International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 3, Issue 2, March – April (2025)

RESEARCH ARTICLE

FLAM-WORK: INTRUSION DETECTION FRAMEWORK FOR IOT USING FLAMINGO SEARCH OPTIMIZATION AND DEEP LEARNING-BASED CLASSIFICATION

Shobana R [1,*], Abitha V K Lija [2] and S. Shikky Marice [3]

[1] Assistant Professor, Computer Science and Engineering, S.A. Engineering college, Chennai, Tamil Nadu, India
[2] Assistant Professor Computer Science and Engineering Meenakshi College of Engineering, Chennai, Tamil Nadu, India
[3] Research Scholar, Sri krishna College of Engineering and Technology, Coimbatore, India

[*]*Corresponding e-mail: rubanshobana@gmail.com*

Abstract – Internet-of-Things (IoT) connects various physical objects through the Internet and it has a wide application such as in transportation, military, healthcare, agriculture, and many more. Detecting attacks in IoT networks involves identifying abnormal patterns in device behavior or network traffic that indicate potential threats. This research enhances system security by enabling early detection. However, these networks face escalating cybersecurity threats that can cause security issues. To overcome these issues a novel FLAMingo based intrusion detection using deep learning netWORK (FLAM-WORK) has been proposed to identifying network traffic behavior and mitigating cyberattacks in IoT to provide guaranteed network security. The network traffic data packets are gathered from the Input Devices. The data are pre-processed to enhance the data quality. The proposed method utilizing the Convolutional Neural Network (CNN) for feature extraction to understand the complex data easier. Next Feature Selection done by Flamingo Search Algorithm (FSA) to enhance classification accuracy. A Ghost Net classification technique classifies the extracted feature into three classes such as Low, Normal, High. Measures including Specificity, F1-Score (F1S), Accuracy, Precision (PR) and Recall (RC) are used to assess the suggested approach. Compared to current models, experimental results using TON-IoT datasets show higher accuracy. The accuracy of the approach in the TON-IoT dataset is 1.3%, 0.7%, and 1.1% higher than that of the current BMEGTO-KNN, EBWO-HDLID and LIME techniques respectively.

Keywords *–Internet-of-Things, Convolutional Neural Network, Ghost Net, Flamingo Search Algorithm.*

1. INTRODUCTION

IoT is a network of devices with sensors that use the Internet to exchange [1]. Intelligent smart cities, smart devices, smart homes, smart transportation, healthcare, smart grid, smart agriculture, and much more are all products of recent IoT advancements. IoT services are essential to the operations of many individuals, companies, and organizations, as well as to many critical infrastructures [2,3].

Despite these advantages, IoT platforms face challenges such as its limited resources render them vulnerable to many types of intrusions. Network intrusions are one of the biggest security threats that many organizations are currently facing [4,5]. Numerous hackers and other malevolent actors strive to create new ways to get access to the computer systems. Researchers categorize IoT dangers, vulnerabilities, and security challenges to facilitate the process of finding solutions. They classified the vulnerabilities based on the layers of the IoT architecture and there is a lack of physical security hardening [6,7].

Intrusion detection systems (IDSs), which are essential security measures to preserve network security, are installed at a vital location within the network [8]. It analyzes system and network activity to identify suspicious patterns that may indicate an attack is underway. IDSs based on signatures, IDSs based on anomalies, and hybrids of signature and anomaly-based IDSs are the primary methods for detecting intrusions [9]. IDSs filter classifying incoming packets as either regular or malicious. The effectiveness and cost of IDSs are adversely impacted when all parameters are included in the detection process [10].

Security professionals are finding it more and more difficult to identify and address these occurrences manually because of the growing complexity and diversity of network threats. IDS using deep learning enhance the security issues and vulnerabilities. Deep learning (DL) has become more and more popular in intrusion detection systems (IDSs). DL approaches are capable of independently identifying high-level latent information without the need for human interaction [11-13]. The following are the main contributions of the suggested work:

- The main objective of the research is to provide an efficient method for attack detection in IoT

networks to provide network security and Stops attacks early.

- To improve the data quality, network traffic data packets from the Input Devices are first pre-processed using data cleaning, normalization, and discretization.
- The FLAM-WORK technique leverages feature extraction by using CNN model to capture features efficiently and raise the classification model's accuracy.
- Next Feature Selection done by FSA to enhance classification accuracy.
- The selected features are then used to train the Ghost Net model for classification, allowing it to correctly classify data into three classes such as low, normal and high.
- The effectiveness of the suggested technique is valued utilizing parameters like Precision, accuracy, recall (RC), f1-scores, specialty.

The remaining sections of the paper are organized as follows. In section II, the literature review is covered in detail. Section III offers a description of the developed IDS based Deep Learning. Section IV presents the experiments findings and observations. Section V contains the conclusion and future work.

2. LITERATURE REVIEW

In 2023, Tekin N et al. [14] suggested a Machine learning (ML)-based Intrusion Detection Systems (IDS) for security and privacy concern. Cloud services platforms are used to train and test machine learning models. The results show that k-NN, DT, RF, and ANN outperform the LR and NB in terms of accuracy with 99%. Finally, the highest F1-score is achieved by k-NN, DT, and RF, which is 98%. However, performing ML tasks requires high energy consumption.

In 2023, Shtayat M.B.M., et al [15] suggested an explainable ensemble DL-based IDS to improve the transparency and robustness in IIoT networks. DL-based IDSs, giving professionals in charge of preserving IIoT network security and creating more cyber-resilient systems insightful information. The system achieves accuracy rates exceeding 99%. However, a limitation of this research is the reliance on a single dataset (ToN-IoT), which may not fully capture the variety of real-world IIoT scenarios.

In 2023, Saran, N. and Kesswani, N., [16] suggested an Intrusion Detection System (IDS) using multiple Machine Learning (ML) Classifier techniques on Message Queuing Telemetry Transport - Internet of Things - Intrusion Detection System dataset (MQTT-IoT-IDS2020) for identifying the multi-class intrusion attacks in the Internet of Things (IoT). The experiment derives more than 97% overall accuracy for all implemented ML classifier algorithms.

In 2023, Wang, J., Xu et al [17] suggested a novel approach that leverages a blending model for attack classification and integrates counter factual and Local Interpretable Model-Agnostic Explanations (LIME) techniques to enhance explanations. The 'Web-Based' attack type achieves a detection accuracy of 89%, primarily attributed to its smaller representation in the dataset compared to other attack types. However, achieving robust performance across diverse IoT deployments is a complex task.

In 2024, Aburasain, R.Y. [18] suggested an Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection (EBWO-HDLID) technique in the IoT-based Smart Farming environment to capture complex patterns and detects significant intrusions. This technique extents improved performance with higher accuracy and F1score values of 98.81%, 90.84%, 78.95%, and 79.49% correspondingly.

In 2024, Asgharzadeh et al [19] suggested an intrusion detection system for IOT that uses deep learning and a multi-objective enhanced gorilla troops optimizer BMEGTO to pick features effectively and identify anomalies more accurately. The proposed model is implemented on two benchmark data sets, NSL-KDD and TON-IoT and tested regarding the accuracy, precision, recall, and F1-score criteria. An accuracy of the BMEGTO-KNN model on the TON-IoT and NSL-KDD datasets are 99.99% and 99.86%, respectively.

In 2024, Al Quayed F et al [20] suggested a predictive framework to enhances the cybersecurity of WSNs in Industry 4.0 using a multi-criteria approach. Decision Tree model provides an accuracy of 99.48%, precision of 99.49%, recall of 99.48%, and F1 score of 99.49% in the detection. However, these tools require more expert power, high-performance computational resources, and continuous training on updated datasets.

3. PROPOSED METHOD

This section presents a classification of unprocessed packets into attacked packets and normal data packets using Deep Learning Technique. The network traffic packets are got from the Input Devices using the tool named Wireshark, records the data in .pcap files. The data are pre-processing using the techniques Data Cleaning, Normalization, Discretization. The Feature Extraction process is done by CNN (Convolutional Neural Network). Next Feature Selection done by FSA (Flamingo Search Algorithm) inspired by Flamingo bird food Searching and Feeding behaviour. This Algorithm used to find the better feature selection. Deep Learning using GhostNet technique classifies the data features into three classes namely Mirai attack, Gafgyt attack and normal data packets.

3.1 Data Collection

The Network traffic packets collected from the IoT devices like smart lights, appliances, or sensors that continuously communicate over a network using the tool wireshark, which records the data in .pcap files contain important data about how the devices are behaving and interacting. This raw data is collected and passed into the system for analysis.

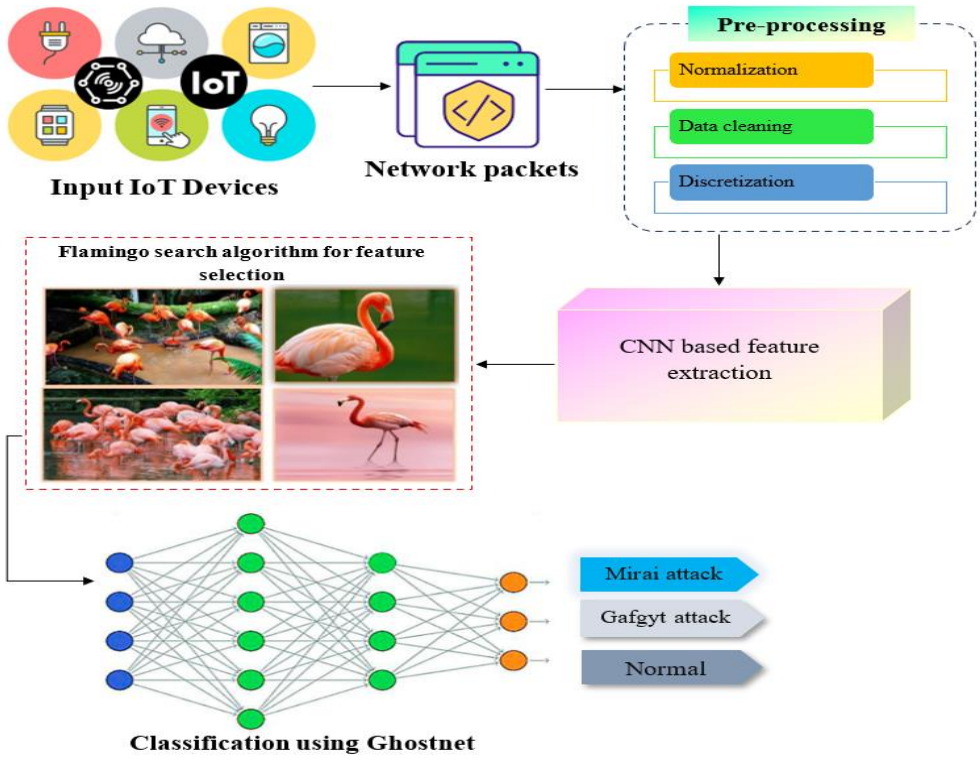

Figure 1. Proposed FLAM-WORK methodology

3.2 Data Pre-Processing

The preprocessing steps of normalization, data cleaning, and discretization are used to enhance the data quality. Data cleaning filling in missing information, and normalization places the value within a predetermined range. Data are categorized by discretization. Accurate data classification requires a pre-processing step**.**

Normalization

The process of converting values measured on various scales to a conceptually similar scale is called normalization. Numerous methods exist for normalization, such as baseline, min-max, and z-score normalization. Each sensor collects a wide variety of resistance values, which, if appropriately normalized, can aid in producing more accurate test data predictions.

Data Cleaning

Data cleaning entails fixing errors, eliminating outliers, and adding missing values. Sensor datasets that contain broken sensor data and settling time zones must be cleansed. Errors in the data collection process or problems with the sensor itself are recorded as broken sensor data.

Discretization

Discretization of continuous predictors is a popular method for preprocessing data, which is an important step before data is entered into multiple machine learning classifiers for learning. To enable effective dataset integration, these models usually require the input data to be pre-processed into discrete numerical values. a technique where the continuous feature is split up into equal segments. It is necessary to decide the number of intervals in advance.

3.3. CNN based Feature Extraction

The convolutional neural network (CNN) has generated a great deal of interest due to the advancement in computer power and training methods. CNNs (Convolutional Neural Networks) identify hidden patterns in data, apply filters to find patterns, and process each layer. The function Relu was used to highlight strong signals and retrieve the most crucial data attributes for classification. The mathematical model outlined in Equation (1) is followed by a conventional CNN.

$$Z_{xy} = (M * N)_{xy} = \sum_q \sum_p M_{(x+q)(y+P)} N_{qp} \qquad (1)$$

Equation (1) states that the sensor features are extracted by the hidden layers via convolution processes, represented by M. A pooling layer that lowers the range comes after it. Zxy is the output feature map at point (x, y) (x, y), and M is kernel of p× q p × q. Ultimately, the convolutional procedure extracted the features. In the following stage, these retrieved characteristics are fed into the ghost net classification model.

3.4 Feature Selection using Flamingo Search Algorithm

Flamingo Search Algorithm is used to select most relevant features after extraction, to improve the accuracy, reducing complexity and minimizing overfitting. The FSA is divided into the foraging and migration behavior of a flamingo population, which explores the search space through inter-population information exchange and fixed location movement rules, striving to find the optimal solution.

Foraging Behaviour

During foraging, flamingos utilize their beaks as a large sieve. With their beaks facing down and swinging in all directions, they collect food and expel excess residue.

Likewise, it selects the optimal feature subset that improves accuracy and reduces redundancy The distance s of the flamingo's beak scanning behavior during foraging can be expressed using the following formula.

$$s = \left| D_1 \times yb_j + \varepsilon_2 \times y_{ij} \right| \quad (1)$$

where ε_2 is −1 or 1, and D_1 is a randomly generated number that follows a standard normal distribution with size (0, 1). y_{ij} represents the position of the i^{th} flamingo bird in the population's j^{th} dimension, and the most abundant food location in the population is denoted by yb_j.

$$g_t = D_2 \times s \quad (2)$$

where D_2 represents a random number that conforms to a standard normal distribution.

Migratory Behavior

When the food in the foraging area is not sufficient for the survival of the flamingos, the flamingos will search and migrate to the next location where food is more abundant. Just as flamingos migrate to better environments, the algorithm shifts solutions toward more promising regions in the search space and improving the chances of finding the optimal feature subset.

$$y_{ij}^{s+1} = y_{ij}^{s} + \omega \times \left(xd_j^s - y_{ij}^s \right) \quad (6)$$

In the above equation, ω is a random number, equal in size to D_1, to simulate the random behavior of flamingos during migration.

3.5 Classification using GhostNet

Using ghost net model, the selected features from network packet data are classified into three classes such as Mirai attack, Gafgyt attack and Normal. This method swiftly and precisely classifies the data. As illustrated in figure 2, the convolutional layer-based mapping is initially used in the Ghost module. Ghost Net uses the two routes listed below:

Primary Path

This path serves as the primary convolutional operation, typically a depth-wise separable convolution. Since depth-wise separable convolutions isolate spatial filtering from channel-wise filtering, they are computationally less expensive than ordinary convolutions. The feature mapping obtained through the primary path is expressed as:

$$\text{Fm} = \text{B} * \text{d} + \text{c} \quad (2)$$

In this case, the feature map is represented by Fm, bias by B ∗d, and conventional filters by c.

Ghost Path

The ghost path is inexpensive and shallow. The term low-complexity operation is frequently used. Other, less computationally costly aspects are captured via the ghost path. The network can become more efficient and gain higher representational power by combining data from both pathways. The feature mapping that was acquired using the ghost path is expressed as follows:

$$\text{Fm} = B * d' \quad (3)$$

where d' is the filter used in the ghost path. The Ghost Net's output is passed into the softmax and fully connected layers, which classify the data into Mirai attack, Gafgyt attack and Normal.

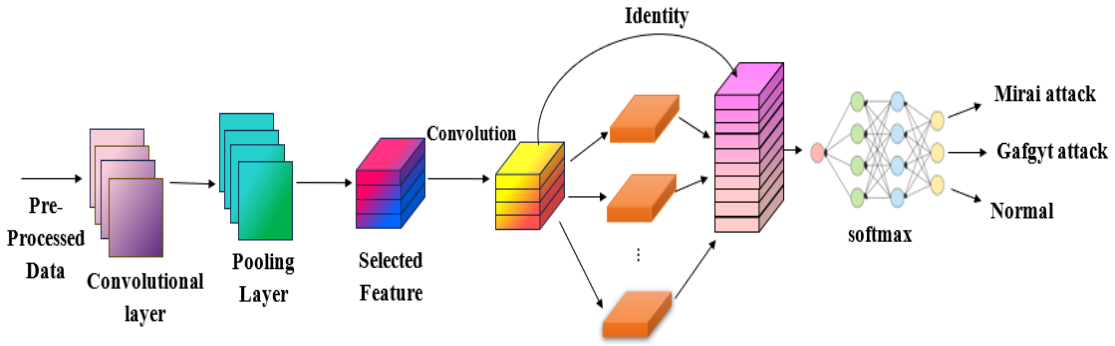

Figure 2. Classification methodology

4. RESULTS AND DISCUSSION

This section explores the effectiveness of the suggested strategy using a range of evaluation measures and gives the experimental findings. Here, the suggested categorization model is implemented using a Python programming tool. Accuracy, precision, recall and F1-score are the evaluation metrics used in the suggested approach.

4.1 Dataset Description

TON-IoT is the dataset used to evaluate the proposed method. It has different samples and characteristics. The TON-IoT dataset is a new generation of IoT/IIoT datasets, network traffic, and operating systems. This dataset has 22,390,223 records, including normal and attack data, of which 461,043 records are extracted from the Internet of Things traffic (300,000 records from normal traffic and 161,043 records from attack traffic. This data set with 44 features and 8 attack types, including normal and abnormal samples.

4.2 Evaluation Metric

This section explains the measures that were used to evaluate the suggested approach. The effectiveness of the recommended strategy has been evaluated using the F1-Score, Recall, Precision and Accuracy measures.

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \quad (4)$$

$$\text{Precision (PR)} = \frac{\text{TP}}{\text{TP+FP}} \quad (5)$$

$$Recall\ (RC)\ = \frac{TP}{TP+FN} \quad (6)$$

$$\text{F1} - \text{score} = \frac{2*(\text{PR}*\text{RC})}{(\text{PR+RC})} \quad (7)$$

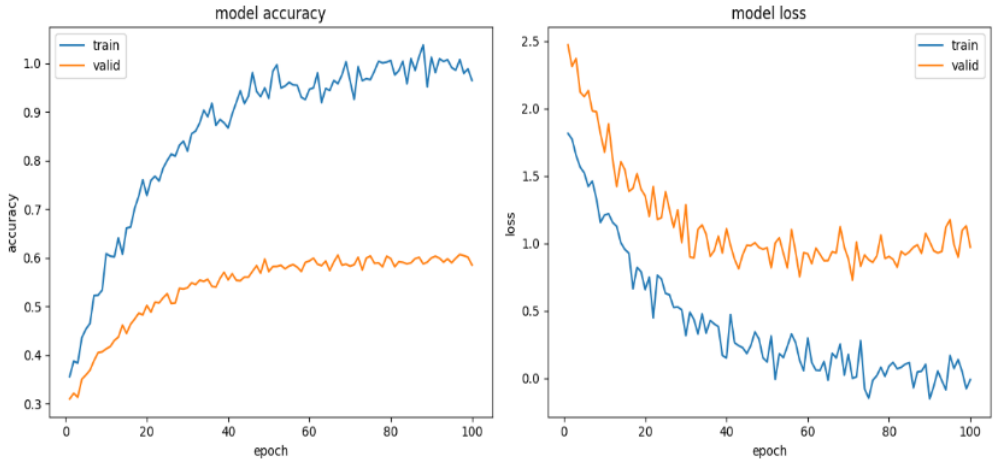

Figure 3. Accuracy and Loss curve for the proposed method

The accuracy and Loss curve in Figure.3 demonstrates how effectively the suggested model learned from the dataset. Using 10 epochs, the model's validation accuracy was 98.84% with a validation loss of 0.0045%. It illustrates the model's efficacy by showcasing its capacity to detect attacks.

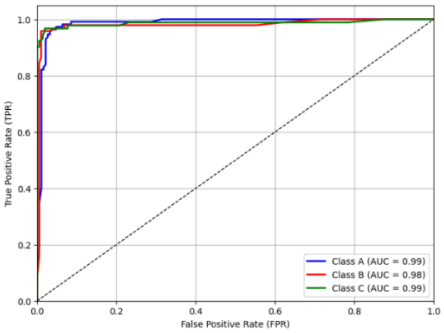

Figure 4. Roc curve of the proposed method

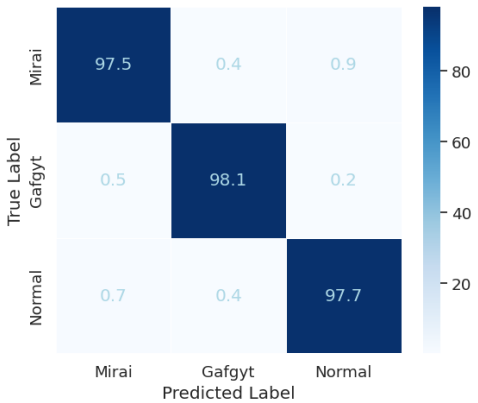

Figure 5. Confusion Matrix

4.3 Performance Analysis

According to the experimental results, the suggested FLAM-WORK technique has been compared with current techniques for detecting attacks on network packet data, including BMEGTO_KNN, EBWO_HDLID and LIME.

For classification tasks, Figure.5 shows confusion matrices with performance predicted labels on low, normal, and high 98.13% of labels are identified, with 1.3% being classified as normal and 1.2% as somewhat elevated. The classifier performs well across all datasets, especially when it comes to detecting attacks.

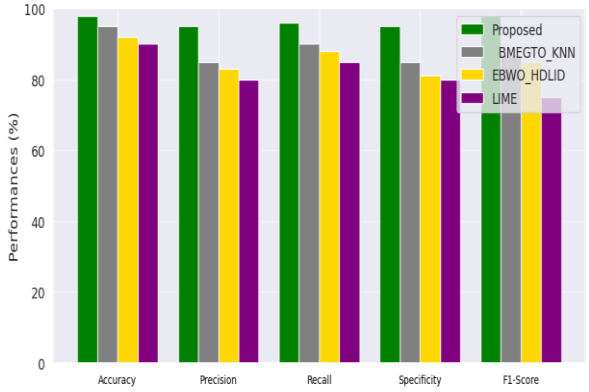

Figure 6. Performance Analysis

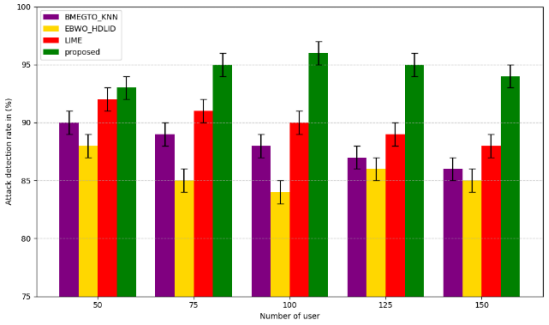

Figure 7. Attack detection analysis

The performance study of categorization classes using the TON-IoT dataset is shown in Figure.6 for the Hypertension dataset, the recommended method's F1-Score,

accuracy, recall, precision, and specificity are 98.61%, 97.73%, 92.44%, and 96.98%, respectively.

Figure.7 compares the attack detection rates of four methods across different user counts. The proposed FLAM-WORK method consistently achieves the highest detection accuracy for all user groups, outperforming BMEGTO_KNN, EBWO_HDLID, and LIME. Detection performance slightly declines for other methods as user numbers increase.

5. CONCLUSION

This study suggested a new FLAM-WORK method for efficiently detecting attacks on IoT based network data packets. The data are pre-processing using the techniques Data Cleaning, Normalization, Discretization to enhance the data quality. The CNN model is utilized for feature extraction in order to efficiently capture features and improve the classification model's accuracy. Next Feature Selection is done by FSA inspired by Flamingo bird food Searching and Feeding behaviour, which used to find the better feature. By fed these selected features into the Ghost Net model, the network is able to classify data reliably into three classes such as Mirai attack, Gafgyt attack and Normal. In addition to increasing intrusion detection, this method enhances security by identifying threats early, preserving data integrity, reducing downtime, and ensuring reliable system performance. The proposed method is evaluated using f1score, recall, accuracy, specificity and precision. For the TON-IoT dataset, the proposed method's F1-Score, accuracy, recall, precision, and specialty are 97.61%, 96.73%, 96.13%, and 97.73%, respectively. The accuracy of FLAM-WORK methodology is 1.3%, 0.7%, and 1.1% higher in the TON-IoT dataset than the current BMEGTO_KNN, EBWO_HDLID and LIME methods. The system can be further developed by leverage AI and real-time analytics for faster, more adaptive threat responses. Integration with IoT and edge computing will enable decentralized, energy-efficient, and scalable solutions.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] N. Tekin, A. Acar, A. Aris, A.S. Uluagac, and V.C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection", Internet of Things, vol. 21, pp. 100670, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] M.B.M. Shtayat, M.K. Hasan, R. Sulaiman, S. Islam, and A.U.R. Khan, "An explainable ensemble deep learning approach for intrusion detection in industrial internet of things", *IEEE Access*, vol. 11, pp. 115047-115061, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] N. Saran, and N. Kesswani, "A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things", *Procedia Computer Science*, vol. 218, pp.2049-2057, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] J. Wang, H. Xu, Y.G. Achamyeleh, S. Huang, and M.A. Al Faruque, "Hyper detect: A real-time hyperdimensional solution for intrusion detection in iot networks", *IEEE Internet of Things Journal,* vol. 11, no. 8, pp. 14844-14856, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] R.Y. Aburasain, "Enhanced black widow optimization with hybrid deep learning enabled intrusion detection in Internet of Things-based smart farming", *IEEE Access*, vol. 12, pp. 16621-16631, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F.S. Gharehchopogh, "An intrusion detection system on the internet of things using deep learning and multi-objective enhanced gorilla troops optimizer", *Journal of Bionic Engineering*, vol. 21, no. 5, pp. 2658-2684, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0", *IEEE Access*, 2024[CrossRef] [Google Scholar] [Publisher Link]

[8] M. Samantaray, R.C. Barik, and A.K. Biswal, "A comparative assessment of machine learning algorithms in the IoT-based network intrusion detection systems", *Decision Analytics Journal*, vol. 11, pp. 100478, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "Toward an intrusion detection model for IoT-based smart environments", *Multimedia Tools and Applications*, vol. 83, no. 22, pp. 62159-62180, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] V. Saravanan, M. Madiajagan, S.M. Rafee, P. Sanju, T.B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network". *Multimedia Tools and Applications*, vol. 83, no. 11, pp. 31505-31526, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Y. Lu, S. Chai, Y. Suo, F. Yao, and C. Zhang. Intrusion detection for Industrial Internet of Things based on deep learning. Neurocomputing, 564, p.126886, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] M. Jouhari, and M. Guizani, "Lightweight cnn-bilstm based intrusion detection systems for resource-constrained iot devices", *In 2024 International Wireless Communications and Mobile Computing (IWCMC),* pp. 1558-1563, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] M.H. Bhavsar, Y.B. Bekele, K. Roy, J.C. Kelly, and D. Limbrick, "Fl-ids: Federated learning-based intrusion detection system using edge devices for transportation iot", *IEEE Access*, vol. 12, pp. 52215-52226, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Almotairi, S. Atawneh, O.A. Khashan, and N.M. Khafajah, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models", *Systems Science & Control Engineering*, vol. 12, no. 1, pp. 2321381, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] K. Kethineni, and G. Pradeepini, "Intrusion detection in internet of things-based smart farming using hybrid deep learning framework", *Cluster Computing*, vol. 27, no. 2, pp. 1719-1732, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning-based approach", *Expert Systems with Applications*, vol. 238, pp. 121751, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] M.K. Nallakaruppan, S.R.K. Somayaji, S. Fuladi, F. Benedetto, S.K. Ulaganathan, and G. Yenduri, "Enhancing security of host-based intrusion detection systems for the internet of things", *IEEE Access*, vol. 12, pp. 31788-31797, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] C. Geetha, S.D. Johnson, A.S. Oliver, and D. Lekha, "Adaptive weighted kernel support vector machine-based circle search approach for intrusion detection in IoT environments", *Signal, Image and Video Processing*, vol. 18, no. 5, pp. 4479-4490, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] D. Jayalatchumy, R. Ramalingam, A. Balakrishnan, M. Safran, and S. Alfarhood, "Improved crow search-based feature selection and ensemble learning for IoT intrusion detection", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] D. Javeed, M.S. Saeed, M. Adil, P. Kumar, and A. Jolfaei, "A federated learning-based zero trust intrusion detection system for Internet of Things", *Ad Hoc Networks*, vol. 162, Pp. 103540, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Shobana R received her master degree from Anna University, Coimbatore, India. Now she is working towards the PhD degree in Anna University, Chennai in India. From 2011 she was working as Assistant Professor and took a break of 7 years. Now she is working as Assistant Professor in S.A. Engineering College from 2022. Her primary research interests are deep learning, cyber security, cloud computing and quantum computing

Abitha VK Lija completed her B.E in CSE from CSI Institute Of Technology, Thovalai affilated to Anna University. She completed her M.E in CSE from Jerusalem College Of Engineering affiliated to Anna University. She is currently working as Assistant Professor in the Department of CSE in Meenakshi College of Engineering, Chennai, India. She is currently pursuing Ph.D. in the Department of Computer Science and Engineering in S.A. Engineering College under Anna University, Chennai, India. Her area of interest includes IoT, Cyber security, Big data, Deep learning and Machine Learning.

Shikky Marice. S, Research Scholar with more than 4 years of teaching experience. I obtained my M.E in Communication Systems Engineering from Cape Institute of Technology (affiliated to Anna University) in the year 2013. My research interests lie in the domain of Computer Vision, Pattern Recognition, Anomaly Detection & Clustering.

Arrived: 15.03.2025
Accepted: 17.04.2025