International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 6, June 2026)

Review on Deep Learning Approach for Botnet Attacks Detection in IoT Environment

Shruti Sahu[1], Dr. Devendra Singh Rathore[2], Dr. Vivek Richhariya[3]
[1]Research Scholar, Department of CSE, Lakshmi Narain College of Technology, Bhopal, India
[2]Associate Professor, Department of CSE, Lakshmi Narain College of Technology, Bhopal, India
[3]Professor, Department of CSE, Lakshmi Narain College of Technology, Bhopal, India

***Abstract*— The increasing integration of Internet of Things (IoT) devices into various domains has made networks more vulnerable to sophisticated cyber threats, particularly botnet attacks. These attacks exploit the limited security mechanisms of IoT devices to form large-scale malicious networks capable of launching harmful operations. This review explores the application of deep learning approaches for the detection and mitigation of botnet attacks in IoT environments. It highlights various deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks, examining their effectiveness in identifying complex patterns and anomalies in network traffic. The study aims to provide insights into current methodologies, datasets, evaluation metrics, and challenges, while outlining future directions for improving detection accuracy and real-time response capabilities in IoT security frameworks.**

***Keywords*—DL, IOT, Botnet, CNN, RNN, LSTM.**

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has transformed modern life by connecting billions of smart devices such as sensors, cameras, smart appliances, wearable technologies, and industrial controllers. These interconnected devices contribute to smarter homes, efficient industries, and real-time healthcare, among numerous other applications. However, this unprecedented growth has also introduced significant security vulnerabilities. Unlike traditional computing systems, many IoT devices operate with limited computational resources and often lack robust security mechanisms, making them easy targets for cyber attackers. Among the various forms of cyber threats, botnet attacks have emerged as one of the most severe and pervasive threats to IoT infrastructures.

A botnet refers to a network of compromised devices—often called "bots" or "zombies"—that are controlled remotely by a malicious actor, commonly known as a "botmaster." Once a device is infected with botnet malware, it becomes part of a larger network that can be orchestrated to perform harmful activities such as distributed denial-of-service (DDoS) attacks, spam distribution, data theft, and unauthorized access to critical services. Botnets can grow rapidly and autonomously, exploiting the heterogeneity and often poor security of IoT devices. High-profile botnet attacks like Mirai have already demonstrated the potential devastation that can be caused by leveraging IoT-based botnets to disrupt large segments of the internet.

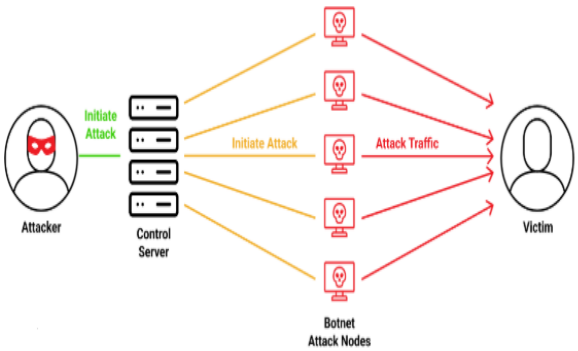

Figure 1: Botnet Attack

Detecting botnet attacks in IoT environments presents numerous challenges. Traditional detection

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 6, June 2026)

techniques that rely on rule-based intrusion detection systems (IDS), signature matching, or blacklisting often fail to identify novel or evolving threats. IoT networks are typically characterized by dynamic topologies, diverse device types, low processing power, and limited storage, which restrict the deployment of conventional security solutions. Furthermore, botnets often utilize stealthy and encrypted communication channels, making it difficult to detect their activities using traditional methods. The need for intelligent, adaptable, and scalable detection techniques has, therefore, become paramount.

In recent years, deep learning has gained prominence as a powerful tool for detecting complex cyber threats due to its ability to model non-linear relationships and recognize subtle patterns in large volumes of data. Deep learning algorithms such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders, and Deep Belief Networks (DBN) have been applied successfully to various cybersecurity tasks, including intrusion detection and anomaly detection. These models can learn from raw network traffic data and extract meaningful features automatically, enabling more accurate and efficient botnet detection compared to traditional methods. Moreover, deep learning models can adapt to evolving attack patterns through continuous learning, making them suitable for real-time and dynamic IoT environments.

This review aims to explore the landscape of deep learning-based botnet detection in IoT environments. It discusses the different architectures, datasets, evaluation metrics, and comparative performance of existing models. The review also highlights key challenges such as high false-positive rates, model interpretability, data imbalance, and computational limitations. In addition, it identifies future research directions for improving detection accuracy, reducing latency, and enhancing the scalability of deep learning-based systems. By providing a comprehensive analysis of current approaches and ongoing research, this review contributes to the development of more robust and intelligent security solutions to safeguard the ever-expanding IoT ecosystem from botnet attacks.

II. LITERATURE SURVEY

A. K. Kumar et al. [1] proposed an Enhanced Hybrid Deep Learning Approach for detecting botnet attacks in IoT environments. The model integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to leverage both spatial and temporal patterns in IoT network traffic. The authors emphasize the importance of real-time detection and present a hybrid model that significantly outperforms traditional machine learning methods in terms of detection accuracy and false positive rates. Evaluated on multiple IoT-specific datasets, the model demonstrates robust generalization across various botnet behaviors. Additionally, the study highlights the need for adaptable models that can be updated frequently to cope with evolving threats. The hybrid architecture provides a balanced trade-off between detection accuracy and computational efficiency, making it suitable for lightweight IoT devices.

M. Alshehri et al. [2] introduced SkipGateNet, a novel lightweight CNN-LSTM hybrid model designed with learnable skip connections to improve the efficiency of botnet attack detection in IoT networks. The learnable skip connections allow the model to dynamically select relevant features across layers, reducing redundant computation while maintaining high accuracy. The paper demonstrates that SkipGateNet achieves better performance in terms of F1-score and processing time compared to conventional deep learning models. The architecture is optimized for resource-constrained IoT devices and shows significant promise for real-time botnet mitigation. Their evaluation on benchmark datasets validates its practical applicability in real-world deployments. Moreover, the model's ability to scale across diverse IoT environments makes it a competitive solution for future botnet detection systems.

M. Al-Fawa'reh et al. [3] presented MalbotDRL, a novel framework utilizing Deep Reinforcement Learning (DRL) for detecting malware botnets in IoT networks. The key innovation lies in treating botnet detection as a sequential decision-making process,

allowing the system to learn optimal detection policies over time. The use of DRL helps in dynamically adapting to new attack patterns, thus offering enhanced performance compared to static models. Experimental results show that MalbotDRL achieves superior detection rates with lower latency and false alarms. The paper also discusses the importance of simulation environments in training DRL agents for cybersecurity applications. This adaptive and intelligent approach contributes significantly to enhancing the resilience of IoT infrastructures against sophisticated and evolving botnet threats.

R. Kalakoti et al. [4] explored the use of Explainable Artificial Intelligence (XAI) for improving IoT botnet detection systems. The authors argue that while deep learning models are powerful, their "black-box" nature limits user trust and interpretability. The study proposes quantitative metrics for evaluating the explainability of different XAI methods applied to botnet detection. Results reveal that integrating explainability does not significantly compromise accuracy, and instead enhances user comprehension and decision-making. The paper emphasizes that future security frameworks must combine both detection accuracy and explainability to be practically deployable. By applying models such as SHAP and LIME, the research offers transparency into how specific features influence botnet classification decisions. This work lays the groundwork for integrating ethical AI in cybersecurity solutions.

X. Yan et al. [5] proposed a domain embedding model combined with smart blockchain infrastructure to detect botnet activity in IoT networks. This hybrid approach enhances security through decentralized trust while using domain embeddings to represent malicious domain patterns. The model significantly reduces false positives and enhances resilience against domain-generation algorithm (DGA)-based botnets. The integration with blockchain ensures tamper-proof logging and trust verification among IoT nodes. The paper illustrates how combining deep learning with blockchain can improve both security and transparency in IoT ecosystems. Moreover, the system's modular design allows for easy integration into existing IoT infrastructures. This study highlights an innovative path toward combining multiple emerging technologies to tackle the complex problem of botnet attacks.

S. Saravanan et al., [6] developed an adaptive scalable data pipeline for multiclass classification of attacks, including botnets, in large-scale IoT networks. Their solution addresses challenges associated with massive data volumes, real-time processing, and heterogeneous device behavior. The architecture employs a layered deep learning framework that includes pre-processing, feature extraction, and classification stages. Their results show high scalability, with real-time performance even in datasets exceeding millions of packets. The study also explores methods for handling data imbalance and missing values in IoT telemetry. Their work demonstrates how intelligent pipeline design can significantly enhance the deployment feasibility of deep learning-based intrusion detection in real-world environments. The proposed model is ideal for centralized security centers overseeing distributed IoT systems.

P.V. Dinh et al. [7] proposed a Constrained Twin Variational Autoencoder (CTVAE) for detecting intrusions in IoT systems, with a particular focus on botnets. This method captures the underlying latent distribution of normal and abnormal traffic and uses a twin-architecture to differentiate between them. The inclusion of constraint mechanisms enhances feature disentanglement and prevents overfitting. The study shows that CTVAE outperforms traditional autoencoders and deep neural networks on benchmark datasets. The method is also shown to be effective in zero-day attack scenarios, a critical need in dynamic IoT settings. The authors suggest that such generative models can serve as foundational modules in future anomaly-based IoT security systems. Their research provides new avenues for leveraging unsupervised deep learning in threat detection.

J. Kabdjou and N. Shinomiya [8] tackled botnet detection through a cyber-deception based architecture

deployed in a Multi-access Edge Computing (MEC) environment. This architecture uses deception techniques such as honeypots and fake vulnerabilities to lure botnets into exposing themselves. A deep learning-based classifier is then used to analyze the malicious activity and detect DDoS attacks on HTTPS traffic. This method also improves Quality of Service (QoS) by reducing the computational burden on central servers. The paper presents empirical evidence showing the effectiveness of combining deception with intelligent analytics in edge environments. It emphasizes the potential of proactive defense techniques rather than purely reactive detection methods. Their work is especially relevant in latency-sensitive applications such as smart healthcare and industrial automation.

A.A. Mohammed and A.A. Ibrahim [9] investigated machine learning-based malware detection in Ad-hoc e-Government Networks, which are increasingly vulnerable to botnet attacks. Their model employs ensemble learning and decision-level fusion to detect malicious activity from heterogeneous traffic sources. Although the study is not exclusively focused on IoT, its methodology is transferable to IoT-based smart governance systems. Results show improved accuracy and precision when compared to traditional single classifiers. The researchers stress the importance of customized training datasets for domain-specific botnet behaviors. The study also highlights potential gaps in governmental cybersecurity policies related to real-time botnet mitigation. This work underlines the necessity of intelligent detection mechanisms in mission-critical e-Government infrastructures.

T. Hasan et al. [10] presented a hybrid deep learning framework specifically tailored for Industrial IoT (IIoT) environments. The model combines CNNs and Bidirectional LSTM (BiLSTM) networks to handle high-speed and large-volume industrial data. Their focus is on securing time-sensitive control systems against botnet threats, which can cripple production lines and cause massive economic losses. Experimental evaluation shows high detection accuracy, low latency, and better generalization to unseen attack types. The authors also discuss integration with industrial protocols and sensor networks, showing adaptability to specific IIoT configurations. Their work serves as a blueprint for designing resilient cyber-physical systems in manufacturing and smart grid applications.

P. Saxena and R.B. Patel [11] proposed an efficient hybrid model that blends Decision Tree and Gradient Boosting techniques for botnet detection in IoT. Their approach uses a lightweight feature selection module to reduce data dimensionality and optimize classifier performance. The model is tested on widely used public datasets such as Bot-IoT and CICIDS2017, where it demonstrates high classification accuracy and reduced training time. The study emphasizes the significance of balancing model complexity with real-time feasibility in IoT devices. Additionally, the model is modular and can be adapted for various cyber threats beyond botnets. Their findings reinforce the relevance of hybrid machine learning approaches in low-resource environments.

F. Sattari et al. [12] presented a hybrid deep learning model for detecting bottlenecks and botnet behaviors in IoT infrastructures. The model integrates CNN for feature extraction and Deep Neural Networks (DNN) for final classification. The system is designed to analyze traffic flow irregularities that may indicate the presence of coordinated botnet activities. Their evaluation shows impressive detection rates with minimal processing overhead, making it suitable for deployment in resource-constrained IoT nodes. The paper also investigates network bottlenecks introduced by botnets and provides insights into traffic-level optimizations. Their approach not only aids in early botnet detection but also contributes to overall network efficiency and stability.

III. CHALLENGES

1. Resource Constraints in IoT Devices

Most IoT devices have limited computational power, memory, and battery life. Deep learning models, especially complex ones like CNNs or LSTMs, require significant resources

for training and inference. Deploying these models on lightweight IoT devices without compromising performance remains a major challenge.

2. High Volume and Variety of Network Traffic

IoT environments generate massive volumes of heterogeneous data in real time. The dynamic and diverse nature of traffic makes it difficult for a single model to capture all attack patterns effectively. Designing models that scale with traffic volume while maintaining accuracy is still a bottleneck.

3. Evolving and Sophisticated Botnet Techniques

Botnet attacks are constantly evolving with advanced obfuscation techniques, such as domain generation algorithms (DGAs), encrypted command and control (C&C) communication, and polymorphic malware. Deep learning models trained on historical data may fail to detect new or zero-day attack variants.

4. Data Labeling and Quality Issues

Supervised deep learning methods require large volumes of accurately labeled data for effective training. However, acquiring labeled datasets for botnet attacks is labor-intensive and often unfeasible due to privacy issues, especially in real-world IoT environments.

5. Imbalanced Datasets

Botnet attack traffic typically represents a small fraction of the total network activity, leading to highly imbalanced datasets. This imbalance causes models to be biased towards normal traffic, resulting in high false negatives and reduced attack detection rates.

6. Real-Time Detection Requirements

IoT systems often require real-time detection to respond instantly to botnet attacks. Deep learning models, especially those with large architectures, may introduce latency, making them unsuitable for time-sensitive applications like industrial control systems or healthcare.

7. Lack of Standardized Benchmark Datasets

Many researchers use custom or simulated datasets, making it difficult to compare results across studies. The absence of standardized, publicly available, real-world datasets hinders the development and benchmarking of deep learning models for botnet detection.

8. Model Interpretability and Explainability

Deep learning models are often criticized as "black boxes." Security analysts and system administrators require explanations of model decisions, especially in critical domains like IoT. The lack of transparency affects trust, debugging, and compliance with data protection regulations.

IV. CONCLUSION

The detecting botnet attacks in IoT environments using deep learning approaches presents a promising yet complex solution to securing interconnected devices. While deep learning models such as CNNs, LSTMs, and hybrid architectures have shown high accuracy in identifying malicious patterns, their deployment is often hindered by challenges like resource limitations, data imbalance, and evolving attack techniques. Addressing issues related to real-time processing, explainability, and generalizability is crucial for practical implementation. With continued research and optimization, deep learning can play a vital role in building intelligent, adaptive, and scalable security solutions to protect IoT ecosystems from increasingly sophisticated botnet threats.

REFERENCES

1. A. K. Kumar *et al*., "Enhanced Hybrid Deep Learning Approach for Botnet Attacks Detection in IoT Environment," *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/ICSPIS63676.2024.10812621.
2. M. Alshehri J. Ahmad, S. Almakdi, M. Qathrady, Y. Ghadi and w. Buchanan, "SkipGateNet: A Lightweight CNN-LSTM hybrid model with learnable skip connections for efficient botnet attack detection in IoT," IEEE Access, vol. 12, pp. 35521–35538, March 2024 https://doi.org/10.1109/access 3371992.
3. M. Al-Fawa'reh, J. Abu-Khalaf, P. Szewczyk, and J.J Kang, MalbotDRL: Malware botnet detection using deep reinforcement learning in IOT Networks. IEEE Internet of Things Journal, vol. 11, no. 6, pp. 9610–9629, October 2023, https://doi.org/10.1109/jiot.2023.3324053
4. R. Kalakoti, H. Bahsi, and S. No mm (2024). Improving IOT security with explainable AI: Quantitative evaluation of explainability for IOT botnet detection. IEEE Internet of Things Journal, vol. 11, no. 10, pp. 18237–18254. January 2024, https://doi.org/10.1109/jiot.2024.3360626
5. X. Yan, X. Yu, S. Yao, and Y. Sun (2024). A domain embedding model for botnet detection based on Smart Blockchain. IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8005–8018, February 2024, https://doi.org/10.1109/jiot.2023.3320046
6. S. Saravanan, and U.M. Balasubramanian, "An adaptive scalable data pipeline for multiclass attack classification in large-scale IOT Networks ". Big Data Mining and Analytics, vol. 7, no. 2, pp. 500–511, April 2024, https://doi.org/10.26599/bdma.2023.9020027
7. P.V. Dinh, Q.U. Nguyen, D.T Hoang, D.N. Nguyen, S.P. Bao and E. Dutkiewicz, "Constrained twin variational auto-encoder for intrusion detection in IOT Systems ". IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14789–14803,2024, https://doi.org/10.1109/jiot.2023.3344842
8. J. Kabdjou, and N. Shinomiya, "Improving quality of service and HTTPS DDoS detection in MEC environment with a cyber-deception based architecture," IEEE Access, vol. 12, pp. 23490–23503,2024, https://doi.org/10.1109/access.2024.3361476
9. A.A. Mohammed, and A.A. Ibrahim, "Malware detection in Adhoc EGovernment Network using machine learning," 5 th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 20 24, https://doi.org/10.1109/hora58378.2023.10156724
10. T. Hasan, J. Malik, I. Bibi, W.U. Khan, F. N. Al-Wesabi, K. Dev and G. Huang, "Securing Industrial Internet of Things Against botnet attacks using hybrid deep learning approach," IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2952–2963, April 2022, https://doi.org/10.1109/tnse.2022.3168533
11. P. Saxena, and R.B. Patel, "Efficient hybrid model for botnet detection using machine learning," 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2024, https://doi.org/10.1109/iccakm58659.2023.10449643
12. F. Sattari, A.H. Farooqi, Z. Qadir, B. Raza, H. Nazari and M. Almutiry. A hybrid deep learning approach for bottleneck detection in IOT. IEEE Access, vol. 10, pp. 77039–77053,2023, https://doi.org/10.1109/access.2022.