International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 7, July 2026)

Deep Learning based Prediction Model for Botnet Attack Detection: A Review

Suraj Kumar[1], Dr. Dayashankar Pandey[2]
[1]M.Tech Scholar, Department of CSE, Sarvepalli Radhakrishnan University, Bhopal, India
[2]Professor, Department of CSE, Sarvepalli Radhakrishnan University, Bhopal, India

***Abstract*— Botnet attacks represent a major cybersecurity threat in which compromised devices are controlled by attackers to perform malicious activities such as distributed denial-of-service attacks, data theft, spam generation, and unauthorized network access. Deep Learning (DL) provides an effective approach for detecting botnet attacks by automatically learning complex patterns from network traffic, communication behavior, and system-level features. This review examines existing DL-based prediction models for botnet attack detection, with particular emphasis on techniques such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Autoencoders, and hybrid deep learning models. The study identifies current research gaps and emphasizes the potential of advanced DL models for developing accurate, adaptive, and efficient botnet attack detection systems.**

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

I. INTRODUCTION

The rapid expansion of Internet of Things (IoT), cloud computing, smart devices, and interconnected digital services has significantly increased the volume of network traffic and simultaneously created new opportunities for cybercriminals to compromise vulnerable systems. Among the major cybersecurity threats, botnet attacks are particularly dangerous because attackers can infect a large number of devices and remotely control them as a coordinated network for malicious activities such as Distributed Denial-of-Service (DDoS) attacks, unauthorized access, data theft, spam distribution, and network disruption [1]. The widespread deployment of resource-constrained IoT devices has further intensified this problem because many devices operate with limited security mechanisms and may remain vulnerable for long periods. Research on IoT security has therefore increasingly focused on identifying compromised devices and abnormal network behavior before botnet-controlled systems can cause large-scale damage [2].

Traditional botnet detection approaches generally rely on predefined signatures, known attack patterns, blacklists, or manually developed rules. Although these techniques can be effective against previously identified threats, their performance may decrease when attackers modify communication patterns, employ encrypted traffic, or introduce previously unseen malware variants. The dynamic nature of modern botnets makes static detection approaches less suitable for continuously changing network environments. Consequently, intelligent detection techniques based on Machine Learning (ML) and Deep Learning (DL) have gained considerable attention because they can learn behavioral patterns from network traffic and identify deviations associated with malicious activities [3]. A systematic review of IoT botnet detection research has reported that ML and DL approaches provide promising capabilities compared with conventional signature-based techniques, although their effectiveness depends considerably on datasets, selected features, preprocessing methods, and evaluation strategies [4].

Deep Learning represents an important advancement in automated botnet detection because deep neural networks can learn hierarchical and complex representations directly from large volumes

of network data. Unlike conventional ML methods that often require extensive manual feature engineering, DL models can identify meaningful relationships among traffic characteristics through multiple processing layers. Convolutional Neural Networks (CNNs), for example, can learn spatial or local patterns from transformed network traffic features, whereas Recurrent Neural Networks (RNNs) are capable of modeling sequential dependencies in network communication [5]. Long Short-Term Memory (LSTM) networks, a specialized form of RNN, are particularly useful for botnet detection because they can retain information from previous traffic observations and therefore capture temporal relationships associated with malicious communication. Studies have reported high detection performance using LSTM-based models on network security datasets, demonstrating their potential for identifying IoT botnet activities [6].

Another important direction is the use of hybrid and optimized deep learning architectures. Combining CNNs with LSTM or other neural architectures can enable a model to learn both local traffic characteristics and temporal behavior. Such approaches are useful because botnet activities may not be distinguishable through a single network feature; instead, their identification can require analysis of packet characteristics, connection patterns, communication frequency, protocols, and temporal relationships. Recent studies have explored CNN, RNN, LSTM, hybrid models, and other DL architectures for botnet detection across benchmark datasets such as BoT-IoT and N-BaIoT [7]. Deep learning has also been investigated for developing computationally efficient detection models suitable for environments where processing resources are limited, which is particularly important for IoT and edge-based security applications [8].

The effectiveness of a DL-based botnet prediction model depends not only on the selected neural architecture but also on the quality and representativeness of the training data. Publicly available datasets such as BoT-IoT, N-BaIoT, UNSW-NB15, and CIC-IDS2017 are frequently used for evaluating cybersecurity models because they provide network traffic containing both benign and malicious behaviors [9]. However, differences in data distribution, attack categories, feature representations, and class balance can significantly influence model performance. Class imbalance is another important challenge because certain attack categories may contain considerably fewer samples than normal traffic or other attack types. Researchers have therefore investigated preprocessing, feature selection, resampling, and data balancing techniques to improve the reliability of botnet detection models [10].

Despite the promising results of DL-based approaches, several research challenges remain. Modern botnets continuously evolve their attack strategies, making generalization to new and zero-day attacks difficult. Furthermore, highly accurate models may require substantial computational resources, while real-time security applications demand rapid detection with low latency. The lack of diverse and realistic datasets also limits the ability of models to perform reliably in practical environments [11]. Recent research additionally identifies explainability, federated learning, privacy preservation, and the development of more representative real-world datasets as important future directions for AI-driven IoT botnet detection [12].

II. LITERATURE SURVEY

Ali et al., [1] developed a hybrid machine learning model for efficient botnet attack detection in IoT environments. The study focused on identifying malicious network behavior from IoT traffic using a combination of machine learning techniques. The hybrid strategy aimed to improve the detection capability compared with individual learning algorithms. The authors emphasized efficient classification of different botnet-related activities in resource-constrained IoT environments. The study demonstrated the potential of hybrid learning for improving the reliability of IoT botnet detection.

Kumar et al., [2] presented an enhanced hybrid deep learning approach for detecting botnet attacks in IoT environments. The study combined deep learning techniques to automatically learn complex patterns associated with malicious network traffic. The proposed approach was designed to improve the identification of botnet activities across different IoT

attack scenarios. The use of hybrid deep learning reduced the dependency on manually designed detection rules. The study highlighted deep learning as an effective approach for accurate and automated botnet attack detection.

Alshehri et al., [3] proposed SkipGateNet, a lightweight CNN-LSTM hybrid model for efficient botnet attack detection in IoT networks. The model incorporated learnable skip connections to improve information propagation and learning efficiency. CNN was used to capture important local characteristics, while LSTM analyzed sequential dependencies in network traffic. The lightweight architecture was designed to reduce computational requirements while maintaining effective detection performance. The study demonstrated the suitability of hybrid CNN-LSTM architectures for resource-constrained IoT security applications.

Al-Fawa'reh et al., [4] introduced MalbotDRL, a malware botnet detection approach based on deep reinforcement learning for IoT networks. The study applied reinforcement learning to identify malicious behaviors and improve botnet detection through an adaptive learning process. The approach considered the changing nature of malware and botnet activities in IoT environments. Deep reinforcement learning provided the capability to learn appropriate detection decisions from network behavior. The research showed the potential of adaptive learning techniques for addressing evolving IoT botnet threats.

Kalakoti et al., [5] investigated the use of explainable artificial intelligence for IoT botnet detection. The study focused not only on detecting malicious traffic but also on understanding the decisions produced by AI-based detection models. Explainability techniques were quantitatively evaluated to determine how effectively model predictions could be interpreted. The work addressed an important limitation of complex machine learning and deep learning models, namely their lack of transparency. The findings emphasized that explainable AI can improve the trustworthiness and practical usability of IoT botnet detection systems.

Yan et al., [6] presented a domain embedding model for botnet detection based on Smart Blockchain technology. The study explored the integration of domain-related information and blockchain-based mechanisms to improve the identification of malicious botnet activities. The domain embedding approach was used to represent relevant information for more effective botnet classification. Blockchain provided an additional mechanism for maintaining reliable and secure information within the detection framework. The research demonstrated the potential of combining intelligent learning and blockchain technologies for enhancing botnet detection.

Saravanan and Balasubramanian [7] developed an adaptive and scalable data pipeline for multiclass attack classification in large-scale IoT networks. The study addressed the challenge of processing and analyzing large volumes of IoT security data for identifying multiple attack categories. The proposed pipeline was designed to support scalable data processing and adaptive attack classification. Such an approach can assist intelligent security systems in handling continuously generated network traffic. The study highlighted the importance of efficient data pipelines for large-scale IoT attack detection and classification.

Dinh et al. [8] presented a constrained twin variational auto-encoder for intrusion detection in IoT systems. The model utilized variational autoencoder-based learning to capture meaningful representations of network traffic and identify abnormal behavior. The constrained twin architecture was designed to improve the capability of the model to distinguish normal and malicious activities. The approach addressed the challenges associated with complex and high-dimensional IoT security data. The study indicated that advanced representation learning can provide an effective foundation for intelligent intrusion and botnet detection.

Kabdjou and Shinomiya [9] investigated HTTPS DDoS detection in a Multi-access Edge Computing (MEC) environment using a cyber-deception-based

architecture. The study focused on detecting malicious traffic while maintaining quality of service in edge computing environments. Cyber-deception mechanisms were incorporated to mislead attackers and facilitate the identification of suspicious activities. The approach is relevant to botnet detection because botnets can generate coordinated DDoS traffic against network and edge resources. The study demonstrated the importance of combining proactive security mechanisms with intelligent attack detection.

Mohammed and Ibrahim [10] studied malware detection in an ad hoc e-government network using machine learning techniques. The research focused on identifying malicious software and suspicious activities within a network environment using automated learning methods. Machine learning was employed to analyze available network characteristics and classify potentially harmful activities. The study demonstrated the applicability of intelligent detection methods in specialized and security-sensitive network infrastructures. Its findings support the broader use of machine learning for automated malware and botnet-related threat identification.

Popoola et al. [11] presented a hybrid deep learning framework for botnet attack detection in Internet-of-Things networks. The study combined deep learning techniques to learn complex patterns from IoT network traffic and distinguish botnet activities from legitimate behavior. The hybrid architecture aimed to exploit the complementary capabilities of different deep learning models. The research addressed the difficulty of detecting sophisticated botnet attacks using conventional security mechanisms. The study established the effectiveness of hybrid deep learning as a promising approach for automated IoT botnet detection.

Popoola et al. [12] presented a federated deep learning approach for zero-day botnet attack detection in IoT edge devices. The study addressed the challenge of identifying previously unseen botnet attacks while preserving the decentralized nature of IoT edge environments. Federated learning enabled multiple devices or edge nodes to collaboratively train a deep learning model without directly sharing their local training data. The approach was particularly relevant to zero-day detection, where conventional signature-based methods may fail. The study demonstrated the potential of federated deep learning for privacy-aware and adaptive botnet detection at the IoT edge.

III. CHALLENGES

Deep Learning-based botnet attack detection provides powerful capabilities for identifying complex and evolving malicious behaviors, but its practical implementation still faces several challenges. The effectiveness of a prediction model depends on the quality and diversity of training data, appropriate feature representation, model architecture, computational resources, and the ability to generalize to previously unseen attacks. Botnet traffic can change rapidly due to variations in communication protocols, attack strategies, encryption, and device behavior, making it difficult for a trained model to maintain consistent detection performance. In addition, issues such as imbalanced datasets, false positives, high computational requirements, lack of interpretability, privacy concerns, and limited real-world datasets can restrict the deployment of deep learning models in large-scale IoT and edge environments.

1. Evolving Botnet Attack Patterns

Botnet attacks continuously evolve as attackers modify malware behavior, communication protocols, and attack strategies. A model trained using historical attack patterns may perform poorly when exposed to new or modified botnet variants. Therefore, prediction models need adaptive learning capabilities to maintain detection performance against continuously changing threats.

2. Zero-Day Attack Detection

Detecting zero-day botnet attacks is one of the major challenges in cybersecurity. Such attacks have no previously known signatures or established behavioral patterns. Conventional detection systems may fail to identify them because they depend heavily on known attack characteristics. Deep learning models must therefore develop strong generalization capabilities to recognize previously unseen malicious behavior.

3. Imbalanced and Limited Datasets

Security datasets frequently contain a large number of normal traffic records but comparatively fewer samples of specific botnet attacks. This class imbalance can cause a model to favor majority classes and produce poor detection results for minority attack categories. Moreover, publicly available datasets may not fully represent current real-world botnet behavior, limiting model reliability.

4. High Computational Requirements

Deep learning architectures such as CNN, LSTM, GRU, and hybrid networks can require substantial computational power and memory during training and inference. This becomes particularly challenging for IoT and edge devices that have limited processing capacity, memory, and energy resources. Developing lightweight architectures without significantly reducing detection accuracy remains an important research challenge.

5. Real-Time Detection and Low Latency

Botnet attacks can spread or generate harmful traffic within a very short period. Therefore, detection systems must analyze network traffic and produce predictions rapidly. Complex deep learning models may introduce computational delays, making real-time deployment difficult. Efficient feature processing, model optimization, and edge-based inference are required to reduce detection latency.

6. False Positives and False Negatives

A reliable botnet detection system should minimize both false positives and false negatives. A false positive may incorrectly classify legitimate network traffic as malicious, causing unnecessary alerts and resource consumption. Conversely, a false negative allows an actual botnet attack to remain undetected. Achieving a suitable balance between detection sensitivity and classification accuracy is therefore challenging.

IV. CONCLUSION

Deep Learning-based prediction models have emerged as an effective approach for detecting botnet attacks because they can automatically learn complex, nonlinear, and temporal patterns from large volumes of network traffic. The reviewed studies demonstrate the effectiveness of CNN, LSTM, hybrid deep learning, deep reinforcement learning, explainable AI, and federated learning approaches for improving botnet detection accuracy and addressing challenges such as evolving attacks and zero-day threats. However, issues related to dataset imbalance, computational complexity, false detection, model interpretability, real-time processing, privacy, and generalization remain important limitations. Future research should focus on developing lightweight, adaptive, explainable, and privacy-preserving deep learning models capable of operating efficiently in IoT and edge environments while providing reliable detection of both known and previously unseen botnet attacks.

REFERENCES

1. M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran and I. Ashraf, "Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment," in *IEEE Access*, vol. 12, pp. 40682-40699, 2024, doi: 10.1109/ACCESS.2024.3376400.
2. 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.

3. 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.
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui and H. Gacanin, "Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4944-4956, 15 March15, 2021, doi: 10.1109/JIOT.2020.3034156.
12. S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3100755.