International Journal of Computer and Engineering Optimization (IJCEO)
Volume 01, Issue 02, November – December (2023)

RESEARCH ARTICLE

CAB-IDS: IOT-BASED INTRUSION DETECTION USING BACTERIA FORAGING OPTIMIZED BIGRU-CNN NETWORK

Jhansi Bharathi Madavarapu[1, *]

[1]Department of Information Technology, University of Cumberlands, 6178 College Station Drive, Williamsburg, KY 40769 USA.

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

Abstract – Internet of Things (IoT) is an advancing technology that enables the development of various essential applications. Despite its potential these applications frequently depend on centralized storage systems which pose challenges such as privacy risks, security threats, and vulnerability to single points of failure. To overcome these issues, a novel CNN-BiGRU based Bacteria foraging optimization for Intrusion Detection System (CAB-IDS) framework is proposed for detecting and mitigating intrusions in IoT networks and to enhance the security. Initially, the generated IoT data packets undergo data pre-processing module which is carried out by data normalization. After pre-processing, feature extraction is performed using a regulated network and the feature selection process is optimized through a Bacteria Foraging Optimization (BFO) algorithm. The chosen features are input into a Bidirectional Gated Recurrent Unit combined with a Convolutional Neural Network (BiGRU-CNN) to carry out the classification which determines whether the data is normal or abnormal. The CAB-IDS method is validated by using Network Simulator 2 (NS2) and assessed by using detection accuracy, false positive rate, residual energy, and computing overhead. The accuracy of the proposed CAB-IDS framework is 97.72% higher than that of the SPIP method which is 83.43%, HybridChain-IDS method which is 88.57% and TLBO-IDS method, which is 92.12% respectively.

Keywords *– Internet of Things, Intrusion Detection System, Bacteria Foraging Optimization, Bidirectional Gated Recurrent Unit - Convolutional Neural Network.*

1. INTRODUCTION

IoT encompasses a network of distributed sensors, devices, and servers that enable simultaneous detection and handling of measurands, creating a direct communication platform among security systems [1,2]. Among the sectors that use IoT applications are smart homes, transportation, healthcare, and agriculture [3]. The vulnerability of the Internet of Things' multi-layered architecture, which consists of the application, network, and perception levels, makes security a major concern. This is true even if IoT offers many advantages in their everyday existence [4,5].

Information security research must include cyberattack detection in order to identify recent or ongoing attacks [6]. Intrusion detection often involves classification tasks to determine whether network usage patterns are normal or abnormal, distinguishing between typical and various types of attacks such as signature attacks, anomalous attacks, Denial of Service (DoS), Root to Local (R2L), and Probe [7].

IoT security involves protecting, detecting, and monitoring risks, and mitigating vulnerabilities in diverse devices, which pose significant security threats [8,9]. Different sensors and actuators in IoT networks contribute to creating intelligent systems that improve transportation, waste management, logistics, security control, emergency services, and healthcare [10,11]. The main criteria for an effective IDS include accuracy in decision-making, response to attacks, identification of attack types and attackers, and the detection techniques employed [12,13]. A CAB-IDS system is proposed in this paper to leverage intrusion detection to improve security in IoT networks. The proposed CAB-IDS approach's primary contribution is presented below.

- Initially, the generated IoT data packets undergo data pre-processing module which is carried out by data normalization.
- Following pre-processing, the data is passed to the Regulated Network (REG-NET), to effectively extracts the necessary features from the IoT data.
- The extracted features are then fed into the Bacteria Foraging Optimization (BFO) Algorithm for feature selection.
- These selected features are fed into a BiGRU-CNN for classification process which identifies either the data is normal or abnormal.
- The performance of the proposed CAB-IDS method is evaluated using metrics such as accuracy, sensitivity, precision, recall, F1 score, and intrusion detection rate.

In the remainder of this work, the following sections are included: Section II discusses the literature review. Part III presents an example of the proposed CAB-IDS technique. Section IV summarizes the debate and conclusion. Section V looks at the conclusion and future directions.

2. LITERATURE SURVEY

This section provides a summary of the literature on existing studies that are relevant to the proposed CAB-IDS framework. The sections also highlight some research gaps and limitations, which are as follows:

In 2021 Abdollahzadeh, et al. [14] suggested the African Vulture Optimization Algorithm (AVOA), a metaheuristic that draws inspiration from African vultures' browsing and foraging behaviors. The program is designed to resemble the vultures' natural foraging habits. Experiments demonstrate that in the majority of engineering applications, AVOA performs better than alternative methods, attaining superior outcomes in 30 of 36 benchmark functions. At a 95% confidence level, statistical analysis employing the Wilcoxon Rank Sum test validates the AVOA algorithm's significant benefits.

In 2022 Yang, et al. [15] offered a comprehensive intrusion detection system that uses knowledge graphs and DL techniques for IoT networks. After transforming IoT network requests into word vectors, a CNN-BiLSTM model that is based on attention is utilized to identify malicious query attacks. This method achieves a 90.01% accuracy rate in detecting intrusions.

In 2023 Keshk, et al. [16] suggested a SPIP framework to assess explainable deep learning (DL) algorithms for the purpose of integrating IDS in IoT environments. Both local and global interpretations are provided by the system by combining a number of techniques from deep learning and explainable artificial intelligence (XAI). Administrators and decision makers are better equipped to recognize complex attack patterns due to the SPIP architecture's excellent detection accuracy.

In 2023 Sharadqh, et al. [17] suggested using blockchain technology to power the HybridChain-IDS framework's two-tier intrusion detection and graph-based attack prevention features. A two-level intrusion detection system based on ResCapNet technology, attack graph generation using the novel KNN algorithm, user planning and access control, and so on are the four sequential activities that make up the system. The potential of HybridChain-IDS to stop attacks is still rather limited, even with its increased accuracy, recall, FAR, F-score, and detection rate.

In 2023 Alotaibi, and Ilyas, [18] suggested a ML-based intrusion detection system for IoT gadgets. To differentiate between regular and random data, the suggested solution employs four supervised machine learning algorithms. The network traffic information from TON-IoT was used to test the suggested approach. The findings demonstrate that this framework enhances intrusion detection system efficacy and attains an accuracy rate of 0.9863 respectively.

In 2023 Awajan, [19] suggested a IoT based intrusion detection using deep learning. The suggested technology is designed as a standalone device with the vocal communication protocol to lessen the complexity of the deployment. Data sets are necessary for deep neural networks (DNNs). It can detect attacks with a median accuracy of 93.74%, including distributed denial of service, vulnerabilities, opportunistic services, and black holes. However, the suggested approach is less efficient and effective.

In 2023 Kaushik, et al. [20] suggested an IDS that is enabled by teaching-learning-based optimization (TLBO-IDS), which guarantees little overhead and provides excellent protection against intrusion threats for networks connected to the wide web. Modern algorithms performance is contrasted with that of TLBO-IDS, which has undergone rigorous testing. Specifically, TLBO-IDS performs 22.2% and 40% better than the Genetic Algorithm (GA) and bat algorithm, respectively.

Based on a literature analysis, the performance, efficiency, false positive rate, and detection accuracy of the aforementioned procedures are low. The proposed intrusion detection system performs much better to the DL model BiGRU-CNN, which serves as the foundation for intrusion detection in the IoT.

3. PROPOSED CAB-IDS METHODOLOGY

In this section a novel CNN-BiGRU based Bacteria foraging optimization for Intrusion Detection System (CAB-IDS) framework is proposed for classifying IoT device data as normal or abnormal. Initially, the data packets from the IoT devices are fed to the pre-processing module. In the pre-processing phase, data normalization has been carried out which removes the duplicate data from the collected data. After pre-processing, the data are given to the Regulated Network (REG-NET) for feature extraction which efficiently extracts the required features from the IoT data. The extracted features are then fed into the Bacteria Foraging Optimization (BFO) Algorithm for feature selection. These selected features are fed into a BiGRU-CNN for classification process which identifies either the data is normal or abnormal. The overall workflow of the CAB-IDS framework is depicted in Figure 1.

3.1. Data Pre-processing

The intensity of IoT network traffic varies. Data preparation reduces the amount of time required to train and assess the detection system by converting this raw data into a format more appropriate for modeling. By effectively recognizing attack patterns in IoT contexts, this procedure raises the detection system's overall efficacy.

Data Normalization

IoT networks based on blockchain are subject to large fluctuations in traffic levels. Our model uses the Standard Scaler regularization technique to scale the feature values in order to address this variability. By doing this, it guarantees that the export detection feature of the system operates well at all times, removing any gaps in incoming traffic without altering it. fundamental mathematical characteristics. The equation (1) illustrates the conversion process. Equation 1.

$$S_k = \frac{V_k - \mu_k}{\sigma_k} \quad (1)$$

where $k \in \{k1, k2, k3.., kn\}$, and sk stands for the standard feature score in the detection system. The

characteristics' mean and standard deviation are denoted by μ_k and σ_k.

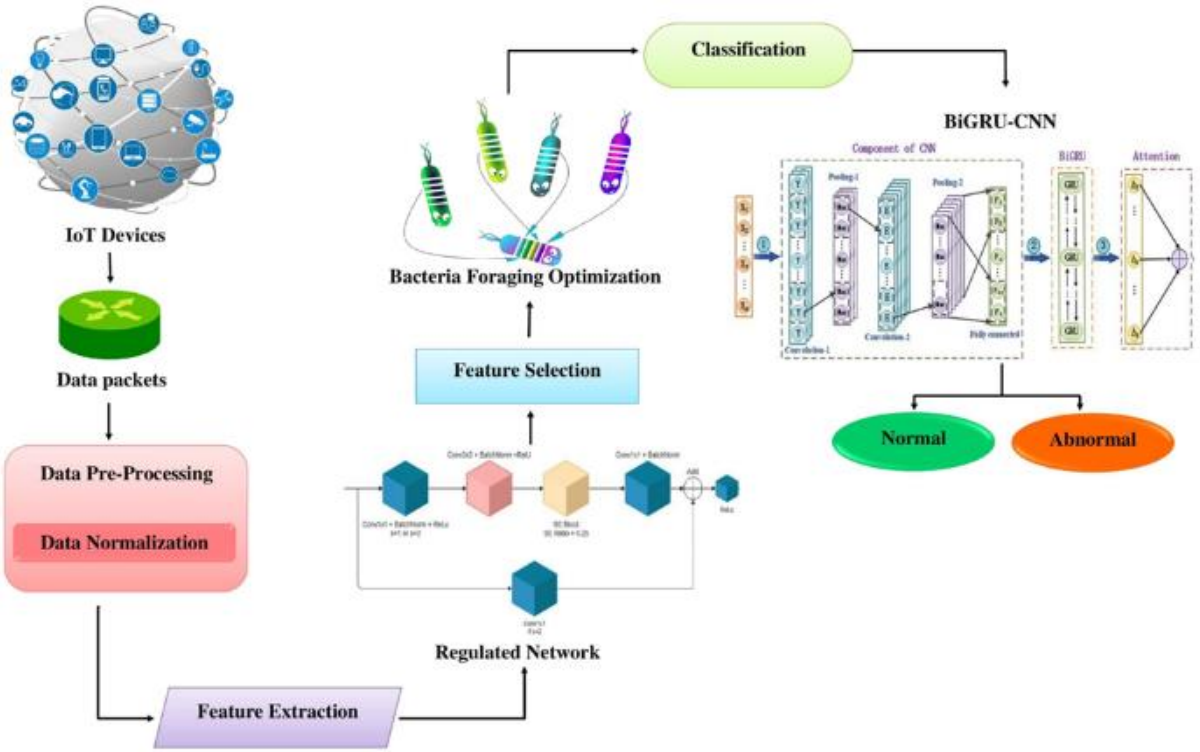

Figure 1. Resultant Graph of the Proposed System

3.2. Feature Extraction Using Reg-NET

ResNet building blocks for feature extraction from compressed digital images were presented, both bottleneck and non-bottleneck. Two distinct RNN-modified ResNet structural modules were created as a result. While one of these modules uses a separate RNN-modified ResNet structural module, the other uses ConvRNN as its regulator.

RegNet Module

The output of the second module, H^t is a representation of the ConvLSTM output of the first module, H^{t-1}. X_1^t is the module feature map representation. ConvLSTM, the $k-th$ RegNet module, can be expressed as. Equation 2, 3, 4, 5 and 6.

$$X_2^t = ReLU\big(BN(W_{12}^t * X_1^t + b_{12}^t)\big), \quad (2)$$

$$[H^t, C^t] = ReLU\left(BN\big(ConvLSTM(X_2^t, [H^{t-1}, C^{t-1}])\big)\right), \quad (3)$$

$$X_3^t = ReLU\big(BN(W_{23}^t * Concat[X_2^t, H^t])\big), \quad (4)$$

$$X_4^t = BN(W_{34}^t * X_3^t + b_{34}^t), \quad (5)$$

$$X_1^{t+1} = ReLU(X_1^t + X_4^t) \quad (6)$$

These are 3x3 convolution kernels made from 1x1 kernels: W_{12}^t, W_{23}^t, and W_{34}^t. BN () represents the batch normalization procedure. Concatenation can be accelerated with the use of concat []. This module feeds the ConvLSTM the input entity X_2^t and the ConvLSTM's prior output, H^t, as shown in equation (2). Depending on the input, ConvLSTM automatically decides whether to propagate the data from the memory cell to the output hidden feature map H^t.

Bottleneck RegNet Modul

The RegNet bottleneck module's core component is the ResNet bottleneck building block. Large image management was the Bottleneck building block's original function. As a result, the bottleneck can be represented by the RegNet module as follows. Equation 7, 8, 9, 10, 11 and 12.

$$X_2^t = ReLU\big(BN(W_{12}^t * X_1^t + b_{12}^t)\big), \quad (7)$$

$$[H^t, C^t] = ReLU\left(BN\big(ConvLSTM(X_2^t, [H^{t-1}, C^{t-1}])\big)\right), \quad (8)$$

$$X_3^t = ReLU\big(BN(W_{23}^t * X_2^t + b_{23}^t)\big), \quad (9)$$

$$X_4^t = ReLU\big(BN(W_{34}^t * Concat[X_3^t, H^t])\big), \quad (10)$$

$$X_5^t = BN(W_{45}^t * X_4^t + b_{45}^t), \quad (11)$$

$$X_1^{t+1} = ReLU(X_1^t + X_5^t), \quad (12)$$

where W_{23}^t is a 3×3 bottleneck kernel and W_{12}^t and W_{45}^t are two 1×1 kernels. A 1x1 kernel called W_{34}^t is used to combine the features in our model.

3.3. Feature Selection using Bacteria Foraging Optimization

The Bacteria Foraging Algorithm (BFA) is a nature-inspired algorithm modeled after the way bacteria locate nutrients. This process consists of three main steps: chemotaxis, reproduction, and elimination-dispersion. During chemotaxis, bacteria spread out from their swarm and move randomly in search of higher nutrient concentrations. They navigate this process through two types of movements: swimming and tumbling. If a bacterium encounters difficulty

while swimming in a certain direction, it tumbles, changing its direction randomly before resuming its search for nutrients. Equation 13.

$$\theta_m(n+1,p,k) = \theta^m(n,p,k) + d(m)\frac{\Delta(\mathrm{m})}{\sqrt{\Delta^{\mathrm{X}}(\mathrm{m})\Delta(\mathrm{m})}} \quad (13)$$

Once a chemotaxis cycle is completed, the healthy bacteria reproduce. This reproduction process helps uncover additional solutions and increases the likelihood of finding more optimal solutions compared to those previously identified. Equation 14.

$$N_{dd}\big(\theta, l(n,p,k)\big) = \sum_{m=1}^{r}\big[-f_{attractant}exp\big(-z_{attractant}\sum_{i=1}^{l}(\theta_i - \theta^m{}_i)^2\big)\big] \quad (14)$$

As a final step, elimination dispersion focuses on removing solutions detected by bacteria that are suboptimal, retaining only the effective ones. In the bacterial food cycle, these three steps collectively describe the process through which bacteria address and solve problems. Equation 15.

$$F_m = \sqrt{(yr-ym)^2 + (wr-wm)^2 + (xr-xm)^2} \quad (15)$$

Chemotaxis is utilized in intelligence to select features from IoT data packets. In this context, a higher frequency signifies a greater concentration, akin to nutrient concentration, guiding bacteria towards the target. During reproduction, certain features selected by bacteria are eliminated. Additionally, the chemotaxis behavior of the remaining bacteria is considered, allowing for the selection of more features. In the elimination step, features associated with both attack and non-attack data are retained, and the selected features are presented as the output of the Bacterial Foraging Algorithm (BFA).

3.4. Classification Using BiGRU-CNN

The CAB-IDS method enhances intrusion detection by integrating a CNN layer after a Bi-GRU layer to form a DL-based BiGRU-CNN model. The Bi-GRU layer is used to extract long-term temporal relationships from the input dataset for intrusion detection. This method sends two hidden state vectors, comprising past and future data, into the CNN layer to capture critical local interactions between the convolution and clustering layers. A higher update gate rating indicates a greater effect, while a reset gate determines the extent to which previous hidden layer neuron outputs are ignored. As the reset gate speed increases, fewer details are overlooked. The hidden layer formula is as follows. Equation 16, 17, 18 and 19.

$$Z_t = \sigma(W_z \cdot [h_{t-1}, x_t]) \quad (16)$$

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \quad (17)$$

$$\bar{h}_t = tanh(W \cdot [r_t * h_{t-1}, x_t]) \quad (18)$$

$$h_t = (1-z_t) * h_{t-1} + z_t * \bar{h}_t \quad (19)$$

The reset gate rate increases the amount of information retained. Convolutional processes are used by a specific type of feedforward neural network known as a CNN. Four layers comprise a CNN: the input layer, pooling layer, convolutional layer, and fully connected layer. The following explains the role of a convolutional layer. Equation 20.

$$Y_i = f(W \cdot x_{i:i+h-1} + b) \quad (20)$$

Where, $x_1, x_2, x_3, \ldots, x_n$ The weight matrix is, the bias vector is, the input vector is, and the nonlinear function is f (*). After convolution kernel extraction, the resultant eigenvector y is. Equation 21.

$$Y = \{Y_1, Y_2, Y_3, \ldots, Y_{n-h+1}\} \quad (21)$$

The maximum pooling technique will select the largest element in the sequence $Y_1, Y_2, Y_3, \ldots, Y_{n-h+1}$ and eventually obtain a new vector y. Equation 22.

$$Y = max(Y_i) \quad (22)$$

To align the dimensions of the BiGRU model, the output from the CNN is reduced. When combining the BiGRU and CNN models, it is essential to assign the appropriate weights to both models, ensuring they share the same feature space index. This process involves selecting one of the two models. The sigmoid function is expressed as. Equation 23.

$$\sigma(z) = \frac{1}{1+e^{-z}} \quad (23)$$

4. RESULT AND DISCUSSION

The CAB-IDS Framework simulation is implemented using NS2 and compared against SPIP, HybridChain-IDS, and TLBO-IDS frameworks. The classification stage utilizes a comprehensive traffic dataset collected from 16 devices. Performance metrics such as detection accuracy and the effectiveness of DL networks are evaluated to demonstrate the accuracy of the classification algorithm.

4.1. Performance Analysis

The following metrics are used to assess the experimental results: recall, accuracy, precision, and F1 score. The parameters are shown in a statistical analysis below. Equation 24, 25, 26, 27 and 28.

$$\text{Accuracy} = \frac{TP+TN}{total\ no.of\ samples} \quad (24)$$

$$Recall = \frac{TP}{TP+FN} \quad 25)$$

$$F1\ score = 2\left(\frac{precision*recall}{precision+recall}\right) \quad (26)$$

$$Sensistivity = \frac{TP}{TP+FP} \quad (27)$$

$$TRP = \frac{TP}{TP+FP} \quad (28)$$

FP stands for false positive, TN for true negative, FN for false negative, and TP for true positive in this case. The prediction performance will be enhanced by raising the precision value.

4.2. Comparative Analysis

A comparative analysis was carried out to show how much better the suggested approach is than the current approaches. Evaluations were conducted on performance parameters such precision, recall, sensitivity, F1 score, and true positive rate (TPR). Figure 2 shows these metrics: precision, sensitivity, recall, F1 score, and specificity. Performance Comparison of CAB-IDS Framework is shown in Figure 2.

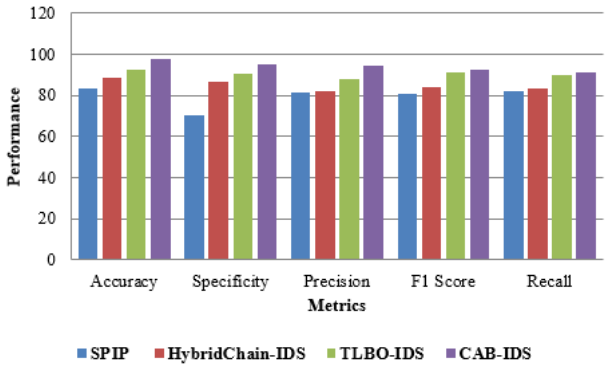

Figure 2. Performance Comparison of CAB-IDS Framework

The CAB-IDS technique achieves an accuracy of 83.43% for SPIP, 88.57% for HybridChain-IDS, 92.12% for TLBO-IDS and 97.72% for the proposed framework to enhance the security in IoT networks. Comparison of Detection Rate is shown in Figure 3.

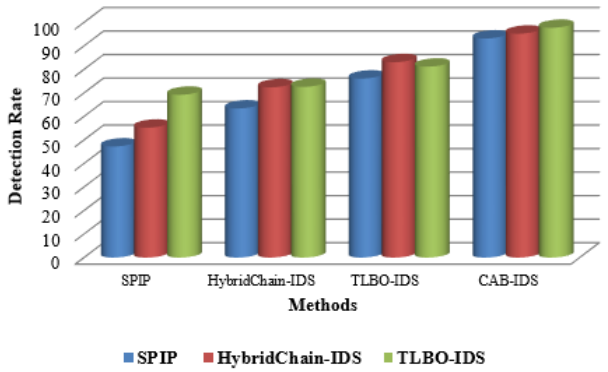

Figure 3. Comparison of Detection Rate

Figure 3 illustrates a comparison of detection rates, which measure the algorithm's efficacy in identifying intruders. This parameter evaluates the classifier's performance by estimating how effectively it detects attacks, presented graphically as the percentage of attacks increases. The BiGRU-CNN classifier distinguishes between regular and attack packets by computing the distance difference between them. Comparison of DL Networks is shown in Figure 4.

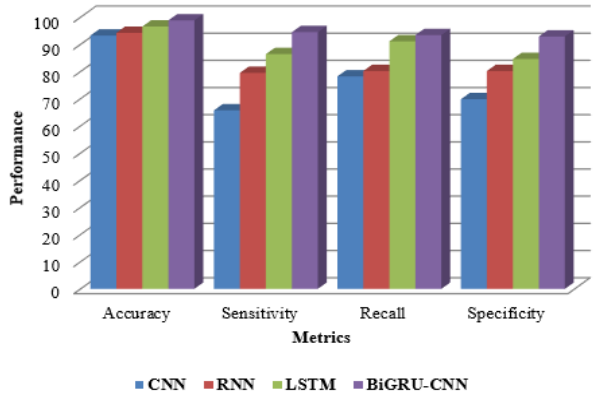

Figure 4. Comparison of DL Networks

This assessment considers authentication processes, detection rates, processing times, and flow-based packet classification within the CAB-IDS framework, aimed at safeguarding IoT and cloud networks. Authentication plays a crucial role in minimizing attack volumes and preventing multi-layer attacks.

5. CONCLUSION

This paper proposes a novel CAB-IDS framework for detecting and mitigating intrusions in IoT networks and to enhance the security. The proposed CAB-IDS approach is simulated by using Network simulator2 (NS2). The proposed model's performance was validated and compared BiGRU-CNN deep learning model using the real-time BoT-dataset. A comparison is made between proposed CAB-IDS framework and existing approaches such as SPIP, HybridChain-IDS and TLBO-IDS in terms of accuracy, precision, recall, sensitivity, and intrusion detection rate. The accuracy of the proposed CAB-IDS framework is 97.72% higher than that of the SPIP method which is 83.43%, HybridChain-IDS method which is 88.57% and TLBO-IDS method, which is 92.12% respectively. Therefore, the proposed CAB-IDS framework increases the accuracy, intrusion detection rate and reduces the delay and computational complexity of the IoT devices.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

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] V. Hnamte, and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system," *Telematics and Informatics Reports*, vol. 10, pp. 100053, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395-9409, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," *Vehicular Communications*, vol. 35, pp. 100471, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] S. Zafar, N. Iftekhar, A. Yadav, A. Ahilan, S. N. Kumar, and A. Jeyam, "An IoT method for telemedicine: Lossless medical image compression using local adaptive blocks," *IEEE Sensors Journal*, vol. 22, no. 15, pp. 15345-15352, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of

Things," *Alexandria Engineering Journal*, vol. 81, pp. 371-383, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] T. Gaber, J. B. Awotunde, M. Torky, S. A. Ajagbe, M. Hammoudeh, and W. Li, "Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks," *Internet of Things*, vol. 24, pp. 100977, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] M. H. Shahriar, Y. Xiao, P. Moriano, Lou, W. and Hou, Y.T., "CANShield: Deep Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal-Level," *IEEE Internet of Things* Journal, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] A. J. G. Malar, C. A. Kumar, and A. G. Saravanan, "Iot based sustainable wind green energy for smart cites using fuzzy logic based fractional order darwinian particle swarm optimization," *Measuremen*t, vol. 166, pp. 108208. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, pp.102211, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Nasir, A. R. Javed, M. A. Tariq, M. Asim, and T. Baker, "Feature engineering and deep learning-based intrusion detection framework for securing edge IoT," *The Journal of Supercomputing*, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] T. Thanjaivadivel, S. Jeeva, A. Ahilan, "Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM," 2019.[CrossRef] [Google Scholar] [Publisher Link]

[12] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet of Things*, vol. 28, pp. 101336, 2024. [CrossRef] [Google Scholar] [Publisher Link]

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

[14] B. Abdollahzadeh, F. S. Gharehchopogh, and S. Mirjalili, "African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems," *Computers Industrial Engineering*, vol. 158, pp. 107408, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] X. Yang, G. Peng, Zhang, D. and Y. Lv, "An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph," *Security and Communication Networks*, no. 1, pp. 4748528, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A.Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Information Sciences*, vol. 639, pp. 119000, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] A. A. Sharadqh, H. A. M. Hatamleh, S. S. Saloum, and T. A. Alawneh, "Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment," *IEEE Access*, vol. 11, pp. 27433-27449, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Y. Alotaibi, and M. Ilyas, "Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security," *Sensors*, vol. 23, no. 12, pp. 5568, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] A. Awajan, "A novel deep learning-based intrusion detection system for IOT networks," *Computers*, vol. 12, no. 2, pp. 34, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] A. Kaushik, and H. Al-Raweshidy, "A novel intrusion detection system for internet of things devices and data. and quot; Wireless Networks" pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] S. Gokul Pran, S. Raja, "An efficient feature selection and classification approach for an intrusion detection system using Optimal Neural Network," *Journal of Intelligent and Fuzzy Systems*, vol. 44, no. 5, pp. 8561-712023. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. G. Pran, S. Raja, S. Jeyasudha "Intrusion detection system based on the beetle swarm optimization and K-RMS clustering algorithm," *International Journal of Adaptive Control and Signal Processing*, vol. 38, no. 5, pp. 1675-89, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Jhansi Bharathi Madavarapu is a seasoned Principal EAI/EDI Consultant specializing in project delivery for Cloud migration, Digital transformation, EDI/B2B legacy modernization, and API integration projects. With a distinguished track record in the information technology industry spanning over ten years, Jhansi has successfully navigated and addressed the intricate challenges of multinational organizations worldwide in business integration. Her expertise lies in designing and implementing innovative business process solutions and integration platforms fortified with robust Cybersecurity measures. Throughout her career, Jhansi has played a pivotal role in aiding businesses to attain their objectives through technology-driven solutions, fostering sustainable results. As a testament to her professional standing, she holds the esteemed position of Senior Member in both the IEEE and ISACA, further attesting to her commitment to excellence in the field.

Arrived: 22.11.2023

Accepted: 24.12.2023