

# Hybrid Machine Learning Model for Efficient Bonet Attack Detection

Mohd Mubashir Affan<sup>1</sup>, Mohammed Thouheeduddin<sup>2</sup>, Ahmed Khan<sup>3</sup>, Mrs. Imreena Ali<sup>4</sup>

<sup>1,2,3</sup>B.E student, Department of CSE, ISL engineering college

<sup>4</sup>Associate Professor PhD, Department of CSE, ISL engineering college

## ABSTRACT

With the rapid development of Internet technology, 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.

## INTRODUCTION

The modern travel industry is undergoing a significant transformation driven by advances in digital technology and increasing user

expectations for personalized and seamless experiences. As travel becomes more accessible, users are no longer satisfied with generic information or rigid tour packages. Instead, they seek platforms that understand their preferences, provide real-time insights, and help plan trips effortlessly.

Traditional travel platforms often fall short in delivering personalized content. They depend heavily on static information, user reviews, or manual itinerary creation, which may be outdated or irrelevant. This results in a fragmented user experience, requiring travelers to switch between multiple apps or websites to fulfill different travel needs such as booking accommodations, exploring attractions, or finding restaurants.

To address these limitations, this project proposes the development of a comprehensive AI-powered web and mobile platform that functions as a One stop travel companion with AI powered destinations insight. This platform aims to combine intelligent trip planning, real-time destination insights, personalized recommendations, and end-to-end booking features into a single intuitive application. By leveraging artificial intelligence technologies like Natural Language Processing (NLP) and machine learning, the system will provide a truly adaptive and enriched travel experience.

## LITERATURE REVIEW

Overview of Travel Planning Platforms

Growing IoT Vulnerabilities: Growth in IoT networks has resulted in an increase in botnet attacks, and hence research has been undertaken into smart detection mechanisms.

Hybrid Deep Learning Models:

Mudasir Ali et al. (2024) introduced an ACLR model (ANN + CNN + LSTM + RNN) with 96.98% accuracy and good generalization capabilities using the UNSW-NB15 dataset.

Shiba et al. (2024) used LSTM Autoencoders and MLP, achieving 99.77% accuracy on big IoT datasets (N-BAIoT2018, UNSW-NB15)  
Real-Time Device-Specific Detection:

Alzahrani and Bamhdi (2021) employed a CNN-LSTM model to identify BASHLITE and Mirai

attacks on IoT cameras with an accuracy of up to 94%, proving deployment feasibility in the real world.

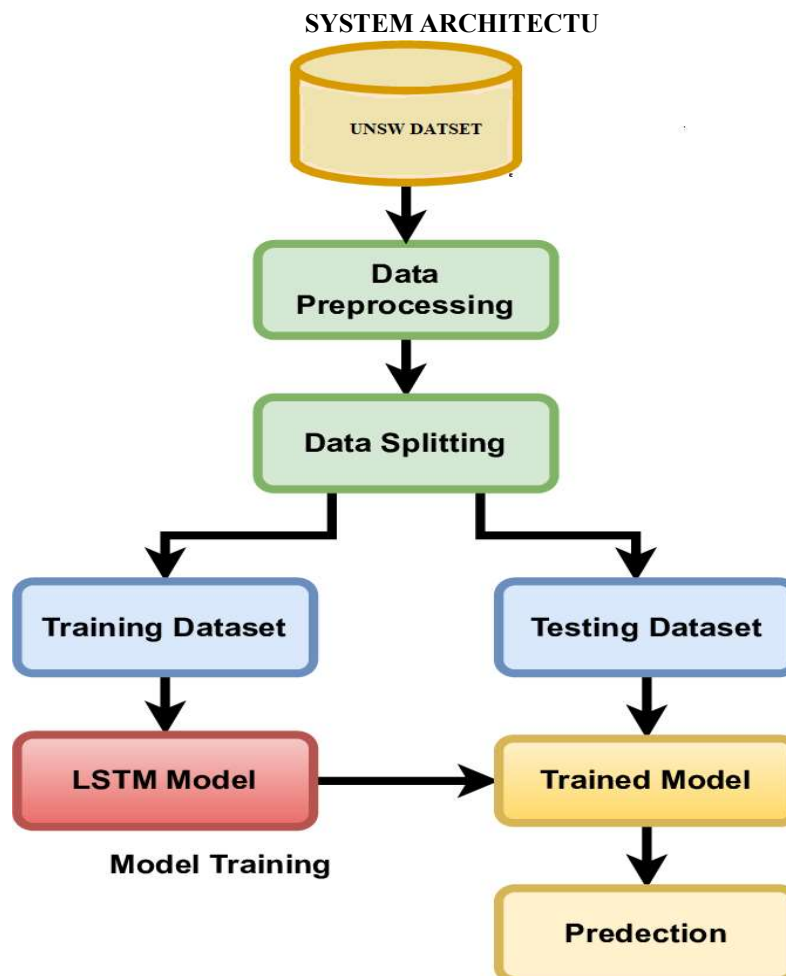
Optimization-Improved Models:

Balaganesh et al. (2023) employed Bi-GRU and RNN with a new SMIE optimizer, with which 97% accuracy was achieved, beating many existing models.

Traditional Machine Learning Methods:

Khalid Alissa et al. (2022) used models such as Decision Trees and XGBoost with SMOTE preprocessing, achieving a highest accuracy rate of 94%, demonstrating that traditional models are still valid when tuned correctly.

General Trend: The literature indicates a trend toward hybrid and optimized deep learning models for enhancing detection accuracy, generalizability, and adaptability in heterogeneous IoT environments.

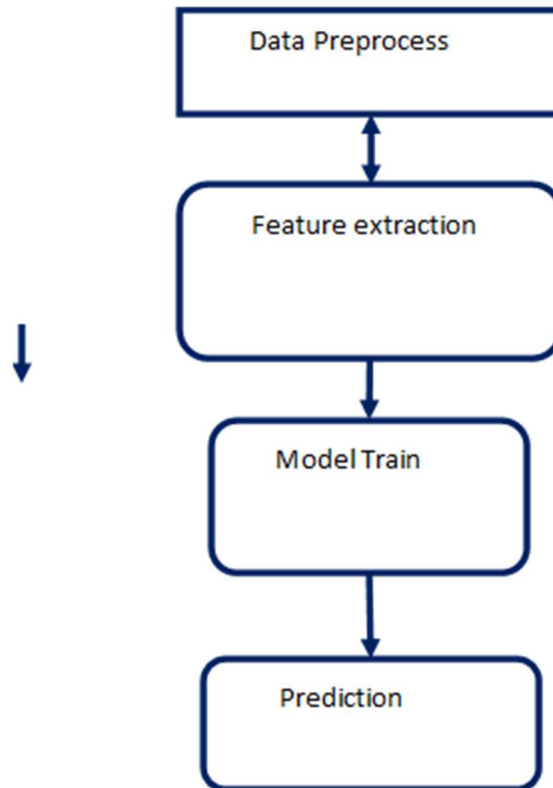


### DATAFLOW DIAGRAM

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured

design).

A DFD shows what kinds of data will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.



### IMPLEMENTATION

This is a Flask web app that is built to identify botnet attacks in network traffic with the aid of a pre-trained LSTM model. The app starts with a simple login, in which the users are required to log in using given credentials. After successful login, they are taken to an input page and enter 15 network features like bytes, sload, dload, and flags like is\_ftp\_login. These inputs are gathered from the form, normalized into a NumPy array, scaled by a preloaded scaler (scaler.pkl), and reshaped according to the input format needed by the LSTM model. The model (lstm\_model.h5) proceeds to predict whether the traffic represents a normal connection or a botnet attack. Depending on the prediction, a proper result

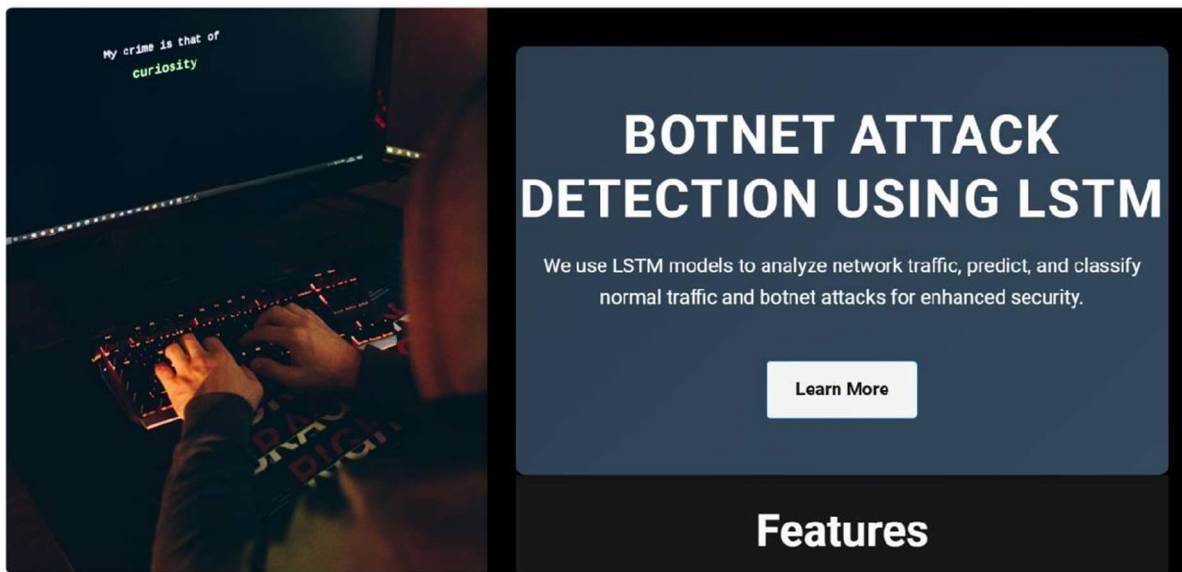
message and attack type are placed in the session. The users are then redirected to the result page showing the prediction result. The app also has other routes for rendering the chart visualizations and an about page. This implementation in total gives a total simple yet functional interface for detecting botnet attacks in real time with machine learning.

that the system meets functional expectations. In the context of data synchronization, it includes checking packet acknowledgements, routing operations, and node status updates.

Finally, a test plan is developed by dividing the project into smaller units, each with its testing strategy. This helps in identifying and fixing bugs in specific components before moving forward with

integration, thereby improving the overall reliability of the system.

## RESULTS



**BOTNET ATTACK  
DETECTION USING LSTM**

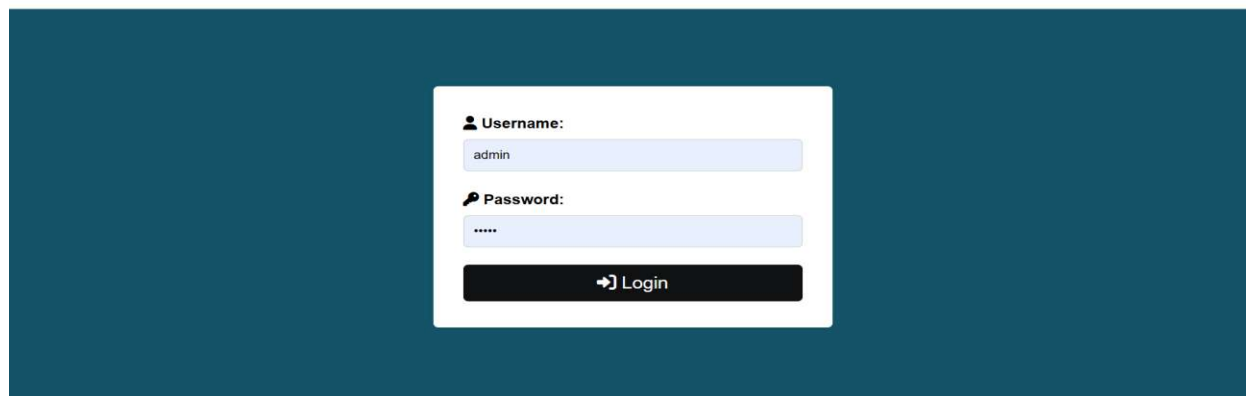
We use LSTM models to analyze network traffic, predict, and classify normal traffic and botnet attacks for enhanced security.

[Learn More](#)

**Features**

 **Login to Your Account**

 [Home](#)



**Username:**

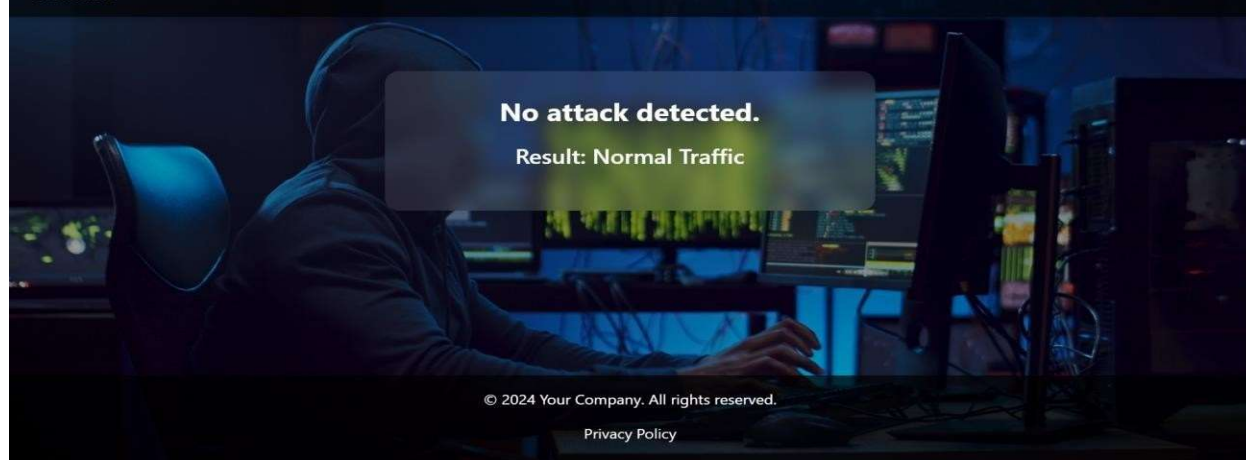
**Password:**

[Login](#)

**Result**

 [Home](#)

 [Chart](#)



**No attack detected.**

Result: Normal Traffic

© 2024 Your Company. All rights reserved.

[Privacy Policy](#)

### 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.

### 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.

### REFERENCE

- [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. Homaoun, 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 24<sup>th</sup> 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.
- [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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] T. H. H. Aldhyani and H. Alkahtani, "Attacks to automotous vehicles: A deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, p. 360, Jan. 2022.
- [18] Nausheen Fathima, Dr. Mohd Abdul Bari, Dr. Sanjay, "Efficient Routing in Manets that Takes into Account Dropped Packets in Order to Conserve Energy", *International Journal Of Intelligent Systems And Applications In Engineering*, IJUSEA, ISSN:2147-6799, Nov 2023
- [19] Afsha Nishat, Dr. Mohd Abdul Bari, Dr. Guddi Singh, "Mobile Ad Hoc Network Reactive Routing Protocol to Mitigate Misbehavior Node", *International Journal Of Intelligent Systems And Applications In Engineering*, IJUSEA, ISSN:2147-6799, Nov 2023
- [20] ) Ijteba Sultana, Dr. Mohd Abdul Bari, Dr. Sanjay, "Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes", *International Journal of Intelligent Systems and Applications in Engineering*, ISSN no: 2147-6799 IJISAE, Vol 12 issue 3, 2024, Nov 2023