automation, efficiency, and decision-making based on data, the distributed nodes decentralized, and heterogeneous nature poses complexities in management and security [2]. The way we utilize technology, and the real world will be drastically altered by the new industry known as the Internet of Things (IoT). It is anticipated that 30 billion IoT-connected devices will exist by 2025. The risk of data breaches resulting from the sometimes-insufficient processing and storage capacity of IoT devices increases with the number of connected devices [3].

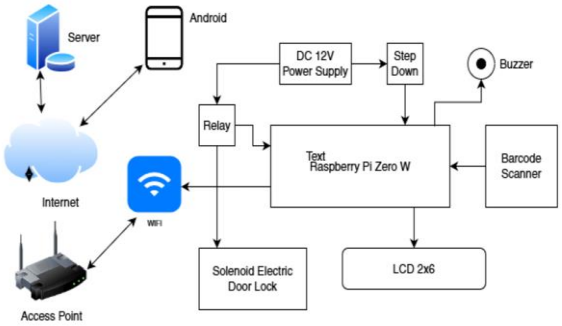

Figure 1 Block Diagram of IoT [4]

Figure 1 is of an IoT-based access control system which makes use of a Raspberry Pi Zero W in which devices such as a barcode scanner, electric door lock, and a buzzer can be sent messages over a Wi-Fi network managed via the Android interface even when it is connected to a server [4]. They represent, therefore, a totality of vulnerabilities: resource-constrained devices, non-standardized security protocols, and attack surfaces. IoT devices usually run minimally because most of them are equipped with minimal processing power, limited memory, and outdated firmware, making them an easy target for exploitation. Weak or default credentials along with weak encryption and poor network segregation all add to the problems [5]. The kind of dependence on wireless communications makes IoT networks vulnerable to attacks through eavesdropping and spoofing, as well as man-in-the-middle attacks. Hacking chances are increased on such IoT networks, hence it becomes attractive for cybercriminals, mainly for botnet attacks, since exploiting weaknesses in such networks gives them leverage over resources to take hold of such devices and develop serious cyber threats [6]. Botnet attacks are a network of controlled compromised machines for the purpose of carrying out coordinated cyberattacks, such as Distributed Denial of Service (DDoS), data theft or malware dissemination across the Internet [7]. Weak security measures and default

credentials deployed in IoT networks make it an attractive target for botnets to seize unauthorized access and control. Once infected, these IoT devices may allow malicious players to send blocking messages, siphon sensitive information, or even further facilitate more general cybercrime activities. The consequences are grave: An IoT botnet in the style of Mirai has proven possible to cause widespread power outages through an overwhelming assault on critical infrastructure. Such attacks are threats that degrade user trust and involve financial losses, posing potential dangers for public safety as well, where such activities prevail, including health and transportation sectors reliant on the augmented systems enabled through IoT [8].

II.IOT NETWORKS AND BOTNETS

IoT networks offer interlinked devices, sensors, and systems, which together intercommunicate to automate processes and data-exchange, assuming critical roles in health, transportation, and smart homes. Because they involve connected devices, IoT presents a highly vulnerable sector to botnet attacks as it mainly depends on the often resource-constrained devices with minimal security measures [9]. Such vulnerabilities are exploited by botnets when they seize several IoT devices and connect them with a command-and-control system to carry out malicious activities, such as DDoS attacks, data theft, and malware propagation. Such attacks can be hazardous as they can disrupt critical services, intrude into privacy, and undermine the very IoT ecosystems. These pose to be big threats for users at both the individual and large infrastructure level.

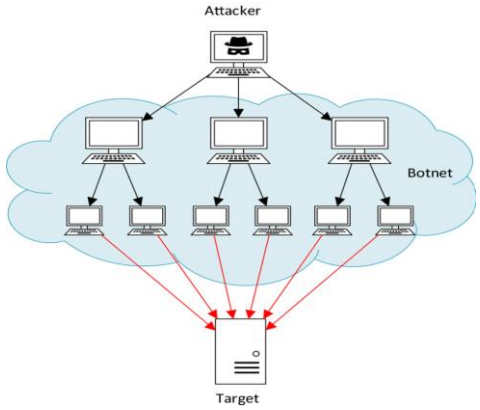

Figure 2 A diagram of a DDoS attack performed with a botnet [10]

Figure 2 illustrates a botnet attack, where an attacker controls a network of compromised devices to target and overwhelm a specific system or server [10]. In most cases, an IoT network's architecture is divided into three elementary layers: the perception layer, network layer, and application layer. The perception layer involves sensing and getting data from the physical environment through sensors and devices. The data, once collected, is then forwarded through the network layer utilizing communication protocols like Wi-Fi, Bluetooth, Zigbee, or cellular networks. The application layer processes information to gain specific services, such as smart home automation, healthcare monitoring, or industrial control [11]. IoT networks are characterized by heterogeneity and scalability; they can work in real-time with communication. Different types of devices are integrated, operate in diverse environments, and usually run on low-resource hardware that imposes demands on lightweight protocols and energy-efficient designs. Although these are some of the benefits, distributed nature and connectivity do make IoT networks intrinsically vulnerable and weak in terms of performance.

IoT networks are dynamic and heterogeneous, and therefore many types of devices can be accommodated that range from low-power sensors to strong edge computing systems. Such networks allow for seamless communication between the different devices and the types of topologies involved include mesh and star or hybrid networks depending on the application and scale. Scalability is another feature that allows IoT networks to expand with newly attached devices without loss of functionality [12]. In addition to that, IoT systems depend on both cloud computing and edge computing to make decisions in real time and analyze the data. This integration ensures that the IoT networks can process volumes of data with minimal latency.

Reliance on specific, optimized protocols for the transmission of data across such networks so that efficient and reliable communications are ensured even in resource-scarce environments is one of the most outstanding characteristics of IoT networks [13]. The protocols used here are MQTT, CoAP, Zigbee, etc. These protocols consume very low bandwidth and less power to suit the scarce computing and power resources in an IoT device. IoT networks also commonly include gateways or centralized management systems for orchestrating the communication of devices, enforcing network security, and supporting updates. Yet, this combined design of connectivity increases its attack surface and makes IoT networks more vulnerable to threats such as unauthorized access, breaches of sensitive information, and spoofing through devices. Hence, the challenge in the robust security and resilience of securing the IoT network remains significant.

III.DEEP LEARNING TECHNIQUES FOR BOTNET DETECTION

Deep learning, which has evolved after analyzing complex patterns and behaviors of large sets, can be used as an intense tool for botnet activity detection in IoT networks. In the context of classifying network traffic as normal or malicious, one has supervised learning approaches such as CNNs and RNNs. Those are actually very effective at feature extraction in network traffic data whereas the temporal patterns in sequential data are very efficiently identified by RNNs, especially LSTM networks [14]. The methods were trained on labelled datasets, which enable them to identify known botnet signatures and behaviors

with a very high degree of accuracy. However, reliance on labelled data can limit their effectiveness against previously unknown or evolving botnet threats.

These approaches of unsupervised and hybrid deep learning correct the limitations identified above, focusing instead on anomaly detection and adaptive learning [15]. Autoencoders learn to identify anomalous patterns unrelated to normal traffic patterns that would characterize botnet activities. Hybrid models combine the best of supervised and unsupervised approaches, applying labelled data to known threats, but using cluster-learning or reinforcement learning methods for detecting new anomalies. These include federated learning and edge-based deep learning, in which scalability in decentralized systems of botnet detection can be supported by processing data locally on the device, thus allowing user privacy to be preserved. Advances alone do not suffice; some of the critical challenges in the deployment of deep learning in practice for botnet detection include resource constraints, adversarial attacks, and quality dataset requirements [16].

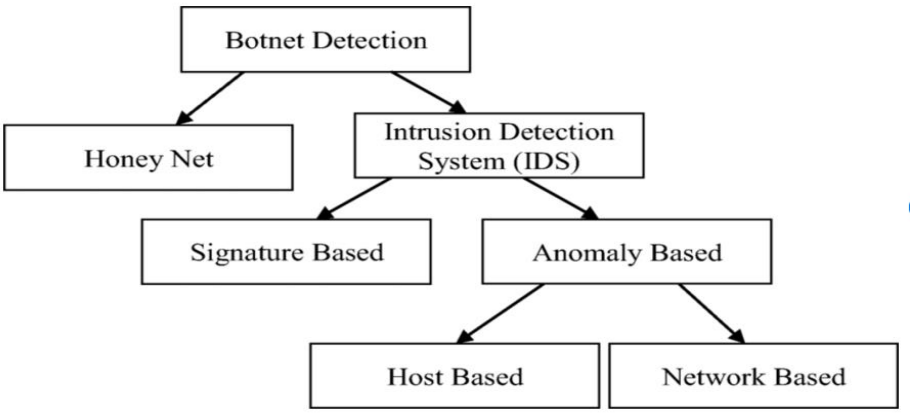

Figure 3 Various Botnet Detection Methods [17]

Figure 3 represents the botnet detection framework divided into Honeynets and Intrusion Detection Systems (IDS). Honeynets are utilized for attracting and studying botnet activities, while IDS is further split into signature-based detection where it identifies the known attack pattern and anomaly-based detection where it focuses on deviation from normal behavior [17]. Therefore, anomaly-based detection is further categorized into host-based approaches, which focus on the monitoring of one device, and network-based approaches, which monitor patterns of traffic across the network to potentially identify the threat. Such a framework will have a defined approach to battling botnet activities appropriately in IoT environments.

A. Common algorithms

Several deep learning algorithms are popular in botnet detection for IoT networks. This is because such algorithms can analyze and classify complex network traffic patterns, especially in detecting botnets whose communication patterns reflect spatially correlated structures [18]. For instance, CNNs are most efficient in extracting spatial features from structured data with network traffic matrices that may reflect static or repetitive patterns in a botnet. While recurrent neural networks have specific expertise in sequential data analysis, which can thus describe malicious activity instances over time, a far more sophisticated version of RNNs has been specifically developed to not only capture long-term dependencies in sequential data but also, more advanced long short-term memory network (LSTM) suitable for identifying complex and persistent botnet behaviors. LSTMs overcome the vanishing gradient problem that inherently arises with traditional RNNs, thereby making it possible to learn from extended sequences of network events. These algorithms are used in single configurations or in hybrid configurations and play an important role in creating robust and scalable deep learning solutions to detect and mitigate botnets in dynamic and heterogeneous environments created by IoT networks.

CNNS

IoT devices have found real significance across numerous industries, ranging from smart homes to cities, industry 4.0, and smart grids. However, the billions of deployed IoT with limited computing capabilities make them an appealing one for botnet attacks. So, to detect these threats, various approaches have been proposed; however, it is difficult to compare them since they differ in preprocessing techniques, algorithms, hyperparameters, and evaluation metrics used. This article presented a performance implementation and comparison of eight different architectures of neural networks on BoT-IoT and N-BaIoT datasets that comprise label IoT network traffic and botnet attack data. The main performance metrics are accuracy, precision, recall, and training loss to be studied [19]. These models were also computed with a throughput in an edge environment by using the NVIDIA Jetson Nano. The study further investigates the effects of 8-bit quantization on model accuracy and throughput. From the obtained

results, it was realized that with hyperparameter tuning, some of the models trained with the BoT-IoT dataset yield more than 99% accuracy, while most N-BaIoT models attain greater than 80% accuracy. However, throughput analysis does produce scenarios under which the best-performing models would not be able to scale well under the density conditions of IoT devices, even when quantization was applied.

This study addressed the severe botnet attacks on IoT devices based on three levels of their resilience, even against the improvement in the intrusion detection methods using traditional and deep learning. The study would focus on the introduction of a three-level classification framework based on the Bot-IoT dataset, regarding which the HCNN approach has been designed. The authors have considered HCNN with two configurations: a non-hierarchical network and a hierarchical network. In the hierarchical model, the features generated at the higher levels are combined with those from the descendant levels, thereby enabling an increased level of refined feature extraction and classification at subsequent layers. The network has 1,790 parameters [20]. The hierarchical network brings in an extra 942 parameters. Classification framework: It is the first-level binary classification, normal vs. attack, five classes at the second level, and 11 classes at the third level. A set of performance metrics available to evaluate the efficiency of the HCNN are Precision, Recall, F1 Score, and Accuracy. A rigorous experiment is set to compare hierarchical networks with non-hierarchical networks as well as with state-of-the-art methods. The result shows that the proposed HCNN can efficiently and effectively detect botnet attacks in the context of IoT environments more efficiently than any existing method.

The vast increase in the development of internet technology has given rise to attacks in cyberspace in the billions; especially, botnet attacks have become one of the most destructive threats since they feature diversified attack vectors and unpredictability. Rising IoT technology has been an added challenge towards the issue since many network-connected devices are being targeted and has created huge losses in all kinds of sectors [21]. This study adopts a stacked model that combines artificial neural networks, CNN, LSTM, and RNN to present a system that would detect botnets. The approach is new for detection systems and is called the ACLR model. Using UNSW-NB15 that contains nine different types of attacks, the ACLR model presents a 0.9698 high testing accuracy and gets strong K-fold cross-validation accuracy of 0.9749 at k = 5 with good generalization. Besides, it holds excellent metrics with a receiver operating characteristic area under the curve (ROC-AUC) of 0.9934 and a precision-recall area under the curve (PR-AUC) of 0.9950. Completing with the state-of-the-art models, an evaluation further confirms that ACLR effectiveness in botnet activity detection and provides a robust solution against malicious inputs of complex cyber threats to increase cybersecurity.

RNNs

IoT devices are widely used for various applications in the civilian and military domains along with environmental data collection. Due to the popularity and increased computing and processing power, IoT devices have become a high preference for malware to target specific IoT devices. This study discusses the possibility of detecting IoT malware using RNNs. A proposed method will exploit RNNs in analyzing the execution Opcodes of IoT applications on ARM-based platforms [22]. A dataset of 281 malicious and 270 benign IoT software samples is considered to train the model. After training the model, three new different LSTM configurations are tested against 100 newly handcrafted IoT malware samples that have not been exposed to the model during training. In fact, the overall highest detection accuracy of 98.18% is achieved with a 2-layer neuron setup in a 10-fold cross-validation experiment. Comparatively speaking, better performance against malware is found with LSTM-based classifiers against other machine learning classifiers, and hence, their success in the detection of IoT malware.

With the spreading of IoT rapidly, the number of cyber-attacks is also increasing rapidly. Of all these, botnet attacks emerge to be one of the greatest threats because they compromise the required networks for IoT devices to function properly. To counter this issue, the authors proposed the GA-HDLAD system here that intends to enhance IoT security by botnet detection. This solution works past the challenge of highly dimensional data where feature selection is performed by using a genetic algorithm, and the approach uses a hybrid deep learning technique that combines Recurrent Neural Networks (RNNs), FETs, and attention mechanisms with complex botnet patterns [23]. Using FETs together with RNNs for spatial feature extraction as well as for capturing temporal dependencies ensures robust anomaly detection. Further optimization of the hybrid model's hyperparameters relies on simulated annealing (SA). As a baseline, some experimental evaluations were carried out using a benchmark botnet dataset. The system is superior in performance compared to the existing state-of-the-art methods, and it potentially can identify and mitigate botnet threats as effectively as possible in IoT environments.

An offshoot of the deep changes IoT has brought about in human relations with the environment is the need for richer security strategies. Having witnessed such a radical change in human interactions with the environment, tailored security strategies over and above traditional corporate networks are needed. While measures such as anti-malware software, firewalls, authentication protocols, and encryption techniques remain established and offer some defense, they do not appreciate the sophisticated nature of threats directed specifically at them from IoT. To handle such challenges, the proposed study will suggest an intrusion detection system suitable for the IoT environment with the help of various models of deep learning: DNN, CNN, and RNN. Each model has three customized and fine-tuned

variants: DNN1, DNN2, DNN3; CNN1, CNN2, CNN3; RNN1, RNN2, RNN3, which would be tested according to their degree of intrusion-behavior differentiation from benign network traffic. One of the most important lessons is to properly calibrate the accuracy curves of the training set and validation. Overfitting and reliability increase will be out of the question in all the tested models. In all tested models, it was RNN1 that peaked with an accuracy of 98.61%, precision of 98.55%, recall of 98.61%, and an F1-score of 98.57%, far surpassing other architectures and benchmark studies [24]. This study contributes to further development of intrusion detection in IoT networks by having a thorough review of deep learning models and grounds for further improvement towards the strengthening of intrusion detection in the dynamic environments of the IoT.

LSTM

An unprecedented growth of Internet of Things, with almost countless integration of different devices and technologies, has raised the attack surface nearly unproportionally to its growth and exposure of vulnerabilities in the industries driven mainly by growth rather than security. The traditional defensive mechanisms do a poor job in the high accuracy detection of both known as well as novel attacks, thus making the growing ecosystem more challenging for innovative approaches. This study proposes a novel method of data preprocessing for sequential networks to make decisions in real time by applying time series analysis on the Bot-IoT dataset, based on realistic IoT network data. A novel feature called Time Difference is proposed to calculate the gap in time between messages exchanged between the source and destination [25]. Using such preprocessing, a simple LSTM network achieves as much as 97% accuracy. The 10 most important features to be used for IDS analysis shall be derived from the LSTM network, thereby giving a basis to apply advanced time series analysis methods on the Intrusion Detection System datasets in the future. Such an approach will be better than any of the existing available multiclass methodologies, thereby suggesting a very robust solution toward upgrading IoT security.

In today's world, dominated by IoT devices, protection of interconnected devices against botnets has emerged as a critical concern. This study tries to outline an advanced hybrid deep learning model using LSTM Autoencoders and Multilayer Perceptron's for effectively discovering botnets in IoT networks. The strengths of the former are fused with those of the latter to enable it to analyze sequential data and identify complex patterns; hence, its use is highly effective in identifying intricate botnet activities [26]. The proposed model has been evaluated under very strict conditions on two vast IoT traffic datasets, which are N-BAIoT2018 and UNSW-NB15. In these experiments, the detection accuracy reported were impressive at 99.77% and 99.67%. Such outstanding outcomes clearly point out that this model can greatly outperform the existing botnet detection schemes.

The Internet of Things (IoT) is expanding at a rapid pace as the transforming communication technology, but its vulnerability has made it a target for many cyberattacks with botnet attacks constituting one of them. An effective classification of botnet traffic is a critical requirement in ensuring that IoT networks are secure. This explanation informs this study to make use of the DL strengths to propose an LSTM model for the classification of botnet traffic in IoT networks [27]. A performance evaluation was conducted and completed on two benchmark datasets for network intrusion, namely CICIDS-2017 and N-BaIoT. For the CICIDS-2017 dataset, the model classified with 99.76% accuracy in the Wednesday data, and, for the entire data set, 99.38% accuracy in classification was found. The model was then tested using MCC, which resulted in scores of 99.52% and 98.76% on the Wednesday data and the complete dataset, respectively. On the N-BaIoT dataset, the proposed model has established a better result than various previous approaches with an accuracy of 99.98% and an MCC value of 99.95%. The results indicate that the model is effective and superior in detecting botnet traffic within IoT environments.

Table 1 Comparative Analysis of Deep Learning Approaches for Botnet Detection in IoT Environments

Reference	Model	Key Findings	Techniques	Performance Metrics
[19]	Various neural network architectures	Evaluated 8 NN architectures on BoT-IoT and N-BaIoT datasets; hyperparameter tuning achieved >99% accuracy on BoT-IoT; N-BaIoT models >80% accuracy.	Neural Networks (NNs), 8-bit quantization, NVIDIA Jetson Nano for throughput	Accuracy: >99% (BoT-IoT), >80% (N-BaIoT); Quantization impacts on scaling in IoT devices.
[20]	HCNN (Hierarchical CNN)	Proposed HCNN with three levels of classification; achieved higher efficiency than non-hierarchical methods.	Hierarchical CNN, feature refinement at layers, three-level classification	Accuracy, Precision, Recall, F1 Score; Outperformed state-of-the-art methods.
[21]	ACLR (ANN, CNN, LSTM, RNN Stacked Model)	Detected botnet activity with 96.98% accuracy; strong K-fold CV accuracy of 97.49% and high ROC-AUC (0.9934) and PR-AUC (0.9950).	Stacked model combining ANN, CNN, LSTM, RNN; Feature extraction, ROC-AUC	Accuracy: 96.98%; K-fold CV: 97.49%; ROC-AUC: 0.9934; PR-AUC: 0.9950.

[22]	RNN for IoT malware detection	Detected IoT malware using RNN; achieved 98.18% detection accuracy using a 2-layer neuron setup.	RNN, analyzing OpCodes of IoT applications on ARM platforms	Accuracy: 98.18%; Tested against handcrafted malware samples; 10-fold CV.
[23]	GA-HDLAD (Hybrid DL with Genetic Algorithm)	Enhanced IoT security by botnet detection using RNNs, FETs, attention mechanisms; optimized with simulated annealing; superior performance over state-of-the-art methods.	Hybrid DL (RNN, FETs), attention mechanisms, genetic algorithm for feature selection, simulated annealing for optimization	Outperformed state-of-the-art; Effective anomaly detection in IoT environments.
[24]	DNN, CNN, RNN Variants	RNN1 variant achieved top accuracy of 98.61%, precision of 98.55%, recall of 98.61%, and F1-score of 98.57%, surpassing DNN and CNN architectures.	Customized DNN, CNN, RNN models; Variant-based testing; Fine-tuned training	Accuracy: 98.61%; Precision: 98.55%; Recall: 98.61%; F1-Score: 98.57%.
[25]	LSTM with Time Series Analysis	Proposed a novel feature "Time Difference" for real-time IoT decisions; achieved 97% accuracy on Bot-IoT dataset; derived 10 key features for future IDS analysis.	Time series analysis, LSTM, Time Difference feature	Accuracy: 97%; Key features derived for IDS datasets; Robust solution for multiclass IoT security methodologies.
[26]	LSTM Autoencoders + MLP (Hybrid Model)	Combined LSTM Autoencoders and Multilayer Perceptrons; achieved 99.77% and 99.67% accuracy on N-BAIoT2018 and UNSW-NB15 datasets, respectively.	Hybrid model (LSTM Autoencoders, MLP), sequential data analysis, pattern detection	Accuracy: 99.77% (N-BAIoT2018); 99.67% (UNSW-NB15); Effective detection of intricate botnet activities.
[27]	LSTM for botnet traffic classification	Achieved 99.76% accuracy on Wednesday data of CICIDS-2017 and 99.38% on the full dataset; MCC scores of 99.52% and 98.76%, respectively; 99.98% accuracy on N-BaIoT.	LSTM, Matthew Correlation Coefficient (MCC)	Accuracy: 99.76% (CICIDS-2017 Wednesday); 99.38% (CICIDS-2017 full); MCC: 99.95% (N-BaIoT).

B. Hybrid Models

Overview of Hybrid Models in Botnet Detection

Deep learning for botnet detection often considers combining several approaches to handle the weaknesses of stand-alone ones. The intention is to use a combination of all the techniques-be it supervised, unsupervised, or reinforcement learning-of putting everything together into one big framework. Supervised learning models are useful when aiming for known botnet signatures since the models get trained on datasets that have labels and classify network traffic according to defined patterns of malicious activity [28]. However, these models break down when new attacks or strategies of attacks significantly differ from their training data. Hybrid models must overcome this weakness of the traditional supervised machine learning approach by embracing unsupervised learning techniques that are not constrained by the need for any labeled data and can highlight anomalies based on the deviations in normal network behavior. Thus, for unsupervised learning, clustering methods or autoencoders may identify novel patterns of traffic that could indicate new botnet activities.

Thus, through the implementation of these approaches, hybrid models can address the known as well as unknown threats. Reinforcement learning can be further used in hybrid systems that enable adaptive learning with real-time feedback [29]. The model can learn from this and continuously adapt its detection capabilities. This feature is particularly desirable in an IoT environment since botnets often change to exploit newly identified vulnerabilities on different devices. Hybrid models can also leverage multi-layered architectures, wherein the first layer could be lightweight unsupervised anomaly detection algorithms that flag suspicious activity and computationally intensive supervised models that confirm if the flagged activity is malicious. The layered approach aids in optimized resource usage, which is one reason why hybrid models are suitable for the heterogeneous, resource-constrained nature of IoT networks while being robust and comprehensive in botnet detection.

Implementation in IoT Networks

The multi-layered hybrid models often combine layers to achieve maximum efficiency: for example, the initial lightweight anomaly detection system flags potentially malicious activities only based on deviations in patterns of traffic, followed by more computationally intensive supervised models, such as Convolutional Neural Networks or Long Short-Term Memory networks, to determine whether these activities correspond to known botnet activity [30]. In addition, reinforcement learning can be used to evolve a model over time and thus, such a model can learn and respond dynamically to new attack strategies. Hybrid models that integrate all the methodologies give better scalability and adaptability to suit real-time detection conditions of resource-constrained IoT environments.

IV.PERFORMANCE METRICS FOR EVALUATION

Performance metrics are integral aspects to assess the efficiency and reliability of deep learning models for botnet detection. They provide a normalized means through which the accuracy of detection is measured as well as reduced error. Some of the common metrics deployed are accuracy, which essentially measures the overall proportion of correctly classified instances in terms of both malicious and normal traffic, and precision, which calculates the proportion of correctly identified malicious activities out of all the instances flagged as malicious. Another important metric is recall or sensitivity, which essentially indicates the ability of the system to identify all the actual malicious activities present in the dataset [31]. The F1-score is a harmonic mean of precision and recall, thus offering a balanced evaluation, especially when datasets are imbalanced or false positives and false negatives have significant consequences.

Apart from these basic measures, some targeted measures are mostly used to make the specific chokepoints of botnets in IoT environments smooth. The false positive rate measures how often the normal activities are mistakenly classified as malicious, which can trigger inappropriate disruption. On the other hand, the false negative rate measures how many botnet activities were missed because it is system security that is compromised when these are overlooked. The ROC curve and area under the curve (AUC) is a graphical as well as numerical interpretation of true and false positive rates of trade-off. Moreover, the available resources for IoT devices are limited; thus, the metrics like latency, energy efficiency, and memory utilization are significant in an IoT network. This can be combined together to critically evaluate and optimize the detection system of botnets in terms of both performance as well as efficiency in resource usage.

V.CHALLENGES

The IoT networks comprise billions of low-computational and memory resource-possessing devices, which makes even the more sophisticated methods of botnet detection challenging in deployment. Most models of deep learning require high processing power; indeed, not all them are feasible to be implemented on low-lightweight IoT devices and remain a challenge in large dense networks with respect to scalability performance.

Botnets evolve continuously, lately incorporating new means of evasion. The environment hosting the botnets is heterogeneous owing to the multitude of different types of devices and applications from smart appliances to industrial sensors. Varying vulnerabilities in the system lead to this threat space becoming vulnerable to exploitation by these botnets. Traditional and static methods for detection are not easily adaptable to these dynamic and complex attack patterns.

The amount of sensitive data produced by IoT networks is very high, and centralized detection methods raise privacy concerns. In addition, there is no standardized dataset, protocol, or even metrics for evaluation, which makes comparison as well as development of a detection system very challenging. These need to be overcome with the use of privacy-preserving techniques, unified datasets, and agreed benchmarks to leverage robust botnet detection in IoT environments.

VI.CONCLUSION

This study highlights the use of deep learning techniques in the mitigation of current challenges in botnet detection against the deployments of IoT networks. What makes IoT so transformative within industries and daily life is that they are rightly considered to be really vulnerable for their resource constraint as well as their wide deployments. This actually gives them the perfect target for sophisticated botnet attacks. Advanced applications in deep learning models have been proven to be effective-including CNNs, RNNs, LSTMs, and hybrids-to analyze complex network traffic patterns and to flag suspicious activities at very high accuracy levels. Another related innovation is hierarchical classification frameworks and the hybrid deep learning models, along with feature extraction and quantization, which enhance their performance and adaptability while addressing effectiveness against evolving threats. However, areas of pressing and long-lasting issues identified include scalability of detection systems in dense IoT networks, fast-changing nature of attack vectors, and absence of standardized datasets, protocols, and metrics for assessment of these systems. Such problems need lightweight and resilient models, with features to process efficiently on resource-constrained IoT devices. Advanced techniques like time-series analysis, attention mechanisms, and reinforcement learning provide a way toward finding adaptive, real-time solutions handling

security concerns as well as user privacy. Conclusion: This is a revolutionary step to introduce deep learning capabilities into botnet detection systems to protect the IoT ecosystems. Continuous innovation and collaborative efforts to set up standardized benchmarks and privacy-preserving techniques will be very important in making intrusion detection systems more effective and resilient for the long-term security of IoT networks against evolving cyber threats.

Conflict of Interest: The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.

References

1. Alsharif, M. H., Kelechi, A. H., Jahid, A., Kannadasan, R., Singla, M. K., Gupta, J., and Geem, Z. W. (2024). A comprehensive survey of energy-efficient computing enables sustainable massive IoT networks. Alexandria Engineering Journal, 91, 12-29. https://doi.org/10.1016/j.aej.2024.01.067
2. Khazane, H., Ridouani, M., Salahdine, F., & Kaabouch, N. (2024). A holistic review of machine learning adversarial attacks in IoT networks. Future Internet, 16(1), 32. https://doi.org/10.3390/fi16010032
3. Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and cyber-physical systems, 4, 110-128. https://doi.org/10.1016/j.iotcps.2023.09.003
4. Atmaja, Ardian & Setia, Luthfiyah & Fajar, Muhammad & Ismar, MH. (2022). Low Cost IoT Based Home Smart Locker to Receive Online Shopping Packages. Andalasian International Journal of Applied Science, Engineering and Technology. 2. 126-132. 10.25077/aijaset. v2i03.57.
5. Alomari, A., & Kumar, S. A. (2024). Securing IoT Systems in a Post-Quantum Environment: Vulnerabilities, Attacks, and Possible Solutions. Internet of Things, 101132. https://doi.org/10.1016/j.iot.2024.101132
6. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors, 24(2), 708. https://doi.org/10.3390/s24020708
7. Sharma, S., Kumar, V., & Dutta, K. (2024). Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review. Internet of Things and Cyber-Physical Systems. https://doi.org/10.1016/j.iotcps.2024.01.003
8. Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., ... & Pathan, M. S. (2023). Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. Journal of King Saud University-Computer and Information Sciences, 101820. https://doi.org/10.1016/j.jksuci.2023.101820
9. Haque, S., El-Moussa, F., Komninos, N., & Muttukrishnan, R. (2023). A systematic review of data-driven attack detection trends in IoT. Sensors, 23(16), 7191. https://doi.org/10.3390/s23167191
10. Najafimehr, Mohammad & Zarifzadeh, Sajjad & Mostafavi, Seyedakbar. (2022). A Hybrid Machine Learning Approach for Detecting Unprecedented DDoS Attacks. The Journal of Supercomputing. 78. 10.1007/s11227-021-04253-x.
11. Burhan, M., Alam, H., Arsalan, A., Rehman, R. A., Anwar, M., Faheem, M., & Ashraf, M. W. (2023). A comprehensive survey on the cooperation of fog computing paradigm-based IoT applications: layered architecture, real-time security issues, and solutions. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3294479
12. Kanellopoulos, D., Sharma, V. K., Panagiotakopoulos, T., & Kameas, A. (2023). Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives. Electronics, 12(11), 2490. https://doi.org/10.3390/electronics12112490
13. Aneja, N., Aneja, S., & Bhargava, B. (2023). AI-Enabled Learning Architecture Using Network Traffic Traces over IoT Network: A Comprehensive Review. Wireless Communications and Mobile Computing, 2023(1), 8658278. https://doi.org/10.1155/2023/8658278
14. Ghaffari, A., Jelodari, N., pouralish, S., derakhshanfard, N., & Arasteh, B. (2024). Securing internet of things using machine and deep learning methods: a survey. Cluster Computing, 1-25. https://doi.org/10.1007/s10586-024-04509-0
15. Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends. Sensors, 24(6), 1968. https://doi.org/10.3390/s24061968
16. Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., ... & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. Journal of King Saud University-Computer and Information Sciences, 102164. https://doi.org/10.1016/j.jksuci.2024.102164
17. Subhashini, R. (2020). Mimicking attack by botnet and detection at gateway. Peer-to-Peer Networking and Applications. 13. 10.1007/s12083-019-00854-9.
18. Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Techniques and optimization algorithms in machine learning: A review. Applied Machine Learning and Deep Learning: Architectures and Techniques, 39-58.
19. Guimarães, L. C., & Couto, R. S. (2024). A Performance Evaluation of Neural Networks for Botnet Detection in the Internet of Things. Journal of Network and Systems Management, 32(4), 98. https://doi.org/10.1007/s10922-024-09875-z
20. Negera, W. G., Schwenker, F., Feyisa, D. W., Debelee, T. G., & Melaku, H. M. (2024). Hierarchical Classification of Botnet Using Lightweight CNN. Applied Sciences, 14(10), 3966. https://doi.org/10.3390/app14103966

21. Ali, M., Shahroz, M., Mushtaq, M. F., Alfarhood, S., Safran, M., & Ashraf, I. (2024). Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3376400
22. Alsadhan, A. A., Al-Atawi, A. A., Jameel, A., Zada, I., & Nguyen, T. N. (2024). Malware Attacks Detection in IoT Using Recurrent Neural Network (RNN). Intelligent Automation & Soft Computing, 39(2). 10.32604/iasc.2023.041130
23. Mutambik, I. (2024). Enhancing IoT Security Using GA-HDLAD: A Hybrid Deep Learning Approach for Anomaly Detection. Applied Sciences, 14(21), 9848. https://doi.org/10.3390/app14219848
24. Abbas, S., Alsubai, S., Ojo, S., Sampedro, G. A., Almadhor, A., Hejaili, A. A., & Bouazzi, I. (2024). An efficient deep recurrent neural network for detection of cyberattacks in realistic IoT environment. The Journal of Supercomputing, 1-19. https://doi.org/10.1007/s11227-024-05993-2
25. Sadeghpour, S., Zareen, F., & Johnson, W. A. (2024, September). From Data to Defense: Real-Time Detection of Botnets in IoT Using LSTM Networks. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 605-611). IEEE. https://doi.org/10.1109/CSR61664.2024.10679488
26. Ali, S., Ghazal, R., Qadeer, N., Saidani, O., Alhayan, F., Masood, A., ... & Gupta, D. (2024). A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks. Alexandria Engineering Journal, 103, 88-97. https://doi.org/10.1016/j.aej.2024.05.113
27. Clinton, U. B., Hoque, N., & Singh, K. R. (2023, July). Botnet-based IoT Network Attacks Identification using LSTM. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-10). IEEE. https://doi.org/10.1109/ICCCNT56998.2023.10307716
28. Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. Sensors, 24(11), 3571. https://doi.org/10.3390/s24113571
29. Abreu, R., Simão, E., Serôdio, C., Branco, F., & Valente, A. (2024). Enhancing IoT Security in Vehicles: A Comprehensive Review of AI-Driven Solutions for Cyber-Threat Detection. AI, 5(4), 2279-2299. https://doi.org/10.3390/ai5040112
30. Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., ... & Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity, 7(1), 20. https://doi.org/10.1186/s42400-024-00212-0
31. Meesters, K., & Buonsenso, D. (2024). Antimicrobial stewardship in pediatric emergency medicine: a narrative exploration of antibiotic overprescribing, stewardship interventions, and performance metrics. Children, 11(3), 276. https://doi.org/10.3390/children11030276