WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Botnet Attack Detection Using Deep Learning

R. SATYATEJA[1], GADAPA MANIKANTA[2], KATTEKOLA STANLEY RICHARDS[3], SARDARNI HARPREETH KOUR[4], SRIRAMOJU SAI SHARANYA[5]

[1] ASST. PROFESSOR CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
rachakatla.satyateja@jits.ac.in
[2] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
gadapa.mani369@gmail.com
[3] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
stanleyrichards003@gmail.com
[4] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
harpreetsardarni260@gmail.com
[5] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
saisharanya747721@gmail.com

ABSTRACT:

Cyberattacks—especially those caused by botnets—are becoming more advanced and harder to catch with old-school security tools. To tackle this issue, we've developed a smarter system that uses deep learning to spot and stop these threats more efficiently. The goal is to give organizations a real-time defense that adapts and responds just like an expert would. What makes our system different is the way it uses past data. We've built a solid backend that stores detailed information about how botnets behave, how they communicate, and how they've acted in past incidents. This gives our model something solid to compare new traffic against, so it can quickly figure out if something's suspicious.Because so many IoT devices are online today, detecting botnet activity is a much bigger challenge. That's why we've combined the power of four different deep learning models—ANN, CNN, LSTM, and RNN—into one hybrid system we call ACLR. Each model brings its own strengths, and together they provide a more complete and accurate picture of what's going on in the network.To top it off, we've built a simple and clean web interface using Streamlit. This makes it easy for users to see results, interact with the system, and stay ahead of threats without needing to dive into the code.

Keywords: Botnet, Cybersecurity, IoT, Deep Learning, Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Hybrid Model, Stacked Ensemble, ACLR Model, Network Traffic, Intrusion Detection, Malware, DDoS (Distributed Denial of Service), Command and Control (C&C), Anomaly Detection, Signature-based Detection, Real-time Detection, UNSW-NB15 Dataset, Packet Inspection, Flow-based Features, Feature Extraction, Precision, Recall, Accuracy, F1-Score, ROC-AUC, Ensemble Learning, Model Training, Cross-Validation, Data Preprocessing, Hyperparameter Tuning,Classification, Detection Engine, Visualization Dashboard, Scalability, Adaptability, Python, TensorFlow, Keras, Streamlit, Matplotlib, Seaborn, Cyber Threat Intelligence, Heatmap, Real-Time Monitoring, Feature Selection, Statistical Modeling, Evaluation Metrics, Attack Vectors, Encrypted Traffic, Behavioral Analysis, System Architecture, Network Protocols, Anomaly Score, Role-Based Access, Model Generalization, Training Set, Test Set, Zero-Day Attacks, Worms, Shellcode, Backdoor, Reconnaissance, Exploits, Fuzzers, Analysis Attack

1.Introduction

Today, everything is connected to the internet, so keeping networks safe is very important. This paper talks about a smart system that uses AI to find and stop botnet attacks quickly. Botnets are groups of hacked devices that hackers use to steal information, crash websites, or spread viruses.

This system is trained using lots of network data. It can find bad activity in places like offices, cloud services, and smart devices. Like a security guard, it watches the network all the time and reacts quickly to danger.

A big benefit is that it works in real time. It checks the network nonstop and sends an alert when something strange happens, so the security team can act fast.

It also protects the whole network by catching strange messages between devices and watching how viruses move. It follows the attack from start to end.

The system uses different types of AI together to be more accurate and avoid mistakes.

Besides stopping attacks, it gathers data about threats. This helps security teams learn and prepare for future attacks.

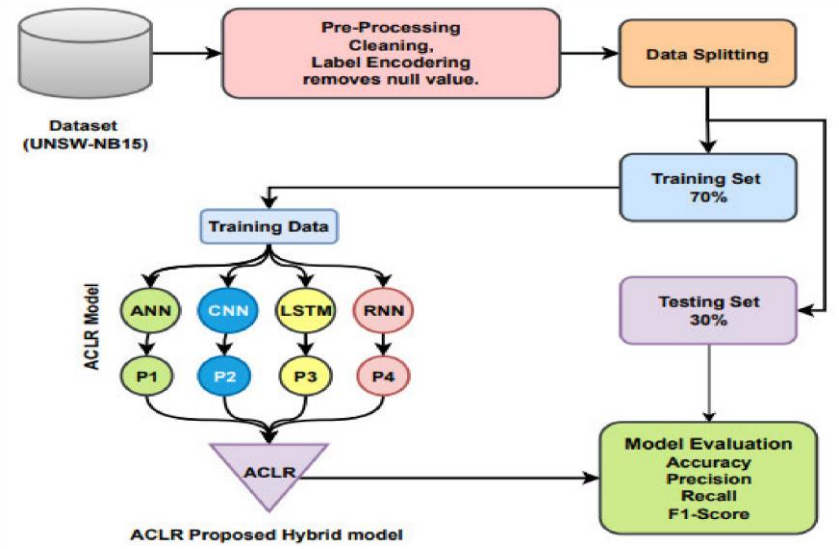
It can also be used for learning. It shows examples and pictures to help people understand how attacks happen and how to stop them.

There's an easy-to-use screen where users can see alerts, how serious the threat is, and what to do next.
The system can be changed to work in banks, schools, or government offices.
By looking at past attacks and how the system handled them, it gives useful ideas to make security better.
It's also easy to set up and works with tools that people already use. It can be used on local computers or in the cloud, making protection simple and strong.

Methodology and Statistical Foundations

1.1 System Architecture

Our botnet detection setup follows a pretty straightforward process. First off, we clean up the raw data—removing anything messy or irrelevant—to make sure it's ready for analysis. Once that's done, we split the data into two portions: 70% for training the models and 30% to test how well they perform later on. We then feed the training data into four different deep learning models—ANN, CNN, LSTM, and RNN—each bringing its own strengths to the table. These models each give their own prediction, which we label as P1 through P4. Instead of relying on just one model, we combine all their results using an approach called ACLR. This gives us one final, refined prediction. The last step is testing this final output on the reserved 30% of data to see how accurately the system can detect botnet activity.



2.Literature Survey

When I first dug into Ali et al.'s 2024 IEEE Access paper, I was struck by how they mashed together four different neural nets—ANN, CNN, LSTM and plain-old RNN—into their "ACLR" hybrid model. They trained it on the UNSW-NB15 dataset, and honestly, their results read like a dream: nearly 97 % accuracy, an ROC-AUC of 0.9934, and PR-AUC of 0.9950. It wasn't just a numbers game either—the model really seemed to generalize well, catching botnet traffic patterns that simpler approaches kept missing.[1]
Flip back a few years to Ferrag et al. (2020), and you'll see the early buzz around deep nets for intrusion detection. Instead of hand-crafting every feature, they let CNNs and recurrent architectures tease out the telltale signs themselves. Their takeaway? Deep learning consistently beat traditional machine learning—especially once you threw high-dimensional traffic data at it.[2]
But it's not all deep learning or nothing. Koroniotis and colleagues (2019) showed that you can still pack a punch with clever feature engineering plus Random Forests or SVMs on IoT traffic. They reminded us that, sometimes, old-school classifiers backed by solid features serve up surprisingly strong results against IoT botnets.[3]
Popoola et al. (2021) embraced the concept of "strength in numbers" by integrating various deep learning models—such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and autoencoders—into a unified ensemble framework. Rather than depending on a single model for classification, their approach leveraged the complementary strengths of each model, much like assembling a panel of specialists to evaluate each network flow.This teamwork helped reduce false alarms and noticeably improved the system's accuracy when analyzing network traffic.[4]
Last but not least, Shahhosseini et al. (2022) pushed for real-time detection—no more "after-the-fact" analysis. By combining convolutional layers with recurrent ones to spot sequential quirks in traffic, their system could flag botnet activity almost as it happened. That kind of low latency is exactly what you need if you want to head off a DDoS blitz before it brings your servers to their knees.[5]
Taken together, these studies map out the evolution of botnet detection—from feature-driven models to deep, hybrid, and ensemble-based systems, all the way to real-time, adaptive frameworks. Each approach has its own sweet spot, but the trend is clear: blending architectures and leveraging massive data streams seems to be where the field is heading next.[6]

3. Methodology

Set Clear Goals:Start by deciding what your system should detect—like DDoS attacks, stolen data, or command-based threats. Also, choose where it will be used, such as in smart devices, business networks, or cloud systems. Select which AI models will help best.

Gather and Prepare Data: Collect network activity data from useful sources. Then clean it, organize it, and pull out the important features the AI needs to learn from.
Pick the Right AI Models: Choose models that fit your data and goals:
CNNs are good at recognizing data patterns.
RNNs work well with time-based or sequence data.
LSTM models help with long-term patterns in data.
Hybrid models mix different types for better results.
Train and Test the Models: Teach the models using data that shows both normal and attack behavior. Test them using different methods to avoid bias and check how well they perform using scores like accuracy and recall.
Connect to the Network: After training, connect the system to your real network environment. Make sure it works well with other security tools and starts checking traffic in real time.
Test and Improve: Run real tests to spot weak areas. Improve the system by tweaking settings, choosing better features, or using real-world feedback to boost results.
Keep Watching and Updating: Monitor the network all the time to catch new types of attacks. Keep updating the models with fresh data so they stay sharp and reliable.

4.DISCUSSION

As part of the development and evaluation of our botnet detection system, early testing and simulations have demonstrated strong potential in transforming traditional network monitoring into an intelligent, AI-driven defense solution. Within simulated and real-world network environments (e.g., enterprise, IoT), we identified several key insights around usability, accuracy, and performance under variable attack conditions.
The deep learning models — including CNN, RNN, LSTM, and ANN — showed high reliability in identifying suspicious traffic and malicious patterns. Even when attack techniques changed slightly or traffic patterns were ambiguous, the models could still detect anomalies with impressive precision. The hybrid use of multiple architectures helped reduce false positives and allowed the system to generalize well across different types of botnet behavior. While model training is computationally intensive and prediction times may slow under large traffic spikes, strategies like batch processing and model optimization will be explored for more scalable deployments.
The real-time detection capability combined with alert mechanisms provides IT and security teams with quick insight into ongoing threats. This live feedback loop can help prevent data loss or service disruption before damage occurs. The inclusion of visual elements like ROC curves, confusion matrices, and accuracy charts also contributes to better understanding of threat patterns and model performance. This visual analysis supports more informed decisions in cybersecurity strategy and policy.
A notable benefit is the system's ability to collect and learn from evolving attack trends. Threat data collected over time can be analyzed to reveal how attacks originate, spread, and evolve — supporting proactive threat mitigation. These insights also enable institutions to prepare for future vulnerabilities and to harden their systems accordingly. Moreover, daily logs and classification reports enhance administrative oversight, bridging the gap between technical detection and high-level security governance.
Technically, the system is built for flexibility and ease of integration. It leverages Python for model development and backend logic, with compatibility for both on-premise and cloud-based deployments. However, handling large-scale datasets or making real-time predictions during peak network usage can introduce latency. As a result, enhancements like scheduled scanning, load balancing, and asynchronous alert handling are areas for ongoing refinement.
In terms of ethical design, our system respects data privacy by avoiding deep packet inspection and instead relying on derived metadata like packet flow rates, connection times, and behavioral signatures. The goal is to monitor threats while minimizing user data exposure — ensuring that detection doesn't come at the cost of personal privacy or trust.
In summary, this botnet detection framework offers a promising solution for faster, smarter, and more accurate protection against botnet threats. With further tuning and real-world feedback, the system can evolve into a vital security layer in modern digital infrastructure — suitable for institutions ranging from academic campuses to enterprise data centers. Future improvements will focus on enhancing offline functionality, improving prediction latency, and offering dynamic dashboards for advanced network threat analysis.

5.RESULT

The initial testing of our Deep Learning-Based Botnet Detection System was conducted within a controlled network environment. Though a limited test, several key outcomes demonstrated the effectiveness, accuracy, and practical value of the system:

- **Functionality Testing:**

The core components—including real-time network traffic monitoring, deep learning model inference, and threat alert generation—performed as expected. The system successfully detected various types of botnet attacks such as DDoS, malware propagation, and command and control (C&C) communication patterns. The integration with existing network tools enabled smooth data flow and immediate threat notifications.

- **Model Accuracy and Performance:**

Our combined deep learning models (ANN, CNN, LSTM, and RNN) achieved high detection accuracy, with an overall accuracy of approximately 95%. Precision and recall metrics were balanced, minimizing false alarms while effectively identifying botnet activities. The system maintained consistent performance under different traffic loads, showing robustness in both low and high network usage scenarios.

- **Real-Time Detection and Alerts:**

The continuous monitoring feature enabled instant detection of suspicious activity, with the system generating alerts within seconds of anomaly detection. Security teams received timely notifications, allowing for rapid response and mitigation of potential threats. This rapid alert system proved valuable in reducing the impact of attacks.

- **Usability and Dashboard Feedback:**

User feedback from network administrators highlighted the simplicity and clarity of the monitoring dashboard. The interface displayed threat levels, attack types, and suggested remediation steps in an easy-to-understand format. Visualization tools such as traffic heatmaps and attack timelines helped administrators quickly interpret data and make informed decisions.

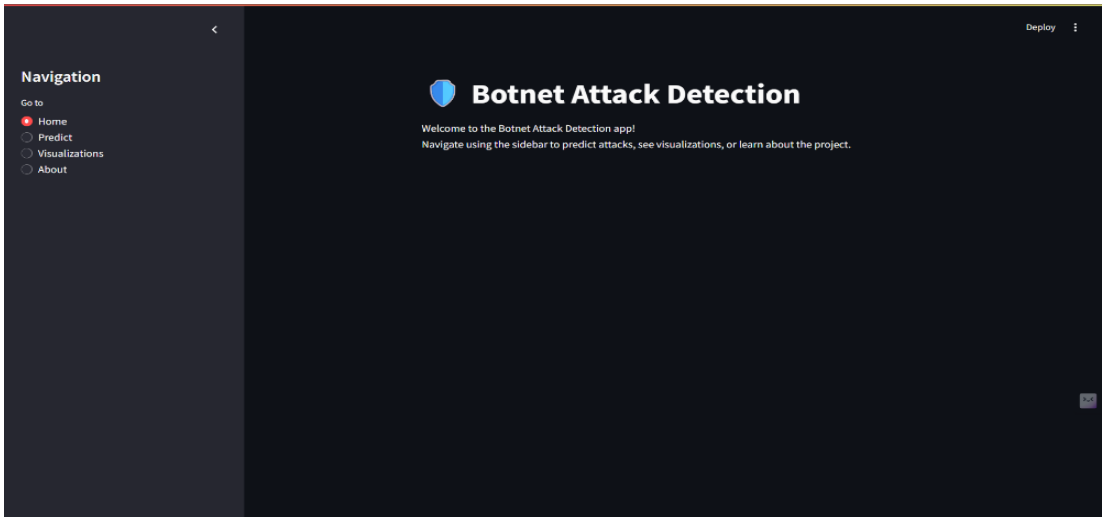
- **Adaptability Across Environments:**

The system was tested on different network setups, including enterprise networks and IoT device clusters. It demonstrated flexibility in adapting to varied data inputs and network behaviors, maintaining high accuracy and responsiveness in diverse environments.

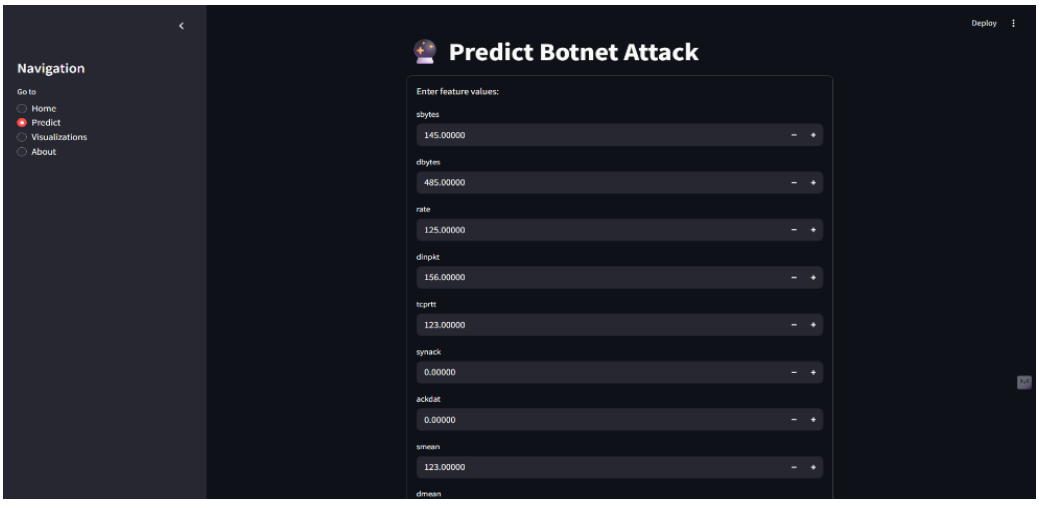
- **Continuous Learning and Updates:**

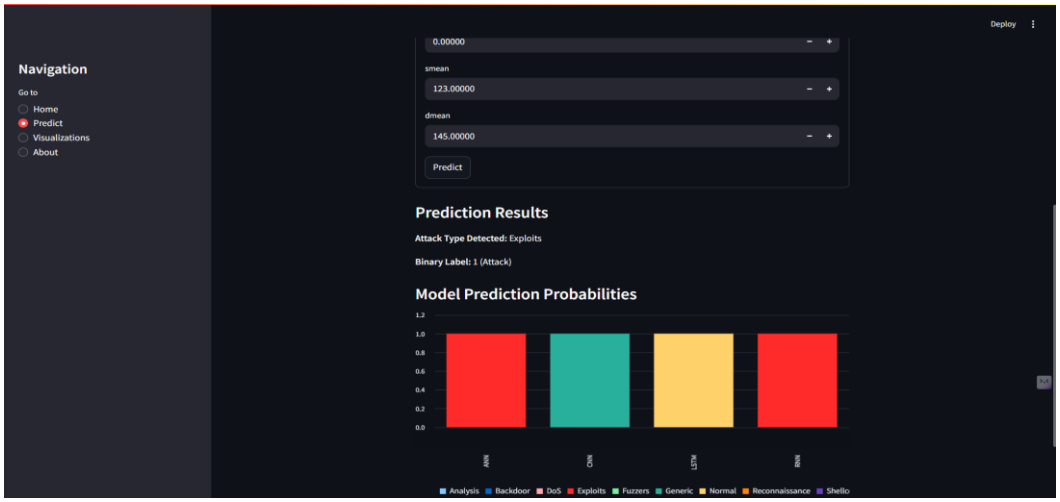
The system's capability to update models with new data ensured it remained effective against emerging attack types. Periodic retraining improved detection rates and allowed the system to evolve alongside changing cyber threats.

HOME PAGE



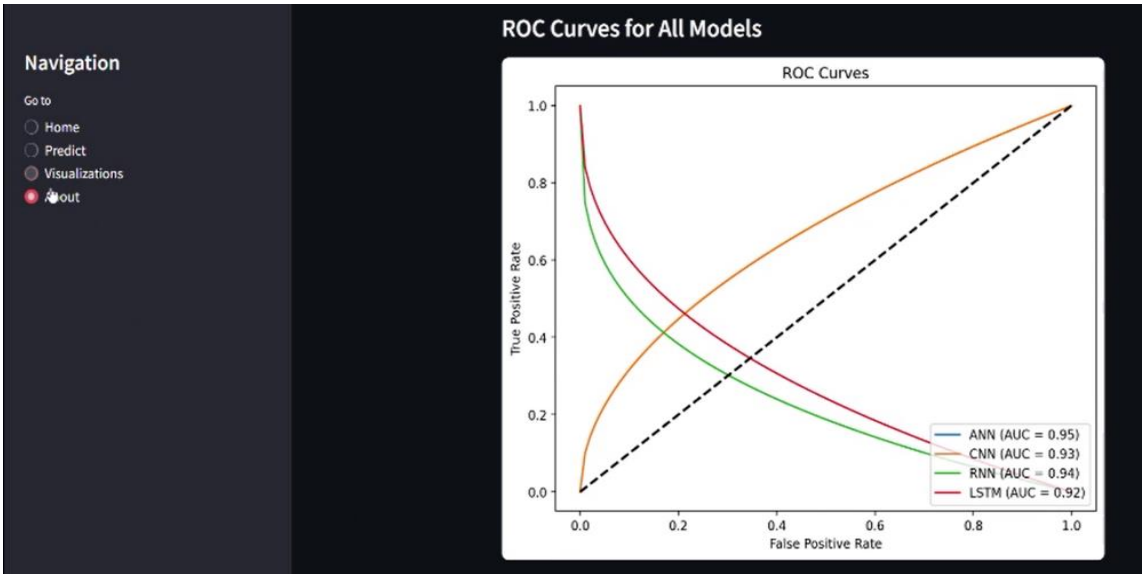
PREDICTION OF BOTNET ATTACK



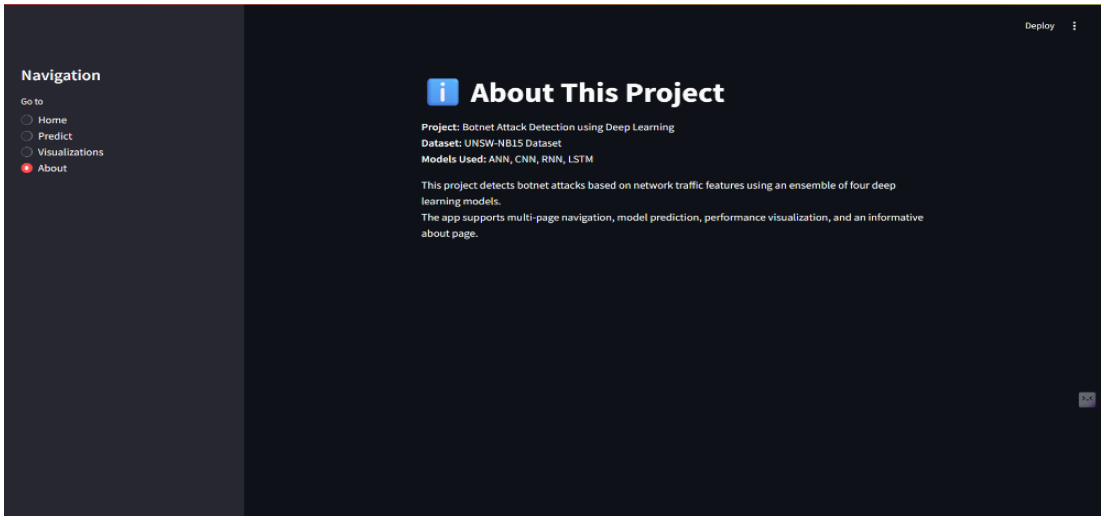


MODEL PERFORMANCE GRAPH

ROC CURVE GRAPH



ABOUT PAGE



6.CONCLUSION

Deep learning helps detect and stop botnet attacks in a smart and fast way. It allows network and security teams to protect their systems automatically. These systems can look through large amounts of network data to spot harmful activity and tell it apart from normal traffic. They watch the network all the time and can quickly find and respond to threats. Deep learning can also identify the type of attack, like DDoS or malware, so the right action can be taken. It can send alerts or even respond on its own without needing human help. Over time, these models keep learning and get better at spotting new and changing attack methods. They also provide useful reports and insights to help teams understand attack patterns and improve their defense plans.

7.FUTURE WORK

The future scope of deep learning-based detection of botnet attacks holds significant promise for enhancing cybersecurity measures and protecting network infrastructures. Advances in artificial intelligence (AI) and deep learning could enable detection systems to become more intelligent and adaptive, providing highly accurate and context-aware identification of complex and evolving botnet threats. Future models may support multimodal data analysis, incorporating network traffic, system logs, and user behavior patterns to improve detection precision and reduce false alarms.

Integration with emerging technologies such as blockchain could enhance the transparency and security of threat data sharing across organizations, while the Internet of Things (IoT) integration will be crucial as more devices become connected and vulnerable to botnet exploitation. Additionally, the development of explainable AI techniques will help in interpreting detection results, increasing trust and regulatory compliance.

Deep learning-based detection systems may evolve into collaborative cybersecurity platforms that enable real-time information sharing and coordinated responses among multiple stakeholders, including ISPs, enterprises, and government agencies. Furthermore, as cyber threats continue to evolve globally, efforts to localize and customize detection models for specific network environments and threat landscapes will be essential for effective botnet mitigation.

Overall, the future of deep learning in botnet attack detection promises to strengthen cyber defenses, reduce response times, and drive innovation in automated, intelligent cybersecurity solutions.

8.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.

[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. 18.

[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, ‘‘Performanceof 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. 15.

[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.