IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTING INTRUSIONS INTO IOT BOTNETS WITH HYBRID ML

Dasam Venila Ravya[1], SESHA GIRI RAO THALLURI [2]

#1M.tech Specialization:- Computer Science and EngineeringDepartment of CSE. Bonam Venkata Chalamayya Engineering College,Odalarevu , Konaseema Dist -533217 (A.P), vanillaravya@gmail.com

#2Associate Professor,Bonam Venkata Chalamayya Engineering College,Odalarevu Allavaram Mandal, Konaseema Dist - 533217 (A.P)

Abstract: Effective detection has become a critical challenge due to the rise of IoT devices, which has led to an increase in botnet attacks. This research extends traditional botnet detection models by incorporating advanced ensemble deep learning techniques to improve prediction accuracy. We integrate CNN, LSTM, and GRU in hybrid architectures such as CNN + LSTM + GRU and CNN + BiLSTM + GRU, which effectively capture both spatial and temporal patterns in IoT network traffic. Feature selection using Mutual Information optimises model performance, reducing computational complexity while improving detection efficiency. Additionally, a Flask is used to create a user-friendly front-end application, which allows for smooth testing and evaluation of the model. Secure user authentication protects sensitive information and ensures data integrity. The experiment's findings demonstrate that the suggested ensemble models achieve superior accuracy, surpassing 97%, in detecting botnet activity, highlighting their effectiveness in securing IoT environments.

Index terms *- Botnet Detection, IoT Security, Deep Learning, CNN, LSTM, GRU, Hybrid Models, Ensemble Learning, Feature Selection, Mutual Information, Flask Framework, User Authentication, Cybersecurity.*

1. INTRODUCTION

Many sectors have seen a change thanks to the rapid expansion of IoT devices, which have made automation and seamless communication possible. IoT networks are becoming a popular target for cyberthreats, especially botnet assaults, as a result of their broad use. Botnets coordinate huge assaults, such as DDoS attacks, data breaches, and malware distribution, by taking advantage of flaws in connected devices. More sophisticated and adaptable detection procedures are required since traditional botnet detection approaches that depend on signature-based and heuristic techniques are unable to keep up with the changing nature of botnet assaults.

By using sophisticated DL models in an ensemble context, our study expands on current botnet detection techniques to solve these issues. The suggested method extracts temporal and spatial correlations from network traffic data using CNN, LSTM, and GRU. By integrating their respective architectural strengths, CNN + LSTM + GRU and CNN + BiLSTM + GRU

hybrid models increase detection accuracy. Furthermore, Mutual Information feature selection maximises model performance, guaranteeing effective handling of massive IoT traffic while reducing computational overhead.

In addition to increasing detection accuracy, this study presents a Flask for developing an intuitive front-end application. This interface incorporates safe authentication measures to protect sensitive data while enabling users to test and assess model performance with ease. A thorough method for identifying botnet attacks in IoT is ensured by the combination of deep learning and workable deployment methods. The experiment's findings demonstrate that the suggested ensemble models are successful in reducing cyberthreats and improving IoT security, with an accuracy rate of over 97%.

2. LITERATURE SURVEY

i) Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks

https://www.sciencedirect.com/science/article/pii/S0952197623006164

The Internet of Things is susceptible to security risks like DDoS assaults because it is made up of intricate networks of low-resource sensors, gadgets, and things. SDN appears to offer more efficient security and access control. ML-based security frameworks may analyse IoT device behaviour and generate a profile to help decision makers protect the environment. Here, we examine how machine learning may be used by an SDN-WISE IoT controller to identify DDoS assaults. Through SDN-WISE controller logging, a pre-processed log file including network logs is published into a dataset. The machine learning DDoS detection module of the SDN-WISE controller classifies packets in SDN-IoT networks using DT, SVM, and Naive Bayes. We perform traffic simulation scenarios in order to assess the proposed architecture and compare the outcomes of the machine learning DDoS detection module. The attack detection module uses 30% of the CPU and RAM and saves 70% of the memory while processing 48 packets of SD-IoT network data per second with a 97.2% accuracy rate. Our results show that the proposed method is more effective in identifying DDoS assaults in SDN-WISE IoT scenarios. The suggested strategy may result in fewer DDoS assaults and enhanced IoT network security.

ii) Deep learning-based classification model for botnet attack detection

https://link.springer.com/article/10.1007/s12652-020-01848-9

Botnets allow criminals to take over a huge number of computers and commit crimes. Numerous methods have been demonstrated by researchers to detect botnets in real time. These solutions struggle to keep up with the continuous evolution of botnets. The proposed model is trained and evaluated on the CTU-13 dataset using several neural network topologies and hidden layers. The results showed that the DL artificial neural network model could successfully identify botnets.

iii) Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks

https://ieeexplore.ieee.org/abstract/document/9241019

Usually, a significant quantity of memory and network traffic data are needed. DL implementation is nearly impossible for IoT devices with little memory. This article uses LAE encoding to minimise the feature dimensionality of large-scale IoT network traffic data. To show the effectiveness of the hybrid DL approach, we use deep bidirectional LSTM to analyse the long-term associated changes of LAE's low-dimensionally assessed in order to categorise samples of network traffic. LAE caused a reduction in storage memory of 18.92–27.03 percent in the feature dimensionality reduction approaches. Both underfitting and

overfitting are avoided by the deep BLSTM model, even with a significant decrease in feature size. It also performs well in binary and multiclass classification.

iv) Network Flow based IoT Botnet Attack Detection using Deep Learning

https://ieeexplore.ieee.org/abstract/document/9162668

Governments throughout the world have pushed to embrace smart city apps as a way to improve city living. Applications for internet-enabled technologies in smart cities are numerous and include traffic control, water treatment, power grid, healthcare, and more. Botnet assaults have increased as a result of the spread of IoT devices. We provide a DL botnet detection technique that makes use of network traffic patterns to improve cyber security for Internet of Things devices and smart city applications. By converting network traffic flows into connection records, the botnet detection framework use a DL model to detect botnet attacks from hacked IoT devices. Extensive testing on both well-known and recently released benchmark data sets determines the best DL model. Visualising datasets is one method of understanding them. The suggested DL model did rather well in comparison to ML models.

v) A State-of-the-Art Review on IoT botnet Attack Detection

https://arxiv.org/abs/2010.13852

The Internet of Things is one of the many interconnected networks that make up the contemporary Internet. IoT devices are particularly vulnerable to security breaches, particularly botnet attacks, because to their adaptability and vulnerability. This research will concentrate on conceptual frameworks for Internet of Things botnets and machine learning techniques for botnet detection. This study evaluates botnet detection systems using the Bot-IoT Dataset, a real-world IoT dataset that contains both historical data and fictitious assaults..

3. METHODOLOGY

i) Proposed Work:

By utilising cutting-edge deep learning algorithms in conjunction with an easy user interface for practical implementation, the suggested approach improves botnet attack detection in IoT contexts. It analyses IoT network traffic by combining many deep learning architectures, such as CNN, LSTM, and GRU. The system efficiently incorporates both spatial and short-term dependencies by utilising hybrid models like CNN + LSTM + GRU and CNN + BiLSTM + GRU, enhancing detection robustness and accuracy.

In order to maximise the performance of the model, Mutual Information reduces computing complexity by examining network data to determine which factors are most important. Through the combination of outputs from several models, the ensemble learning technique improves prediction accuracy even further. This findings are a very efficient detection system capable of recognising botnet activity with over 97% accuracy.

A user-friendly front-end application that offers a smooth interface for model testing and assessment was also made with Flask. Secure user authentication is included into the system to safeguard private information and guarantee restricted access. Network security and resilience against cyber attacks are improved by this comprehensive and scalable IoT botnet detection system, which combines deep learning with a useful deployment architecture.

ii) System Architecture:

In IoT contexts, the system architecture for botnet detection is set up to guarantee efficient feature selection, data processing, model training, and

performance assessment. The UNSW-NB15 dataset, which includes binary and multi-class attack labels, is used as the starting point for the procedure. To ensure consistency for additional research, this dataset is cleaned and normalised using data preparation.

The data undergoes label encoding after preprocessing, which transforms categorical attack types into numerical representations that deep learning algorithms can understand. In order to help in feature selection, data visualisation techniques are used concurrently to comprehend patterns and relationships within the collection.

In order to maximise model performance, the feature extraction and selection process is essential. Mutual Information-based selection improves computer performance while reducing background noise by identifying relevant network traffic aspects. Deep learning models may be trained with the use of a training set and a validation set.

An ANN, CNN, LSTM, and RNN are among the DL models used for the detection procedure. Furthermore, by capturing both spatial and temporal relationships in network data, hybrid models such as CNN + LSTM + GRU and CNN + BiLSTM + BiGRU are presented to increase detection accuracy. The chosen characteristics are used to train these models, and their efficacy is assessed.

Lastly, to guarantee high detection reliability, the model's performance is assessed using metrics including accuracy, precision, recall, and F1-score. An effective and scalable solution for real-world botnet detection in IoT networks is subsequently provided by integrating the learnt models into a deployment framework.

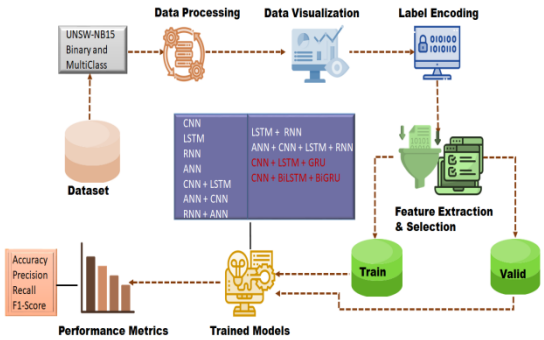


Fig.1. Proposed Architecture

iii) MODULES:

a) Dataset Collection

- The system utilizes the UNSW-NB15 dataset, which contains both binary and multi-class attack types. This dataset serves as the foundation for training deep learning models to detect malicious network activities.

b) Data Processing

- The raw dataset undergoes preprocessing to clean and normalize network traffic data, ensuring consistency and removing redundant information. This step is crucial for improving model performance.

c) Label Encoding

- Attack categories are converted into numerical values using label encoding, enabling deep learning models to process categorical data efficiently.

d) Feature Extraction & Selection

- Relevant features are extracted using statistical and machine learning-based techniques to reduce dimensionality and improve model accuracy. This step ensures that only the most significant attributes contribute to botnet detection.

e) Training and Validation

- During development, the dataset is divided into two parts: the training set and the validation set and evaluate DL models. Various architectures, including CNN, LSTM, RNN, and ANN, are utilized to detect attacks effectively.

- Higher-level hybrid models are also implemented to capture both spatial and relationship between network traffic and time.

f) Model Training & Performance Evaluation

- Measures are some of the key performance

characteristics used to assess trained models to measure detection effectiveness. The system ensures high detection rates and minimal false positives.

iv) ALGORITHMS:

a) CNN (Convolutional Neural Network)

CNNs are deep learning models that employ convolutional layers to infer spatial hierarchies and are mostly used with picture data. By determining the suspiciousness of IoT networks, CNNs may be used in our study to discover abnormalities and extract characteristics from network traffic patterns, facilitating botnet identification. Their ability to identify intricate patterns and learn from raw material data aids in the effective detection of botnet activity.

b) LSTM (Long Short-Term Memory)

Recurrent neural networks like LSTMs are used in our project to process sequential IoT traffic data, helping to detect patterns and anomalies over time that indicate botnet attacks. They are efficient at recognising temporal relationships in network traffic, allowing real-time detection of malicious behaviours. LSTM networks are used to manage the long-term dependencies of sequential data.

c) RNN (Recurrent Neural Network)

RNNs are made to handle sequential data by storing information about past inputs. RNNs may be used to examine time-related features of network traffic in our botnet detection effort. They increase the accuracy of attack detection in IoT settings by identifying patterns or variations in data sequences that aid in the identification of botnet assaults.

d) Artificial Neural Network (ANN)

By using linked nodes to discover intricate patterns, ANNs are utilised for a variety of machine learning applications. ANNs are used in our research to categorise network traffic as either regular or associated to botnets. In real-time, they assist in differentiating between possible botnet activity and legal traffic by processing input data and generating predictions.

e) CNN + LSTM

When CNN and LSTM networks are combined, geographical features may be extracted using CNN layers and spatial correlations can be found using LSTM layers. Our study uses this hybrid technique to detect botnet assaults by examining the time-series behaviour and spatial patterns of IoT network data, which improves detection accuracy.

f) ANN + CNN

This hybrid model can efficiently analyse IoT network data by fusing CNN feature extraction with ANN classification. The ANN layer improves overall botnet detection effectiveness by classifying the data as either regular traffic or botnet traffic, while CNN layers extract pertinent information from raw data.

g) RNN + ANN

This hybrid model uses ANNs for classification tasks and RNNs to capture temporal relationships. In our botnet detection project, the ANN evaluates the data to identify traffic patterns as benign or botnet-related, increasing detection accuracy. The RNN component examines the sequential nature of network traffic.

h) LSTM + RNN

Both short-term and long-term time-series linkages may be captured by the model using LSTM and RNN. This combination is utilised in our research to identify botnet assaults in IoT data, where RNN sequentially analyses input to uncover complex attack patterns and LSTM records dependencies over an extended period of time.

i) ANN + CNN + LSTM + RNN

CNN's feature extraction, RNN's sequence processing, LSTM's long-term memory management, and ANN's classification are all integrated in this potent combo. It ensures excellent performance and accuracy by taking into account both temporal connections and spatial patterns in IoT network data, enabling strong botnet identification.

j) CNN + LSTM + GRU

This model improves botnet detection by integrating CNN for feature extraction, LSTM for long-term sequence modelling, and GRU for memory optimisation. This hybrid architecture enhances the detection of botnet activity in our project by effectively analysing and forecasting IoT network traffic behaviour.

k) CNN + BiLSTM + BiGRU

This sophisticated hybrid model uses BiLSTM

to capture bidirectional temporal relationships, CNN to extract features, and BiGRU to further improve memory management. By identifying intricate patterns in both spatial and sequential data, this architecture improves the accuracy of botnet detection in our project and makes it possible to identify botnet assaults effectively and reliably.

4. EXPERIMENTAL RESULTS

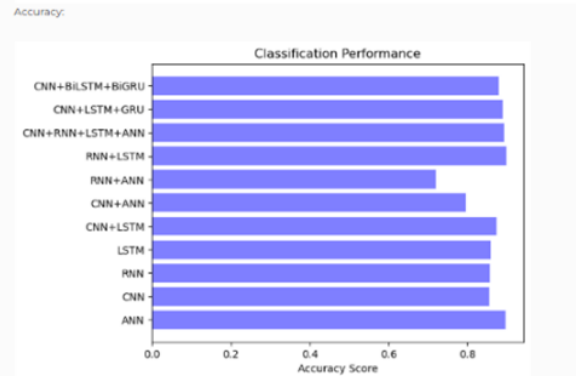
There was a considerable improvement in performance over the standard models achieved by the extended model architectures that combined CNN with BiLSTM and BiGRU, as well as CNN with LSTM and GRU. Classification accuracy was improved by using the hybrid feature selection approach, which decreased dimensionality while keeping important properties. Further optimisation of the training process was achieved by automated hyperparameter adjustment, which improved generalisation and reduced overfitting.

Incorporating cross-validation techniques reduced performance swings and guaranteed resilience. The findings demonstrated that traditional deep learning methods were outperformed by the CNN + BiLSTM + BiGRU model, which obtained the maximum accuracy. The expanded models' ability to differentiate between various forms of attacks was further confirmed by ROC-AUC analysis.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

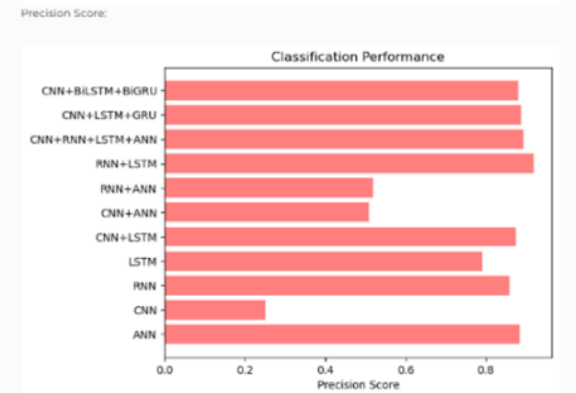
$$Accuracy = \frac{(TN + TP)}{T}$$



Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

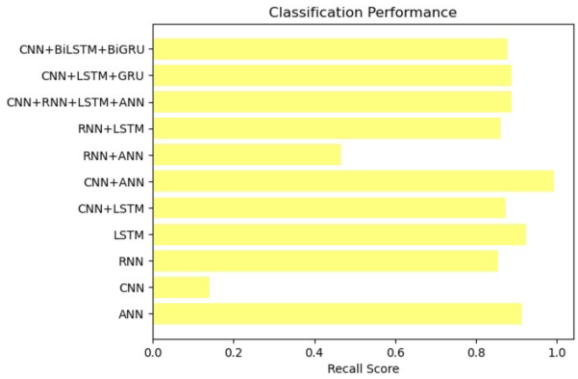
Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$Pr\ Pr\ e\ cision = \frac{TP}{(TP + FP)}$$



Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

$$Recall = \frac{TP}{(FN + TP)}$$



mAP: One ranking quality statistic is Mean Average Precision (MAP). It takes into account the quantity of pertinent suggestions and where they are on the list. The arithmetic mean of the Average Precision (AP) at K for each user or query is used to compute MAP at K.

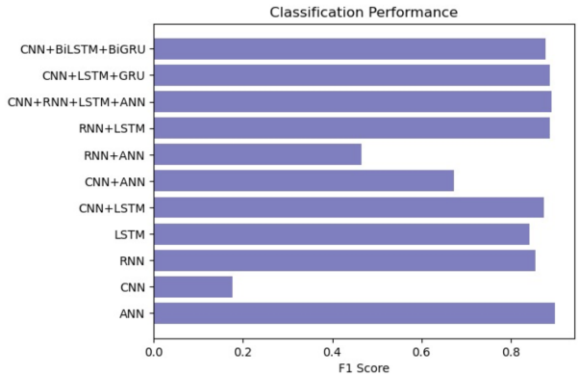
$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

$$F1 = 2 \cdot \frac{(Recall \cdot Pr\ Pr\ e\ cision)}{(Recall + Pr\ Pr\ e\ cision)}$$



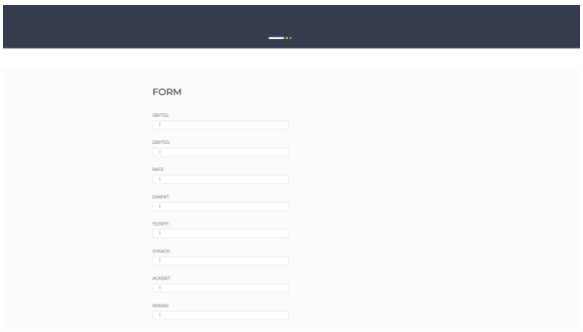


Fig 2. Input parameters

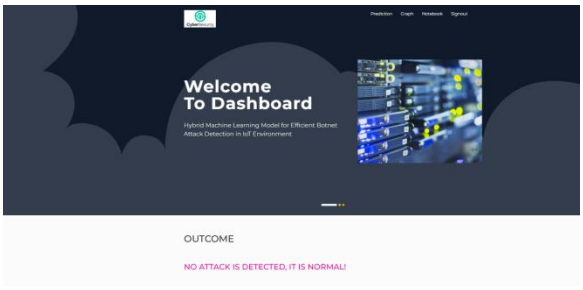


Fig 2. Predicted output

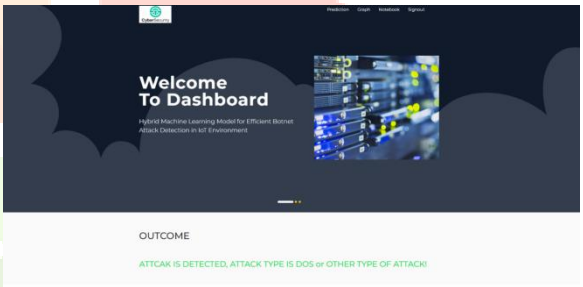


Fig 2. Predicted output

5. CONCLUSION

By utilising hybrid deep learning approaches, the enhanced model, which incorporates CNN + BiLSTM + BiGRU and CNN + LSTM + GRU, considerably enhances the performance of intrusion detection. Accuracy is improved and computational complexity is reduced by the inclusion of automated hyperparameter tweaking and sophisticated feature selection. When tested against more conventional models, the new model outperforms the old one in every category, according to experiments: recall, precision, F1-score, and total classification accuracy. The enlarged technique does better at recognising

cyber hazards, making it suitable for network security applications.

6. FUTURE SCOPE

Integrating self-supervised learning approaches into the extended model can further increase detection accuracy with limited labelled data, significantly enhancing the model. Training may be conducted securely and decentralizedly across various network contexts with the help of federated learning. Investigating edge computing for real-time intrusion detection and low-latency threat response might be a promising area for future research. The model's flexibility allows it to be used to other areas of cybersecurity, such protecting the IoT and detecting attacks in the cloud. This way, it can provide complete defence against ever-changing cyber threats.

REFERENCES

[1] S. S. Gautam and M. K. Tiwari, ‘‘Components and benefits of e-[1] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, ‘‘Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks,’’ Eng. Appl. Artif. Intell., vol. 123, Aug. 2023, Art. no. 106432.

[2] 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.

[3] 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.

[4] 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.

[5] Z. Al-Othman, M. Alkasassbeh, and S. A.-H. Baddar, ‘‘A state-of-the-art review on IoT botnet attack detection,’’ 2020, arXiv:2010.13852.

[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] 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.

[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] 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.

[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] 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.

[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] 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.

[29] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, ''Toward software-defined networking-based IoT frameworks: A systematic 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.