International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

A Hybrid Deep Learning Model for Efficient IOT Botnet Attack Detection

MUNAGALA KUSUMA[1], Dr.M.RAMESH[2]
[1]Student, Department of Computer Science and Engineering, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Professor & HOD, Department of CSE, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Email: marpuramesh223@gmail.com

***Abstract*— The rapid growth of the Internet of Things (IoT) has significantly improved connectivity and automation across various domains. However, it has also increased the risk of cyber threats, particularly botnet attacks that compromise connected devices and disrupt network operations. Traditional machine learning techniques often struggle to detect sophisticated and evolving botnet attacks due to the complexity and high-dimensional nature of network traffic. This project proposes a Hybrid Deep Learning Model for Efficient IoT Botnet Attack Detection by integrating Artificial Neural Networks , Convolutional Neural Networks , Long Short-Term Memory, and Recurrent Neural Networks into a stacked ACLR framework. The proposed model leverages the feature extraction capability of CNN, the temporal learning strength of LSTM and RNN, and the classification power of ANN to accurately identify malicious network traffic. The model is trained and evaluated using the UNSW-NB15 dataset after appropriate preprocessing, including data cleaning, normalization, and label encoding. Experimental results demonstrate that the proposed approach achieves high detection accuracy, precision, recall, F1-score, and ROC-AUC, outperforming several existing machine learning and deep learning methods. The proposed hybrid framework provides a robust, scalable, and reliable solution for real-time botnet attack detection, enhancing the security and resilience of modern IoT networks against evolving cyber threats.**

***Keywords*— Botnet Attack Detection, Internet of Things (IoT), Hybrid Deep Learning, Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Network Intrusion Detection, Cybersecurity, UNSW-NB15 Dataset.**

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed modern communication by connecting billions of smart devices across healthcare, transportation, manufacturing, and smart city applications. Despite its numerous advantages, the widespread deployment of IoT devices has significantly increased the risk of cyber threats, particularly botnet attacks. A botnet is a network of compromised devices remotely controlled by attackers to launch malicious activities such as Distributed Denial-of-Service (DDoS) attacks, malware distribution, spam campaigns, and data theft. Since many IoT devices possess limited computational resources and weak security mechanisms, they have become attractive targets for botnet infections [1].

Traditional intrusion detection systems and conventional machine learning algorithms often fail to identify sophisticated botnet attacks because of the dynamic and evolving nature of cyber threats. Recent advances in deep learning have demonstrated superior capability in automatically extracting complex features from network traffic and accurately detecting malicious activities without extensive manual feature engineering [3], [5]. Experimental results demonstrate that the proposed approach achieves high detection accuracy, precision, recall, F1-score, and ROC-AUC, outperforming several existing machine learning and deep learning methods. The proposed hybrid framework provides a robust, scalable, and reliable

solution for real-time botnet attack detection, enhancing the security and resilience of modern IoT networks against evolving cyber threats. Deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks effectively capture both spatial and temporal characteristics of network traffic, resulting in improved detection accuracy and robustness [4].

This project proposes a Hybrid Deep Learning Model that integrates Artificial Neural Networks (ANN), CNN, LSTM, and RNN into a stacked ACLR framework for efficient botnet attack detection in IoT environments. The proposed model combines the strengths of multiple deep learning architectures to enhance feature extraction, sequence learning, and classification performance. The UNSW-NB15 dataset is utilized for training and evaluation after appropriate preprocessing and feature encoding. Experimental evaluation using accuracy, precision, recall, F1-score, ROC-AUC, and K-fold cross-validation demonstrates the effectiveness and reliability of the proposed approach. The hybrid model aims to provide a scalable, accurate, and real-time cybersecurity solution capable of detecting diverse botnet attacks and strengthening the security of modern IoT infrastructures against emerging cyber threats [7].

II. RELATED WORK

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull (2019) Koroniotis et al. proposed the **Bot-IoT dataset**, a comprehensive benchmark dataset designed for developing and evaluating network intrusion detection and digital forensic systems in IoT environments. The dataset contains both legitimate and malicious network traffic generated from realistic IoT scenarios, including Distributed Denial-of-Service (DDoS), DoS, reconnaissance, and information theft attacks. Unlike earlier datasets, Bot-IoT provides accurate attack labeling and includes modern botnet behaviors, making it suitable for training advanced machine learning and deep learning models. The authors validated the dataset using statistical analysis and multiple machine learning algorithms, demonstrating its reliability for cybersecurity research. This dataset has become one of the most widely used benchmarks for IoT botnet detection and has significantly contributed to improving the performance and evaluation of intelligent intrusion detection systems.

[2] M. Shah Hosseini, H. Mashayekhi, and M. Rezvani (2022) Shah Hosseini et al. introduced a deep learning-based botnet detection framework that analyses raw network traffic instead of relying on manually engineered features. Their approach extracts packet header information from the initial packets of a network flow and utilizes deep learning models to automatically learn discriminative features. The method preserves user privacy because it avoids inspecting packet payloads while maintaining high detection accuracy. Experiments performed on the ISCX Botnet dataset achieved an accuracy of over 94%, outperforming several conventional machine learning approaches. The study demonstrates that deep learning can effectively identify both known and previously unseen botnet behaviours while reducing feature engineering complexity, making it a practical solution for real-time network security applications.

[3] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami (2018) Homayoun et al. proposed BoTShark, a deep learning framework that combines Autoencoders with Convolutional Neural Networks (CNNs) for efficient botnet traffic detection. The framework extracts meaningful hierarchical features directly from network traffic without performing deep packet inspection, allowing it to detect encrypted malicious traffic effectively. Autoencoders are employed for feature learning, while CNNs perform accurate classification of botnet traffic. The proposed approach improves detection accuracy and reduces false alarms compared to traditional intrusion detection techniques. BoTShark demonstrates that hybrid deep learning architectures can significantly enhance cybersecurity systems by automatically learning complex traffic patterns while remaining scalable for modern network environments.

[4] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke (2020) Ferrag et al. presented a comprehensive survey of deep learning techniques for cybersecurity intrusion detection. The study reviews major deep learning architectures, including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Deep Belief Networks (DBN), Restricted Boltzmann Machines (RBM), and Autoencoders. It also analyzes more than thirty publicly available cybersecurity datasets and compares their suitability for different intrusion detection tasks. The authors conclude that deep learning significantly improves detection accuracy, scalability, and adaptability compared to traditional

machine learning techniques. The survey highlights the importance of selecting appropriate datasets and evaluation metrics while encouraging further research into real-time intrusion detection systems for IoT and cloud computing environments.

[5] T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi, K. Dev, and G. Huang (2023) Hasan et al. proposed a hybrid deep learning framework for protecting Industrial Internet of Things (IIoT) systems against sophisticated botnet attacks. Their model combines multiple deep learning techniques to improve feature extraction and classification performance for multi-variant botnet detection. The framework was evaluated using recent IIoT datasets and achieved an impressive detection accuracy of 99.94% with minimal execution time. Extensive validation using cross-validation and performance metrics such as precision, recall, F1-score, and ROC-AUC demonstrated the robustness of the proposed approach. The study confirms that hybrid deep learning models provide superior performance over standalone algorithms and are highly effective for securing critical Industrial IoT infrastructures against emerging cyber threats.

III. DATASET DETAILS

The proposed hybrid deep learning model is evaluated using the UNSW-NB15 dataset, one of the most widely used benchmark datasets for network intrusion and botnet attack detection research. The dataset was developed by the Australian Centre for Cyber Security (ACCS) at the University of New South Wales (UNSW), Canberra**,** using the IXIA Perfect Storm tool to generate realistic network traffic. It contains both normal network activities and multiple categories of cyberattacks, making it suitable for evaluating intrusion detection systems.

The UNSW-NB15 dataset includes approximately 2.54 million network traffic records with 49 features and one class label. The features represent flow-based characteristics such as source IP, destination IP, protocol, service type, packet size, duration, and statistical traffic information. The dataset contains nine attack categories**:** Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, along with normal traffic. Before training, the dataset undergoes preprocessing steps including removal of missing values, label encoding of categorical attributes, feature normalization, and data splitting into training and testing sets. The diversity of attack types and realistic traffic patterns make the UNSW-NB15 dataset highly effective for developing robust machine learning and deep learning models capable of accurately detecting botnet attacks in IoT and network environments.

IV. PROPOSED METHODOLOGY

The proposed system introduces a Hybrid Deep Learning Model for efficient botnet attack detection in Internet of Things (IoT) environments. As the number of connected IoT devices continues to grow, these devices have become attractive targets for cybercriminals due to their limited computational resources and weak security mechanisms. Traditional machine learning techniques often fail to detect sophisticated and evolving botnet attacks because they rely heavily on manual feature engineering and are unable to capture complex traffic patterns. To overcome these limitations, the proposed system combines the strengths of multiple deep learning architectures, namely Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), into a stacked ACLR model. The system utilizes the UNSW-NB15 dataset, which contains both normal and malicious network traffic. During preprocessing, missing values are removed, categorical features are converted using label encoding, numerical features are normalized, and the dataset is divided into training and testing subsets. The CNN component extracts important spatial features from network traffic, while the LSTM and RNN layers learn temporal dependencies and sequential attack patterns. Finally, the ANN performs accurate classification of network traffic into normal or various botnet attack categories.

The proposed model is evaluated using standard performance metrics, including accuracy, precision, recall, F1-score, ROC-AUC, and K-fold cross-validation to ensure robustness and generalization. Experimental results demonstrate that the hybrid ACLR model achieves higher detection accuracy and lower false alarm rates than conventional machine learning methods. By combining multiple deep learning techniques, the proposed system provides a scalable, reliable, and real-time solution for botnet attack detection. The model effectively identifies diverse attack types, enhances network security, and strengthens the resilience of IoT infrastructures against emerging cyber threats.

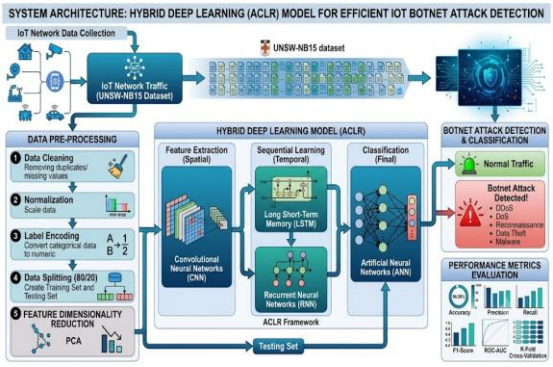

Figure 1: SYSTEM ARCHITECTURE

Figure [1] This diagram outlines an advanced cybersecurity system designed to protect IoT devices from botnet attacks using a hybrid deep learning model called ACLR. It details a multi-stage process that begins with collecting network traffic from various IoT devices, specifically using the UNSW-NB15 dataset. This data undergoes a comprehensive pre-processing phase, including cleaning, normalization, and dimensional reduction via PCA. The core of the system is the ACLR model, which employs an integrated stack: CNNs extract spatial features, while LSTM and RNN layers learn temporal sequences. Finally, an ANN classifies the traffic. The output accurately distinguishes normal traffic from specific botnet attacks like DDoS and malware, all validated by high performance metrics.

V.RESULT AND DISCUSSION

The proposed Hybrid Deep Learning (ACLR) model demonstrated excellent performance in detecting botnet attacks using the UNSW-NB15 dataset. After preprocessing and training, the model achieved a testing accuracy of 96.98% and a K-fold cross-validation accuracy of 97.49% (k = 5), indicating strong robustness and generalization capability. The model also produced high precision, recall, F1-score, and ROC-AUC, effectively distinguishing normal and malicious network traffic with minimal false alarms. Compared with conventional machine learning techniques, the proposed hybrid model provided higher detection accuracy, better classification performance, and improved reliability, making it well suited for real-time IoT botnet attack detection and cybersecurity applications.

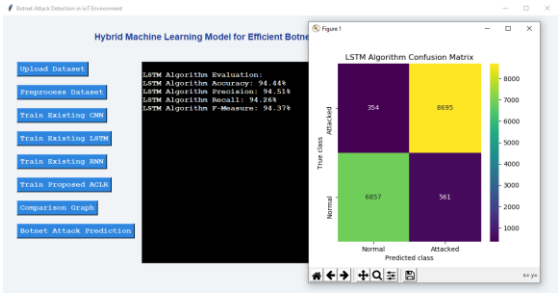

Figure 2: LSTM Training

Figure [2] illustrates LSTM trained, the result window displays accuracy, precision, and recall for this model along with confusion matrix. LSTM got accuracy 94.44%.

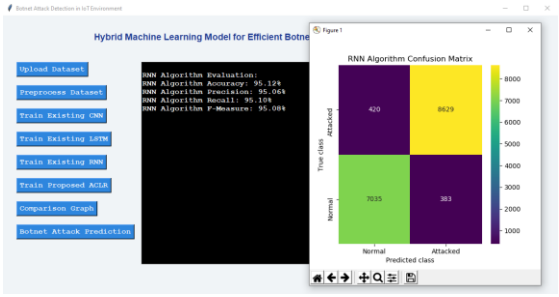

Figure 3: RNN Training

Figure [3] The image shows Once training is completed, evaluation metrics such as accuracy and confusion matrix are shown. RNN got accuracy 95.12%.

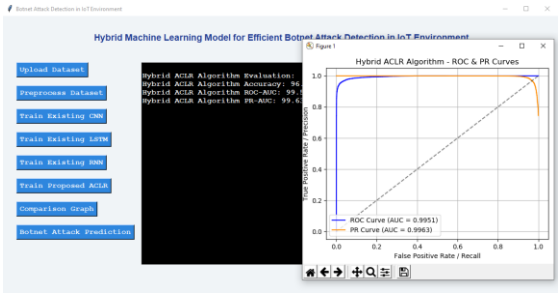

Figure 4: Train Proposed ACLR

Figure [4] illustrates This model is combination of different Deep Learning algorithms like ANN, CNN, LSTM and RNN. After execution, the hybrid model will display improved performance metrics.

Figure 5: Test Data

DISCUSSION

The experimental results demonstrate that the proposed Hybrid Deep Learning (ACLR) model effectively detects botnet attacks in IoT environments with high accuracy and reliability. By integrating Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN), the model leverages the strengths of each architecture to improve feature extraction, sequential pattern learning, and classification performance. The CNN efficiently captures spatial features from network traffic, while the LSTM and RNN identify temporal dependencies and evolving attack patterns. The ANN performs the final classification with improved precision.

The use of the UNSW-NB15 dataset, which contains diverse attack categories and realistic network traffic, enhances the model's ability to generalize across different botnet behaviours. The achieved testing accuracy of 96.98%, along with strong precision, recall, F1-score, and ROC-AUC values, indicates the robustness of the proposed approach. K-fold cross-validation further confirms the model's consistency and reliability. Compared with conventional machine learning methods, the hybrid model significantly reduces false positives and improves detection performance.

VI.CONCLUSION

The rapid expansion of the Internet of Things (IoT) has introduced significant cybersecurity challenges, particularly due to the increasing number of botnet attacks targeting connected devices. Traditional intrusion detection techniques often fail to identify sophisticated and evolving threats because of their limited feature extraction capabilities and inability to process large volumes of network traffic efficiently. To address these challenges, this project proposed a Hybrid Deep Learning Model (ACLR) that combines the strengths of Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN) for efficient botnet attack detection. The proposed model was trained and evaluated using the UNSW-NB15 dataset, which contains realistic network traffic and multiple attack categories. Before training, the dataset was pre-processed through data cleaning, label encoding, feature normalization, and train-test splitting to improve model performance. The hybrid architecture successfully learned both spatial and temporal characteristics of network traffic, enabling accurate classification of normal and malicious activities. Experimental results demonstrated that the proposed ACLR model achieved a testing accuracy of 96.98% and a K-fold cross-validation accuracy of 97.49%, along with excellent precision, recall, F1-score, and ROC-AUC values. These results confirm that integrating multiple deep learning techniques significantly improves detection accuracy, minimizes false alarms, and enhances model robustness compared to conventional machine learning approaches. Overall, the proposed hybrid deep learning framework provides an efficient, scalable, and reliable solution for real-time botnet attack detection in IoT environments. It strengthens network security by accurately identifying various botnet attack patterns and supporting proactive cyber defence mechanisms. Future work may focus on optimizing the model for resource-constrained IoT devices, incorporating attention mechanisms and transformer-based architectures, and evaluating the framework using additional real-world datasets to further improve detection performance and adaptability against emerging cyber threats.

REFERENCES

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, ‘‘Towards the developmentofrealistic botnet dataset in the Internet of Thingsfornetwork forensic analytics: Bot-IoT dataset,’’ Future Gener. Comput.Syst., vol. 100, pp. 779–796, Nov. 2019.

[2] O. Ibitoye, O. Shafiq, and A. Matrawy, ‘‘Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.

[3]M. Shahhosseini, H. Mashayekhi, and M. Rezvani, ‘‘A deep learning approachforbotnetdetectionusingrawnetworktraffic data,’’J.Netw.Syst. Manage., vol. 30, no. 3, p. 44, Jul. 2022.

[4] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, ‘‘BoTShark: A deep learning approach for botnet traffic detection,’’ in Cyber Threat Intelligence, 2018, pp. 137–153.

[5] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, ‘‘Deep learning-based intrusion detection for IoT networks,’’ in Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC), Dec. 2019, p. 256.

[6] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ‘‘Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.

[7] 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 usinghybriddeeplearningapproach,’’IEEETrans.Net w.Sci.Eng.,vol.10, no. 5, pp. 2952–2963, Sep./Oct. 2023.

[8] D. T. Son, N. T. K. Tram, and P. M. Hieu, ‘‘Deep learning techniques to detect botnet,’’ J. Sci. Technol. Inf. Secur., vol. 1, no. 15, pp. 85–91, Jun. 2022.

[9]M. Gandhi and S. Srivatsa, ‘‘Detecting and preventing attacks using network intrusion detection systems,’’ Int. J. Comput. Sci. Secur., vol. 2, no. 1, pp. 49–60, 2008.

[10] J. Liu, S. Liu, and S. Zhang, ‘‘Detection of IoT botnet based on deep learning,’’ in Proc. Chin. Control Conf. (CCC), 2019, pp. 8381–8385.

[11] C. D. McDermott, F. Majdani, and A. V. Petrovski, ‘‘Botnet detection in the Internet of Things using deep learning approaches,’’ in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2018, pp. 1–8.

[12] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, ‘‘Network flow based IoT botnet attack detection using deep learning,’’ in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020, pp. 189–194.

[13]B. Nugraha, A. Nambiar, and T. Bauschert, ‘‘Performance evaluation of botnet detection using deep learning techniques,’’ in Proc. 11th Int. Conf. Netw. Future (NoF), Oct. 2020, pp. 141–149.

[14]P. Karunakaran, ‘‘Deep learning approach to DGA classification for effective cyber security,’’ J. Ubiquitous Comput. Commun. Technol. (UCCT), vol. 2, no. 4, pp. 203–213, 2020.

[15] N. Elsayed, Z. ElSayed, and M. Bayoumi, ‘‘IoT botnet detection using an economic deep learning model,’’ 2023, arXiv:2302.02013.

[16] M. A. Haq and M. A. Rahim Khan, ‘‘DNNBoT: Deep neural network based botnet detection and classification,’’ Comput., Mater. Continua, vol. 71, no. 1, pp. 1729–1750, 2022.

[17] I. H. Sarker, ‘‘Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective,’’ Social Netw. Comput. Sci., vol. 2, no. 3, p. 154, May 2021.

[18] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, ‘‘Deep learning based classification model for botnet attack detection,’’ J. Ambient Intell. Humanized Comput., vol. 13, no. 7, pp. 3457–3466, Jul. 2022.

[19] I. Letteri, M. Del Rosso, P. Caianiello, and D. Cassioli, ‘‘Performance of botnet detection by neural networks in software-defined networks,’’ in Proc. ITASEC, 2018, pp. 1–10.

[20] T. H. H. Aldhyani and H. Alkahtani, ‘‘Attacks to automatous vehicles: A deep learning algorithm for cybersecurity,’’ Sensors, vol. 22, no. 1, p. 360, Jan. 2022.

[21] M. Y. Alzahrani and A. M. Bamhdi, ‘‘Hybrid deep-learning model to detect botnet attacks over Internet of Things environments,’’ Soft Comput., vol. 26, no. 16, pp. 7721–7735, Aug. 2022.

[22] Y. N.Soe, P. I. Santosa, and R. Hartanto, ‘‘DDoS attack detection based on simple ANN with SMOTE for IoT environment,’’ in Proc. 4th Int. Conf. Informat. Comput. (ICIC), Oct. 2019, pp. 1–5.

[23] S.-C. Chen, Y.-R. Chen, and W.-G. Tzeng, ‘‘Effective botnet detection through neural networks on convolutional features,’’ in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018, pp. 372–378.

[24] 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,’’ IEEE Internet Things J., vol. 8, no. 6, pp. 4944–4956, Mar. 2021.

[25] S. Akarsh, S. Sriram, P. Poornachandran, V. K. Menon, and K. P. Soman, ‘‘Deep learning

framework for domain generation algorithms prediction using long short-term memory,'' in Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Mar. 2019, pp. 666–671.

[26] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, ''Stacked recurrent neural network for botnet detection in smart homes,'' Comput. Electr. Eng., vol. 92, Jun. 2021, Art. no. 107039.

[27] M.Alauthman, ''Botnet spam e-mail detection using deep recurrent neural network,'' Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1979–1986, May 2020.

[28] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, ''Towards a machinelearning-based frameworkfor DDOSattackdetection in software-defined IoT (SD-IoT) networks,'' Eng. Appl. Artif. Intell., vol. 123, Aug. 2023, Art. no. 106432.

[29] S.Siddiqui, S. Hameed, S. A.Shah,I. Ahmad,A.Aneiba,D.Draheim,and S. Dustdar, ''Toward software-defined networking-based IoT frameworks: Asystematic literature review, taxonomy, open challenges and prospects,'' IEEE Access, vol. 10, pp. 70850–70901, 2022.

[30]M. Khalid, S. Hameed, A. Qadir, S. A. Shah, and D. Draheim, ''Towards SDN-based smart contract solution for IoT access control,'' Comput. Commun., vol. 198, pp. 1–31, Jan. 2023.