HYBRID MACHINE LEARNING MODEL FOR EFFICIENT BOTNET ATTACK DETECTION IN IOT ENVIRONMENT

Shaimaa Shahabuddin[1], Summaya Afreen[2], Sarah[3], Sarah Shazmeen[4], Ms. Lubna Nausheen[5]
[1,2,3,4]UG Scholar, Dept of CSE, Shadan Women's College of Engineering and Technology, Hyderabad,
[5]Asst. Professor, Dept of CSE, Shadan Women's College of Engineering and Technology

ABSTARCT
Fueled by breakthroughs in Internet technologies, cyber-attacks are becoming increasingly sophisticated, with botnet attacks emerging as one of the most harmful threats. Botnet identification is challenging due to the wide range of attack vectors and the continuous evolution of malicious software. As the Internet of Things (IoT) technology expands, many network devices are susceptible to botnet attacks, leading to significant losses in various sectors. This paper proposes a botnet identification system using a Long Short-Term Memory (LSTM) model, a popular deep learning approach, to effectively distinguish between normal network traffic and botnet attacks. The model classifies network traffic into two categories: normal (0) and botnet attack (1). Experiments were conducted using the UNSW-NB15 dataset, which contains nine types of attacks, including 'Normal', 'Generic', 'Exploits', 'Fuzzers', 'DoS', 'Reconnaissance', 'Analysis', 'Backdoor', 'Shell code', and 'Worms'. The LSTM-based model achieved an impressive testing accuracy of 90%. The proposed approach demonstrates strong performance in identifying botnet activities, with high receiver operating characteristic (ROC) area under the curve (AUC) and precision-recall area under the curve (PR-AUC) scores, indicating its effectiveness in classifying normal and attack traffic. Performance comparisons with existing state-of-the-art models further validate the robustness of the proposed LSTM-based approach. This research contributes to enhancing cybersecurity procedures by providing a reliable tool for detecting botnet attacks in evolving network environments.

1. INTRODUCTION

The rapid advancement of Internet technology has significantly transformed how we interact with the world, creating new opportunities for communication, commerce, and innovation. However, alongside these advancements comes a growing threat of cyberattacks, with botnet attacks emerging as one of the most severe and widespread. A botnet is a network of compromised devices that are controlled by malicious actors, often used to launch large-scale attacks such as Distributed Denial of Service (DDoS) or to perform data theft and other harmful activities. The growing sophistication and complexity of these attacks pose significant challenges for network administrators and cybersecurity experts, as botnet activities are difficult to detect and mitigate. The primary reason for this difficulty lies in the vast range of attack vectors that botnets employ, coupled with the continuous evolution of malware and attack techniques designed to bypass traditional security measures. The rise of the Internet of Things (IoT) has further compounded this issue. As more devices, including everyday appliances, are connected to the Internet, they become vulnerable to botnet infections. Many of these devices lack the security features required to protect against cyber threats, making them prime targets for attackers. The consequences of botnet attacks are far-reaching, affecting critical infrastructure, financial systems, personal data, and even national security. As the Internet becomes increasingly integral to all aspects of life, the ability to effectively identify and neutralize botnet threats has never been more urgent. This project proposes an innovative solution to address the challenge of botnet detection in modern network environments. Leveraging the power of Long Short-Term Memory (LSTM) networks, a type of recurrent neural network (RNN) that excels at processing sequential data, this system aims to accurately classify network traffic as either normal or indicative of a botnet attack. The LSTM model's ability to capture long-term dependencies in data makes it particularly well-suited for analyzing network traffic patterns, which often involve sequences of actions over time. By training the LSTM model on the UNSW-NB15 dataset, which includes a variety of network traffic types and attack categories, the system is designed to distinguish between benign and malicious behavior with high.

OBJECTIVE

The objective of this project is to design and develop a robust botnet detection system using Long Short-Term Memory (LSTM) networks to classify network traffic as normal or malicious (botnet attack). The project aims to leverage deep learning techniques to analyze network traffic patterns and effectively identify botnet activities in real-time. Using the UNSW-NB15 dataset, which includes various attack types and normal traffic data, the model will be trained to distinguish between normal and botnet traffic. The primary goal is to achieve high detection accuracy and evaluate the model's performance using metrics like accuracy, ROC AUC, and PR AUC. The project also aims to compare the proposed LSTM-based approach with existing detection models to assess its effectiveness and practicality in real-world cybersecurity applications. Ultimately, the

objective is to enhance cybersecurity measures by providing a reliable tool for detecting and mitigating botnet attacks.

2.1 PROBLEM STATEMENT

With the rapid growth of digital networks and the increasing interconnectivity brought by the Internet of Things (IoT), cyber threats have become more complex and frequent. Among these, botnet attacks pose a severe and evolving risk, exploiting vulnerable devices to launch large-scale attacks, disrupt services, steal sensitive data, and compromise network integrity. Traditional security methods often fail to detect such threats effectively due to the dynamic behavior and stealthy nature of botnet traffic. Additionally, the continuous evolution of attack strategies and malware variants further challenges existing detection systems. Therefore, there is a critical need for intelligent, adaptive, and automated solutions that can accurately identify and classify malicious botnet activities in real-time. This project addresses this challenge by proposing a hybrid machine learning approach using Long Short-Term Memory (LSTM) networks to analyze sequential network traffic data and distinguish between normal and botnet traffic patterns with high accuracy. The aim is to enhance the overall cybersecurity framework by providing a reliable and efficient detection mechanism capable of adapting to evolving threat landscapes.

2.2 EXISTING SYSTEM

The existing system for botnet detection often employs machine learning techniques such as Support Vector Machines (SVM). SVM is a powerful supervised learning algorithm used for classification tasks, including the identification of botnet activities in network traffic. In the context of botnet detection, SVM works by finding the optimal hyperplane that best separates the data into different classes, such as botnet traffic and normal traffic. The algorithm is effective in high-dimensional spaces, making it suitable for analyzing complex network traffic data with multiple features. However, SVM can have limitations, especially when handling large datasets with a high level of noise or when the data is not linearly separable. In these cases, the performance of SVM may degrade, and it may require careful tuning of hyperparameters like the kernel function and regularization parameter. Despite these challenges, SVM has been widely used in botnet detection due to its simplicity, efficiency, and ability to generalize well when provided with a well-structured feature set. However, compared to more advanced deep learning models, SVM might struggle to capture intricate patterns and temporal dependencies in network traffic data, which are crucial for detecting sophisticated and evolving botnet attacks.

Disadvantage of Existing System

- SVM can require significant memory, especially with large datasets, as it stores support vectors for classification.
- SVM is sensitive to noise in the data, which can negatively impact its performance and lead to inaccurate classifications.
- SVM struggles with scalability, particularly when dealing with large-scale datasets, as its training time increases with data size

2.3 Proposed System

The proposed project aims to develop an advanced botnet detection system using Long Short-Term Memory (LSTM) networks to classify network traffic as either normal or indicative of botnet activity. LSTM, a type of recurrent neural network (RNN), is well-suited for this task due to its ability to capture long-term dependencies in sequential data, which is essential for analyzing network traffic patterns over time. By training the model on the UNSW-NB15 dataset, which contains a variety of attack types and normal traffic, the system will be able to effectively differentiate between benign and malicious behaviors. The proposed LSTM-based model will be evaluated using key performance metrics such as accuracy, ROC AUC, and PR AUC to assess its effectiveness in identifying botnet activities. Compared to traditional methods, the LSTM approach is expected to offer enhanced performance in detecting sophisticated and evolving botnet attacks. The project will demonstrate the potential of deep learning to improve botnet detection in modern, dynamic network environments.

Advantages of Proposed System

- Efficient Handling of Sequential Data: LSTM networks are effective at processing sequential data, making them ideal for time-dependent tasks like network traffic analysis.
- LSTM networks achieve high accuracy by capturing complex patterns and dependencies in data.
- LSTMs use gating mechanisms to prevent the vanishing gradient problem, allowing them to retain long-term information

2. RELATED WORKS

Attacks on computer networks can read, damage, and steal data, which has a devastating impact on how well the system performs as a whole. Pre-intrusion actions like port scanning and IP spoofing come before attacks. Attacks are discovered by keeping track of data from source and destination IP addresses, ports, protocol specifics, header specifics, etc. [9]. Attacks can be divided into two categories: passive and active, depending on their nature. The passive attack may be network- or system-based, with the attacker covertly monitoring the network to obtain private data.

Monitoring passive attacks might be tricky. Active attackers bypass all security precautions and gain access to networks by taking advantage of security flaws, posing as a reliable system, or stealing credentials. A. CYBER SECURITY To recognize and reduce one of the biggest hazards to systems connected to the internet, cyber security is a crucial duty. Botnets are collections of hacked computers that are coordinated by a master host and used for malicious 40684 purposes like spam distribution, DDoS, and data theft. Traditional botnet detection techniques, like anomaly-based identification and signature-based approaches, have trouble identifying unknown botnets, encrypted traffic, and complex evasion strategies used by attackers. Deep learning methods, however, present a more promising strategy for overcoming these difficulties. Theauthors [10] were the first to employ machine learning for botnet traffic detection.

3. METHODOLOGY OF PROJECT

The proposed botnet detection system follows a structured methodology comprising six key modules to ensure accurate and efficient classification of network traffic. Initially, the dataset (UNSW-NB15) is loaded, which contains both normal and malicious traffic records. In the preprocessing stage, the data undergoes cleaning, normalization, and label encoding to make it suitable for model training. Feature extraction is then performed to select the most relevant attributes that contribute to effective classification. Following this, the core component—an LSTM-based deep learning model—is trained using the preprocessed and feature-optimized dataset to learn temporal patterns and relationships in network traffic.

MODULE DESCRIPTION:

Loading Dataset:

The first step of the project involves loading the dataset for botnet detection, in this case, the UNSW-NB15 dataset, which contains both normal and malicious network traffic data, including various botnet attack types. The dataset is loaded into memory for processing.

Preprocessing:

Using. Preprocessing is performed to clean and prepare the data for use in training the machine learning model. Any missing or null values in the dataset are identified and handled, either by imputing missing values with appropriate strategies or removing incomplete records. Feature values are normalized or standardized to ensure that they fall within a consistent range. This step improves the performance of machine learning algorithms by preventing any single feature from dominating the model due to large value scales

Feature Extraction:

Select and extract relevant features from the dataset that can help in detecting botnet activities (e.g., packet size, protocol type, duration). Create time-based features to capture sequential patterns in the data that may indicate botnet behavior.

Training the Model:

Define the architecture of the LSTM model, including the number of layers, neurons per layer, activation functions, and dropout layers to prevent overfitting .Choose an appropriate loss function (e.g., binary cross-entropy) and optimizer (e.g., Adam). Train the LSTM model on the preprocessed training dataset. Monitor the training process by tracking loss and accuracy over epochs to ensure the model is learning effectively.

Model Evaluation:

Evaluate the trained model on the test set using key metrics like accuracy, precision, recall, F1-score, and AUC.Use confusion matrices to further analyze the model's ability to distinguish between normal traffic and botnet attacks.

Prediction:

Classify traffic as either normal or botnet attack, based on the model's output.

4. ALGORITHM USED

The proposed project aims to develop an advanced botnet detection system using Long Short-Term Memory (LSTM) networks to classify network traffic as either normal or indicative of botnet activity. LSTM, a type of recurrent neural network (RNN), is well-suited for this task due to its ability to capture long-term dependencies in sequential data, which is essential for analyzing network traffic patterns over time. By training the model on the UNSW-NB15 dataset, which contains a variety of attack types and normal traffic, the system will be able to effectively differentiate between benign and malicious behaviors. The proposed LSTM-based model will be evaluated using key performance metrics such as accuracy, ROC AUC, and PR AUC to assess its effectiveness in identifying botnet activities. Compared to traditional methods, the LSTM approach is expected to offer enhanced performance in detecting sophisticated and evolving botnet attacks. The project will demonstrate the potential of deep learning to improve botnet detection in modern, dynamic network environments.

6. SYSTEM ARCHITECTURE

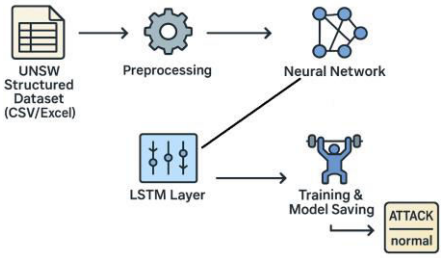
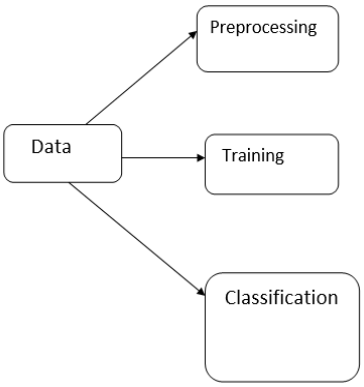


Fig: 6 SYSTEM ARCHITECTURE

The diagram illustrates a comprehensive workflow for building a cybersecurity threat detection system using the UNSW-NB15 dataset and an LSTM (Long Short-Term Memory) model. The process begins with the acquisition of the UNSW dataset, which contains labelled network traffic data representing both normal activity and various types of cyberattacks. The first step is data preprocessing, where the raw dataset is cleaned, normalized, and encoded to ensure it is suitable for machine learning. This may involve handling missing values, converting categorical features into numerical format, and scaling the data. Following preprocessing, the dataset is split into two subsets: the training dataset and the testing dataset. The training dataset is used to train an LSTM model, a type of recurrent neural network well-suited for analysing sequential or time-series data such as network traffic flows. During the training phase, the LSTM model learns to recognize patterns associated with both normal and malicious traffic. Once training is complete, the model becomes a trained model capable of making predictions. This trained model is then evaluated using the testing dataset to assess its performance in identifying threats it has never seen before. Finally, the model performs predictions, classifying new network traffic data as either benign or malicious. This entire pipeline is designed to detect network intrusions effectively and can be implemented as part of an intelligent intrusion detection system.

5. DATA FLOW DIAGRAM



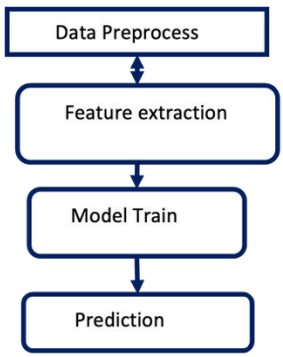


Fig: 5 Flow Diagram

7. RESULTS

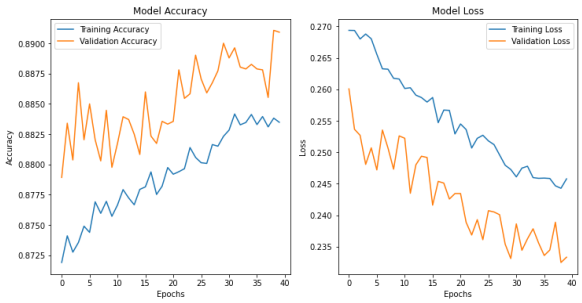


Fig 7. (a) Accuracy and Loss Model

The training and validation curves indicate that the model is learning effectively. Both training and validation accuracy improve over the epochs, while training and validation loss consistently decrease. The validation accuracy remains slightly higher than training accuracy, and validation loss stays lower than training loss, suggesting good generalization without signs of overfitting or underfitting. Overall, the model demonstrates stable and reliable performance throughout training.

.

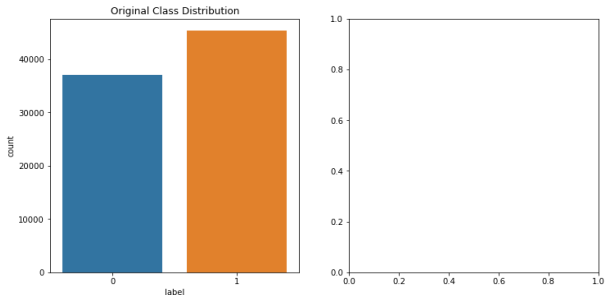


Fig 7. (b) Resampled Class Distribution

Resampled Class Distribution refers to the class balance in a dataset after applying resampling techniques like oversampling (adding minority class samples) or undersampling (reducing majority class samples) to fix class imbalance. It helps improve model performance by making classes more evenly represented.

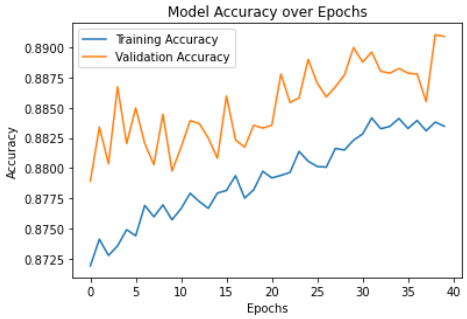


Fig 7. (c) Model Accuracy over Epochs

The plot shows the model's accuracy over 40 epochs for both training and validation data. Training accuracy increases steadily, while validation accuracy remains consistently higher and fluctuates slightly. This

indicates that the model is learning well and generalizing effectively without overfitting.

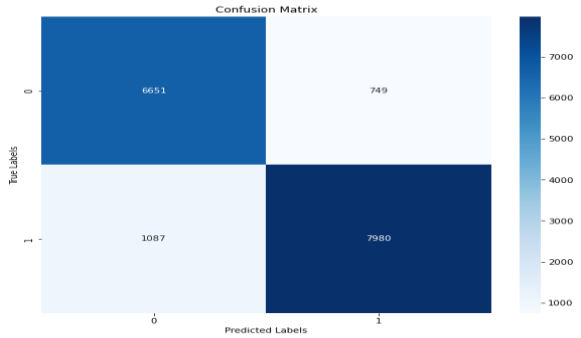


Fig 7. (d) Confusion Matrix

The confusion matrix indicates that the model performs well in distinguishing between the two classes. It correctly identifies 6,651 negative cases and 7,980 positive cases, with relatively few misclassifications—749 false positives and 1,087 false negatives. This suggests that the model has strong predictive accuracy and is effective at handling both classes with minimal errors.

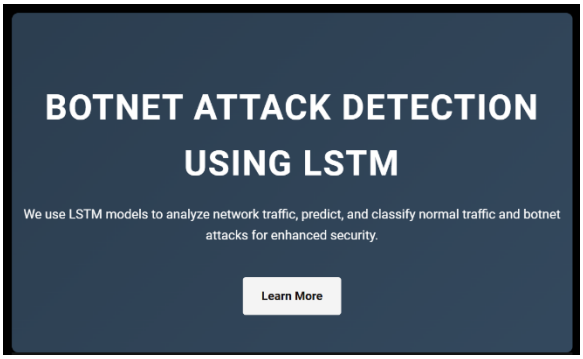


Fig 7. (e) Homepage

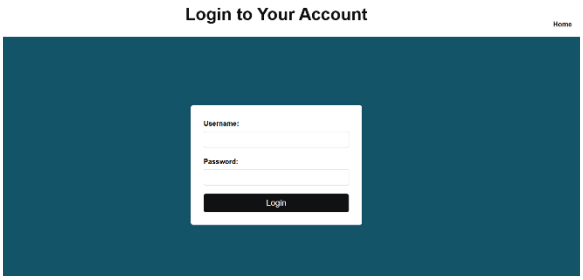


Fig 7. (f) Login Page

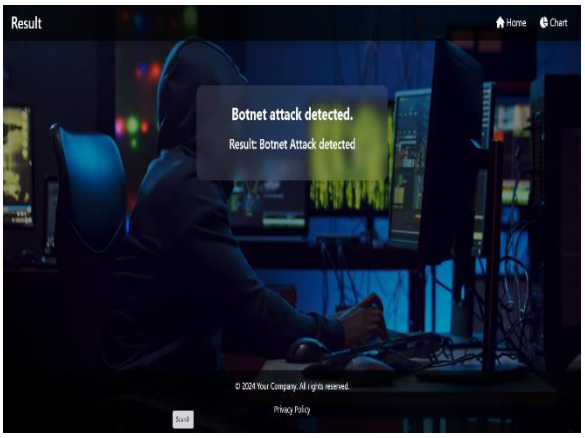


Fig 7. (g) Botnet Attack Detected

8. CONCLUSION

In conclusion, this project successfully demonstrates the potential of using Long Short-Term Memory (LSTM) networks for botnet detection in network traffic. By leveraging the sequential data processing capabilities of LSTMs, the proposed system is able to identify complex patterns indicative of botnet activities, offering a significant improvement over traditional methods like Support Vector Machines (SVM). The system, trained on the UNSW-NB15 dataset, achieved high accuracy in classifying normal traffic and botnet attacks, proving its effectiveness in real-world cybersecurity applications. The results highlight the strength of LSTMs in handling time-series data, capturing long-term dependencies that are crucial for detecting evolving threats. While the proposed model has shown promising results, there are opportunities for further refinement. Future work could focus on integrating the LSTM model with other deep learning architectures to improve detection capabilities, optimizing it for real-time applications, and expanding its ability to adapt to new and emerging botnet strategies. Additionally, improvements in feature selection, data augmentation, and scalability would enhance the system's efficiency and applicability to larger network environments. Overall, this research contributes to the growing field of cybersecurity by providing a reliable and scalable solution for detecting and mitigating botnet threats, offering enhanced protection against increasingly sophisticated cyber-attacks.

9. FUTURE ENHANCEMENT

Future enhancements for the proposed LSTM-based botnet detection system can focus on several areas to improve its performance, scalability, and adaptability. One key enhancement would be integrating the LSTM model with other advanced deep learning techniques, such as Convolutional Neural Networks (CNNs) or Transformer models, to capture both spatial and temporal patterns in network traffic more effectively. Additionally, optimizing the system for real-time

detection of botnet activities would allow for immediate responses to potential threats, reducing the latency of predictions. As botnet attacks continue to evolve, future improvements could involve updating the model with new data continuously, using techniques like transfer learning to adapt the system to emerging attack strategies. Data augmentation techniques could also help by generating synthetic traffic patterns, increasing the diversity of the training dataset and enhancing the model's ability to detect novel threats. Furthermore, enhancing feature selection methods would ensure that the model focuses on the most relevant features, reducing complexity and improving efficiency. Another important direction is improving the scalability of the system to handle large-scale networks with millions of connected devices. This could include optimizing the model to process high volumes of traffic quickly and efficiently. Combining the LSTM model with other security tools, such as Intrusion Detection Systems (IDS) or firewalls, could also provide a multi-layered defense against botnet attacks. Finally, increasing the explainability of the LSTM model would make it more transparent to cybersecurity professionals, enabling them to better understand the reasoning behind its predictions and make more informed decisions. These enhancements would further strengthen the botnet detection system, making it more robust and applicable to diverse, large-scale network environments.

10. REFERENCES

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, ''Towards the development of realistic botnet dataset in the Internet of Things for network 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 approach for botnet detection using raw network traffic 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 using hybrid deep learning approach,'' IEEE Trans. Netw. 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.

[15] N. Vo and K. Lee, ''Where are the facts? Searching for fact-checked information to alleviate the spread of fake news,'' in Proc. Conf. Empirical Methods Natural Lang. Process. (EMNLP), 2020, pp. 7717–7731.

[16] P. Patwa, S. Sharma, S. Pykl, V. Guptha, G. Kumari, M . Akhtar, A. Ekbal, A. Das, and T. Chakraborty, ''Fighting an infodemic: COVID-19 fake news dataset,'' in Proc. Int. Workshop Combating Line Hostile Posts Regional Lang. During Emergency Situation. Cham, Switzerland: Springer, 2021, pp. 21–29.

[17] L. Zadeh, ''Fuzzy sets,'' Inf. Control, vol. 8, no. 3, pp. 338–353, 1965.

[18] L. Zadeh, Fuzzy Logic. New York, NY, USA: Springer, 2023, pp. 19–49.

[19] J.-S. R. Jang, ''ANFIS: Adaptive-network-based fuzzy inference system,'' IEEE Trans. Syst. Man, Cybern., vol. 23, no. 3, pp. 665–685, Jun. 1993.

[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 networkbased 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 learningbased 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] Kumar, Anuj. "Optimization of Process Parameters in Metal Additive Manufacturing for Defect Reduction Using Machine Learning." International Journal of Engineering Research and Science & Technology, Vol. 14, No. 1, 2018, pp. 41-60
[22] M. Z. Sikder, M. A. I. Shakil, A. Ahad, M. F. Karim, B. Intakhab, and D. A. Islam, "Microwave-based detection of early-stage renal cell carcinoma using UHF range antenna," In: Proceedings of 2025 International Conference on Computer Systems and Technologies (CompSysTech); Ruse, Bulgaria. 2025, pp 1–6. https://doi.org/10.1109/CompSysTech65493.2025.11137356
[23] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.