Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.037673
Article

Intrusion Detection in the Internet of Things Using Fusion of GRU-LSTM Deep Learning Model

Mohammad S. Al-kahtani[1], Zahid Mehmood[2,3,*], Tariq Sadad[4], Islam Zada[5], Gauhar Ali[6] and Mohammed ElAffendi[6]

[1]Department of Computer Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj, 16273, Saudi Arabia
[2]Department of Computer Engineering, University of Engineering and Technology, Taxila, 47050, Pakistan
[3]The FAMLIR Group, The University of Lahore, Lahore, 54000, Pakistan
[4]Department of Computer Science, University of Engineering & Technology, Mardan, 23200, Pakistan
[5]Faculty of Computing, International Islamic University, Islamabad, 44000, Pakistan
[6]EIAS Data Science and Blockchain Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, 11586, Saudi Arabia
*Corresponding Author: Zahid Mehmood. Email: zahid.mehmood@uettaxila.edu.pk
Received: 12 November 2022; Accepted: 04 May 2023; Published: 23 June 2023

Abstract: Cybersecurity threats are increasing rapidly as hackers use advanced techniques. As a result, cybersecurity has now a significant factor in protecting organizational limits. Intrusion detection systems (IDSs) are used in networks to flag serious issues during network management, including identifying malicious traffic, which is a challenge. It remains an open contest over how to learn features in IDS since current approaches use deep learning methods. Hybrid learning, which combines swarm intelligence and evolution, is gaining attention for further improvement against cyber threats. In this study, we employed a PSO-GA (fusion of particle swarm optimization (PSO) and genetic algorithm (GA)) for feature selection on the CICIDS-2017 dataset. To achieve better accuracy, we proposed a hybrid model called LSTM-GRU of deep learning that fused the GRU (gated recurrent unit) and LSTM (long short-term memory). The results show considerable improvement, detecting several network attacks with 98.86% accuracy. A comparative study with other current methods confirms the efficacy of our proposed IDS scheme.

Keywords: Cyber security; deep learning; intrusion detection; PSO-GA; CICIDS-2017; intelligent system; security and privacy; IoT

1 Introduction

The expansion of information technology has been tremendous, facilitating the seamless exchange of information globally. Smart cities have emerged in many nations to handle urbanization development effectively by employing resources efficiently. IoT promotes swift, precise communication in the contemporary world with smart cities by connecting several devices [1]. A major attribute of internet-connected devices is that they collect real-time data through sensors and are always connected to the

internet. These devices have found their application in various sectors including transport, military, agriculture, education, healthcare, and commerce, to name a few as presented in Fig. 1. Despite the approved protocols for communication exchange, the various domains of applications have led to the recognition of multiple communication devices, protocols, and standards [2]. The acquired data from the sensors can be utilized to create a smart approach. However, advancements in technology have also created challenges for the communication system, facing intrusions in the form of various attacks. The intrusion detection system (IDS) is one tool for combating these challenges, as it has detection algorithms that can categorize or identify potential cyberattacks. IDS can be labeled into two classes: signature and anomaly-based IDSs (SIDS and AIDS). In contrast, SIDS can detect intrusions by monitoring traffic patterns and comparing them to regular patterns. AIDS has an edge over SIDS since it can identify fresh network threats. HIDS can spot risks from within the system by examining data from the database logs, firewall, server, OS, or application system audit. Before an external attack hits a computer network, NIDS can detect it by tracking and examining network traffic gathered from various sources.

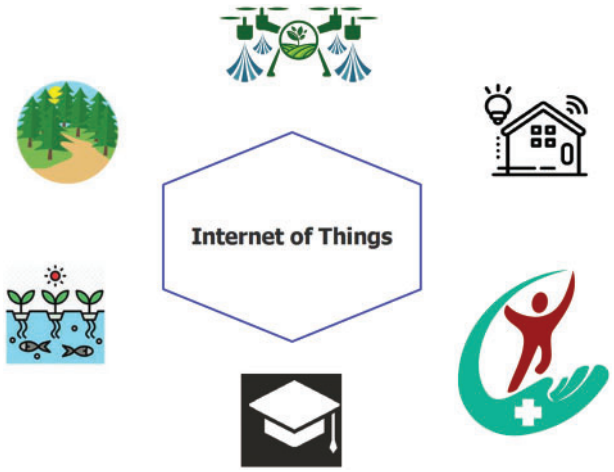

Figure 1: Framework of IoT deployment

To maintain confidentiality, integrity, and availability; a computer security program safeguards computing resources from external threats. An intrusion into the network could cause a serious threat to the victim server and the rest of the network [3]. IDS allows system administrators to detect intrusions and respond to them. Hacks have become more frequent as people's faith in the internet has expanded. Defensible against a denial-of-service attack is a well-executed security assault. IDS allows for internal and external attacks on a company's computer network. IDSs and burglar alarms are different, even though they are comparable. We describe ways to identify and categorize intrusions in IoT networks in this research because security and privacy are critical issues in all IoT appliances.

2 Background of Intrusion Detection System

IDS plays a vital role in detecting malicious activities on a network. These technologies are made to spot hazardous behavior or potential regulatory violations. Administrators are frequently informed of malicious activities or security breaches using a SIEM (security information and event management) system. To discriminate between legitimate and erroneous alarms, SIEM designs incorporate data from several sources. IDS devices monitor networks for suspicious behavior, however, they are susceptible to

false positives. Hence, while introducing IDS devices, businesses must ensure that they are optimized. By implementing intrusion prevention systems, the system should be able to discriminate between safe network traffic and harmful activities. In addition, intrusion detection systems monitor the network packets entering the device to alert the user of any unusual behavior.

2.1 Types of IDS

There are four types of IDS whose details are given in the following subsequent sections:

2.1.1 Network Intrusion Detection System (NIDS)

Multiple network appliances can be systematically analyzed with NIDS. By using a database of known attacks, all traffic on the subnet can be monitored, and any intrusion or suspicious activity is immediately reported to the administrator. In the subnet where they are installed, NIDS is specially made to find and report attempts to breach firewalls.

2.1.2 Host Intrusion Detection System (HIDS)

Any suspicious or disruptive behavior on a server must be found by a HIDS, which must then alert the administrator. HIDS can monitor data in transit to identify risks over a network. Any changes in or loss of crucial system files are notified to the administrator for evaluation by the software, which continuously compares the state of device files to those from a recent backup. There is no limit as to how many devices can be put on HIDS, including mission-critical systems and other devices unlikely to be modified in any way.

2.1.3 Protocol-Based Intrusion Detection System (PIDS)

A secure web server is achieved by accepting the appropriate HTTP protocol and supervising the HTTPS stream routinely. Before proceeding to the web presentation layer, the device should stay within this interface because HTTPS is not completely secure.

2.1.4 Application Protocol-Based Intrusion Detection System (APIDS)

Devices or groups of agents located on several servers are referred to as APIDS. APIDS uses application-specific logs to analyze traffic between servers to detect potential intruders. This technology can be used to monitor, for example, SQL communication between a web server and a database by the middleware.

2.2 Motivation

The modern age is replete with internet-connected devices, and we depend on these technologies to fulfill our daily requirements. However, this increased reliance on such systems leads to a higher risk of security breaches and intrusions. There has been an impressive deal of research into enhancing IDS using machine learning and deep learning. Nevertheless, existing IDSs still struggle to improve detection rates, minimize false positives, and recognize unknown intrusions. To address these challenges, a hybrid-based approach can be employed to differentiate between normal and abnormal data.

3 Literature Review

The increased frequency of cyber-attacks has put IoT devices at high risk, requiring urgent attention. Several solutions have been recommended in the literature to prevent and detect these

attacks, with the help of machine learning (ML) and deep learning (DL) techniques [3–6]. For instance, in one study, authors utilized artificial neural networks (ANN) to detect network intrusion [7]. Another study [8] employed a hybrid feature selection and classification method using NSL-KDD and KDDcup99 datasets. They applied a combination of K-means and random forest and achieved an accuracy of 99.85% using the NSL-KDD dataset. Different ML methods for identifying network anomalies with reduced features and full features were proposed in [9] using UNSW-NB15. The authors applied XGBoost for feature selection and claimed that K-nearest neighbors (KNN) achieved a training accuracy of 95.86% through reduced features. An ensemble model using meta-classification was proposed by the authors of [10] to achieve more accurate predictions. A 94.27 percent accuracy rate was achieved with the UNSW-NB15 and an 82.22% accuracy rate with the UGR16 datasets. Additionally, several ML models were tested in [11] using a voting classifier, resulting in an accuracy rate of 99.7%.

ML techniques are commonly utilized to identify cyber intrusions due to their ability to operate automatically and promptly. Nevertheless, cyber intrusions are constantly evolving, necessitating the development of more adaptable detection systems. To address this challenge, scalable detection systems are needed. Scalable and flexible detection systems can be made using DL algorithms. For example, the authors employed CICIDS-2017 to evaluate the performance of the IDS model [12]. Before training the model, PSO-GA (PSO-based GA), a hybrid technique of swarm intelligence and evolution, is applied To improve the dependability of ELM, their model is assessed using ELM-BA based on bootstrap resampling. Their work attained the greatest accuracy of 100% on PortScan, SQL Injection, and Brute Force Attack, demonstrating the viability of the suggested model for cybersecurity applications. For the Internet of medical things (IoMT) networks, authors in [13] suggested a deep learning-based IDS, resulting in enhanced performance. Using recurrent neural networks (RNN) [14], the authors detected cyberattacks by configuring features using a modified seagull optimization method (SOA). The authors attained an accuracy rate of 94.12% using the KD-Cup99 dataset. Deep-convolutional neural network (DCNN) was used in a related study [15] to identify a malicious attack in IoT networks using IoTID20 dataset and achieved an accuracy of 98.38%. Using deep neural networks (DNNs) as an IDS system, the authors of [16] found that the AntiRectifier layer performed better than other machine learning classifiers.

The existing literature highlights the need for more effective models to address the challenges posed by advanced cyber-attacks in IoT domains. Additionally, hybrid methods of learning can improve the accuracy of IDS [17]. This makes them an attractive option for enhancing the effectiveness of IDS.

The primary contribution of this manuscript can be concise as follows:

- We optimized the performance of the CICIDS-2017 dataset for accurate attack categorization by fine-tuning it, eliminating redundant features, and selecting only the most distinguishing features using PSO-GA.
- We implemented an IDS that utilizes DL techniques, specifically adapting the LSTM-GRU framework for this purpose.

4 Proposed Model

To ensure optimal performance of the hybrid DL technique, namely the LSTM-GRU framework, a feature selection method called PSO-GA was employed to select the most suitable feature set. The proposed IDS model's flow diagram is illustrated in Fig. 2.

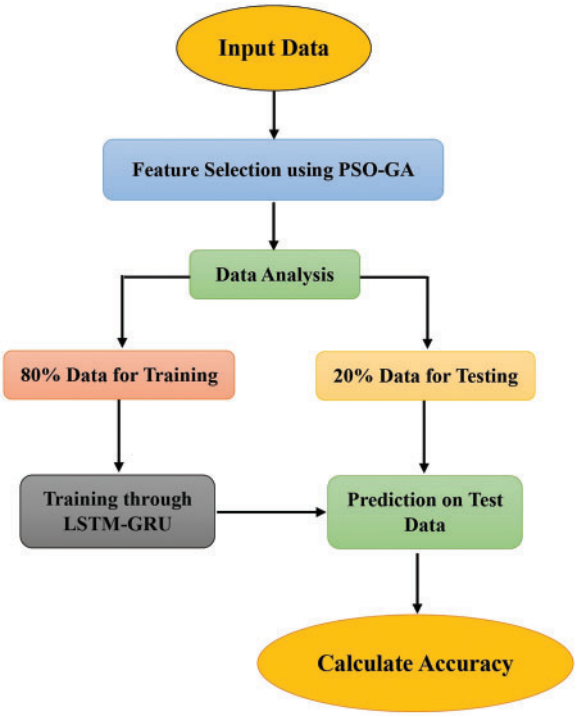

Figure 2: The proposed IDS model

4.1 Dataset

IDS and IPS are critical defense mechanisms against the rising tide of sophisticated network attacks. However, anomaly-based IDSs face significant challenges in accurately detecting attacks due to the lack of reliable validation records. To address this issue, we utilized the CICIDS-2017 dataset [18], which contains a wide range of attack types, including DoS, DDoS, brute force attacks, web attacks, botnets, infiltration, and port scans [19,20]. The details of the CICIDS-2017 dataset features are presented in Table 1.

Table 1: Number of features of the CICIDS-2017 dataset

No	Feature name	No	Feature name	No	Feature name
1.	Bwd IAT Std	27.	Flow Bytes/s	53.	AvgFwd Segment Size
2.	Bwd IAT Max	28.	Flow Packets/s	54.	AvgBwd Segment Size
3.	Bwd IAT Min	29.	Flow IAT Mean	55.	Fwd Header Length
4.	Fwd PSH Flags	30.	Flow IAT Std	56.	FwdAvg Bytes/Bulk
5.	Fwd Packets's total Length	31.	Flags of Bwd PSH	57.	FwdAvg Packets/Bulk
6.	Bwd Packets's total Length	32.	Flags of Fwd URG	58.	FwdAvg Bulk Rate
7.	Fwd Packet's Length Max	33.	Flags of Bwd URG	59.	BwdAvg Bytes/Bulk
8.	Fwd Packet's Length Min	34.	Length of Fwd Header	60.	BwdAvg Packets/Bulk
9.	Fwd Packet's Length Mean	35.	Length of Bwd Header	61.	BwdAvg Bulk Rate

(Continued)

Table 1: Continued

No	Feature name	No	Feature name	No	Feature name
10.	Bwd Packet's Length Max	36.	Bwd Packets/s	62.	SubflowFwd Bytes
11.	Bwd Packet's Length Min	37.	Min Packet's Length	63.	SubflowBwd Packets
12.	Init_Win_bytes_forward	38.	Packet Length Std	64.	PSH Flag Count
13.	Init_Win_bytes_backward	39.	Packet Length Variance	65.	ACK Flag Count
14.	act_data_pkt_fwd	40.	FIN Flag Count	66.	Flow IAT Min
15.	min_seg_size_forward	41.	SYN Flag Count	67.	Fwd IAT Total
16.	Active Mean	42.	Destination Port	68.	Fwd IAT Mean
17.	Active Std	43.	Flow Duration	69.	Fwd IAT Std
18.	Active Max	44.	Total Fwd Packets	70.	Fwd IAT Max
19.	Active Min	45.	Total Backward Packets	71.	Fwd IAT Min
20.	Idle Mean	46.	URG Flag Count	72.	ECE Flag Count
21.	Idle Std	47.	CWE Flag Count	73.	Down/Up Ratio
22.	Idle Max	48.	Flow IAT Max	74.	Bwd IAT Total
23.	Idle Min	49.	Average Packet Size	75.	Bwd IAT Mean
24.	Fwd Packet's Length Std	50.	Fwd Packets/s	76.	SubflowFwd Packets
25.	Bwd Packet's Length Std	51.	Packet Length Mean	77.	RST Flag Count
26.	Bwd Packet's Length Mean	52.	Max Packet's Length	78.	SubflowBwd Bytes

4.2 Features Selection

As part of the feature selection stage, a given data set is analyzed to identify the most appropriate set of features. This is done to effectively reduce computational costs and improve input data selection. To achieve this, we propose a hybrid-based approach called PSO-GA, which fused PSO and GA. PSO is an effective method for subselecting features with strong local search capabilities [21]. However, it tends to get stuck in local optima, hampering its exploration capability. Moreover, PSO lacks control over the number of search characteristics and does not make advantage of feature correlation knowledge [22]. On the other side, GA may use a crossover to accomplish incredible search space exploration. But he is unable to benefit from it. PSO-GA strikes a balance between exploring and using the search space by fusing the advantages of the two methodologies [23]. PSO searches for related particles, whereas GA is good at passing on useful skills from one generation to the next. Results are improved and are more applicable as a result of this combination [17]. Table 2 represents the features that were chosen.

Table 2: Selected attributes for the proposed IDS model

Attack type	Total features	Selected features
BruteForce		40
DoS		39
DDoS		43
Bot	78	41

(Continued)

Table 2: Continued

Attack type	Total features	Selected features
Infiltration		38
WebAttacks		37
PortScan		42

4.3 LSTM-GRU Architecture

In this work, the fusion of gated recurrent unit (GRU) and long short-term memory (LSTM) techniques are being used for predictive analytics as presented in Fig. 3. The proposed architecture has six hidden layers, each with 256 hidden units. Three of these hidden layers are composed of LSTM units, while the other three are composed of GRU units. The activation function used in all of these hidden layers is tanh, which is a commonly used non-linear activation function in neural networks. One dense layer and one unit are used in the output layer, which employs a linear activation function. By reducing the output dimension from the previous layers, the output from the dense layer is transmitted to the output layer. Due to the linear activation function in the output layer, the output values are not limited to a specific range, which is advantageous in some applications.

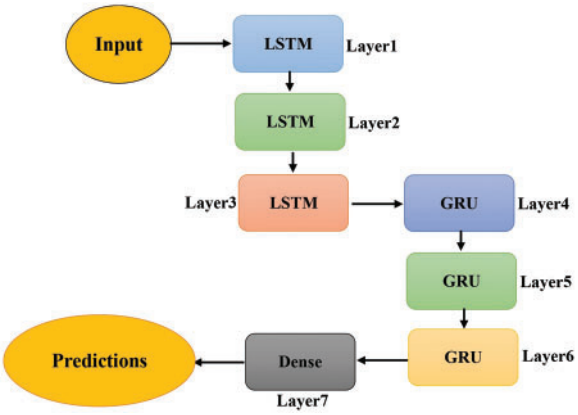

Figure 3: LSTM-GRU architecture for the proposed IDS model

4.3.1 Gated Recurrent Unit (GRU)

The GRU is designed to tackle the problem of vanishing or exploding gradients. It is an improved version of the LSTM model and controls information flow using gate structures as well. It is important to note that GRU does not have an output gate, which leaves all information open to the public. GRUs only have two gates: the reset and the update gate, whereas the LSTM combines input and forget gates. GRUs have fewer parameters and improve performance due to their simpler structure. GRU reset and update gates are represented by the following equations:

$$m_s = \sigma\left(W_m\left[h_{\{s-1\}}, x_s\right] + U_m h_{\{s-1\}} + b_m\right) \tag{1}$$

$$n_s = \sigma\left(W_n\left[h_{\{s-1\}}, x_s\right] + U_n h_{\{s-1\}} + b_n\right) \tag{2}$$

where m_s is the reset gate at time step s, n_s is the update gate at time step s, $h_{\{s-1\}}$ is the hidden state at time step $s-1$, x_s is the input at time step s, W_m and W_n are weight matrices for the reset and update

gates, U_m and U_n are weight matrices for the reset and update gates applied to the hidden state, b_m and b_n are the biases for the reset and update gates, and σ is the sigmoid activation function.

The candidate hidden state, $\check{h}_s$, is then calculated as follows:

$$\check{h}_s = \tanh\left(W\left[m_s * h_{\{s-1\}}, x_s\right] + b\right) \tag{3}$$

where W is a weight matrix and b is a bias label.

An interpolation is then performed between the previous hidden state and the candidate hidden state to determine the hidden state at time step s, h_s:

$$h_s = (1 - n_s) * h_{\{s-1\}} + n_s * \check{h}_s \tag{4}$$

where the carry gate $(1 - n_s)$ is located, which determines the point to which the previous hidden state will be carried forward, and the range to which the candidate's hidden state will be used to update the past hidden state.

4.3.2 Long Short-Term Memory (LSTM)

There are three gates in an LSTM, a type of recurrent neural network. These gates include the forget, the input, and the output gate. In traditional RNNs, the gradient is vanishing due to the LSTM's vanishing gradient algorithm [24]. Whether to discard or keep previously learned information depends critically on the forget gate. It determines whether to maintain or discard the data from the preceding time step's cell state after evaluating its relevance. The mathematical equation for the Oblivion Gate is as follows:

$$p_s = \sigma\left(W_{p\left[h_{s-1}, x_s\right]} + b_p\right) \tag{5}$$

where h_{s-1} is the prior hidden state, W_p is the weight matrix, x_s is the input at time s, and b_p is the bias vector; p is the forget gate activation vector at time s.

The input gate, on the other hand, determines what new data should be added to the cell state. A vector of potential new candidate cell state values is created using the tanh function, and values that need to be refreshed are determined using the sigmoid function. Using the mathematical formula below, we can calculate the input gate's performance:

$$q_s = \sigma\left(W_{q\left[h_{s-1}, x_s\right]} + b_s\right) \tag{6}$$

$$v_s = \tanh\left(W_{v\left[h_{s-1}, x_s\right]} + b_v\right) \tag{7}$$

where q_s is the input gate activation vector at time s, W_q is the weight matrix, h_{s-1} is the previous hidden state, x_s is the input at time s, b_s is the bias vector, v_s is the vector of new values for the cell state, W_v is the weight matrix, and b_v is the bias vector.

Last but not least, the output gate is in charge of producing the output depending on the modified cell state. The output is obtained by applying the tanh function on the updated cell state after using the sigmoid function to select which values should be output. The output gate's mathematical equation is as follows:

$$f_s = \sigma\left(W_{f\left[h_{s-1}, x_s\right]} + b_f\right) \tag{8}$$

$$h_s = f_s * \tanh(v_s) \tag{9}$$

5 Implementation

The model used for training comprises six LSTM-GRU layers, one dense layer, and a single output layer. The initial layer has 700 neurons, with subsequent layers containing 600, 500, 400, 300, and 200 neurons. All layers use the ReLU activation function, and the loss function used for the deep learning models is cross-entropy, with the optimizer being Adam. During training, a batch size of 32 is employed for ten epochs, resulting in the final layer of the model having seven neurons for predicting the seven attack classes: DoS, BruteForce, DDoS, Infiltration, WebAttacks, PortScan, and Bot.

6 Results and Discussions

To accurately identify abnormal traffic, a trial method is utilized. To determine the most effective features, we employ PSO-GA followed by the application of the LSTM-GRU model for superior classification results. To estimate the model's performance, several parameters are calculated, including false positives (F+), false negatives (F−), and two more values. The model's accuracy was evaluated using these parameters.

$$Accuracy = \left\{ \frac{(T+) + (T-)}{(T+) + (F-) + (F+) + (T-)} \right\} \tag{10}$$

This model structure and training approach has proven successful in achieving high accuracy in detecting and classifying various types of cyber attacks, as evidenced by the results presented in Table 3. To ensure accuracy, multiple epoch settings were utilized while considering the training and validation data loss. The model achieved greater than 96% accuracy for all attack types, with the Bot exhibiting the highest accuracy. Furthermore, the proposed LSTM-GRU model outperformed other Convolutional Neural Network models, achieving an average classification accuracy of 98.86%. The use of LSTM-GRU layers, along with the Adam optimizer and ReLU activation function, facilitates capturing temporal dependencies in the data and enhances the model's performance.

Table 3: Accuracy of the proposed IDS model on each attack

Attack	Accuracy
DoS	97.93
BruteForce	99.90
DDoS	98.60
Infiltration	97.12
WebAttacks	99.45
PortScan	99.08
Bot	99.98

Fig. 4 provides evidence of the usefulness of our proposed model. The results of the attack were aggregated and yielded an accuracy of 98.86%. The chart clearly shows that our model performed exceptionally well.

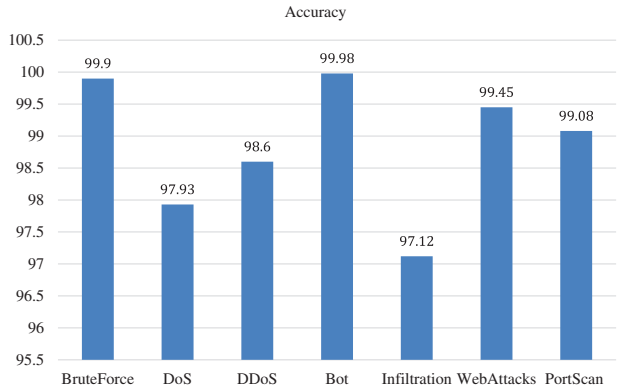

Figure 4: Accuracy of the proposed IDS model on different attacks

Below is an analysis and comparison of various works done in the cyber security domain, specifically on the CICIDS-2017 dataset. Table 4 compares the accuracy achieved by each method, including the proposed work. In [25], a combination of CNN and LSTM networks was used, achieving an accuracy of 98.67%. In [26], a CNN-GRU was used on the CICIDS-2017 dataset, achieving an accuracy of 98.73%. The proposed work utilized a fusion of PSO and GA to optimize the input features for the LSTM-GRU network, achieving an accuracy of 98.86%. Accordingly, both existing works were less accurate than the proposed work.

Table 4: Performance analysis of the proposed IDS model with state-of-the-art models

Reference	Method	Dataset	Accuracy
[25]	CNN-LSTM		98.67%
[26]	CNN–GRU	CICIDS-2017	98.73%
Proposed IDS model	PSO-GA followed by LSTM-GRU		98.86%

7 Conclusion

IoT-based systems offer a convenient way for users to access their data, but on the other hand, they also pose security risks that may compromise the confidentiality and integrity of the information. This research work proposes an intrusion detection model that employs an ensemble DL model. We combine evolutionary and swarm intelligence algorithms to select features for the model, namely PSO-GA. The selected features are then fused with the LSTM-GRU model to detect various types of attacks. The proposed method demonstrates remarkable accuracy in detecting attacks and achieves an accuracy of 98.86% on the CICIDS 2017 dataset, which is considered state-of-the-art. Future work will involve evaluating the model on other datasets using advanced DL techniques. The proposed IDS model achieves improving security in IoT-based systems.

Acknowledgement: This work was supported by the EIAS Data Science and Blockchain Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh Saudi Arabia, and the Department of Computer Engineering, Prince Sattam Bin Abdulaziz University, Saudi Arabia.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Saba, "Intrusion detection in smart city hospitals using ensemble classifiers," in *2020 13th Int. Conf. on Developments in eSystems Engineering (DeSE)*, Liverpool, United Kingdom, pp. 418–422, 2020.

[2] H. Shi, L. Zhai, H. Wu, M. Hwang, K. S. Hwang *et al.,* "A multitier reinforcement learning model for a cooperative multiagent system," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 12, no. 3, pp. 636–644, 2020. https://doi.org/10.1109/TCDS.2020.2970487

[3] T. Saba, T. Sadad, A. Rehman, Z. Mehmood and Q. Javaid, "Intrusion detection system through advance machine learning for the internet of things networks," *IT Professional*, vol. 23, no. 2, pp. 58–64, 2021. https://doi.org/10.1109/MITP.2020.2992710

[4] T. Saba, A. Rehman, T. Sadad, H. Kolivand and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, no. 1, pp. 1–14, 2022.

[5] Q. A. Al-Haija and A. Al-Badawi, "Attack-aware IoT network traffic routing leveraging ensemble learning," *Sensors*, vol. 22, no. 1, pp. 1–16, 2021. https://doi.org/10.3390/s22010241

[6] G. Bovenzi, G. Aceto, D. Ciuonzo, A. Montieri, V. Persico *et al.,* "Network anomaly detection methods in IoT environments via deep Learning: A fair comparison of performance and robustness," *Computers & Security*, vol. 128, no. 1, pp. 103–167, 2023. https://doi.org/10.1016/j.cose.2023.103167

[7] H. Zhao, Y. Feng, H. Koide and K. Sakurai, "An ANN based sequential detection method for balancing performance indicators of IDS," in *2019 Seventh Int. Symp. on Computing and Networking (CANDAR)*, Nagasaki, Japan, pp. 239–244, 2019.

[8] K. Samunnisa, G. S. V. Kumar and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," *Measurement: Sensors*, vol. 25, pp. 1–12, 2023.

[9] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," *Journal of Big Data*, vol. 7, no. 1, pp. 1–20, 2020. https://doi.org/10.1186/s40537-020-00379-6

[10] S. Rajagopal, P. P. Kundapur and K. S. Hareesha, "A stacking ensemble for network intrusion detection using heterogeneous datasets," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–9, 2020.

[11] T. Saba, A. R. Khan, T. Sadad and S. P. Hong, "Securing the IoT system of smart city against cyber threats using deep learning," *Discrete Dynamics in Nature and Society*, vol. 2022, no. 1, pp. 1–9, 2022.

[12] M. N. Alatawi, N. Alsubaie, H. U. Khan, T. Sadad, H. S. Alwageed *et al.,* "Cyber security against intrusion detection using ensemble-based approaches," *Security and Communication Networks*, vol. 2023, no. 1, pp. 1–7, 2023.

[13] R. M. Swarna Priya, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu *et al.,* "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, no. 1, pp. 139–149, 2020.

[14] A. A. Ewees, R. R. Mostafa, R. M. Ghoniem and M. A. Gaheen, "Improved seagull optimization algorithm using Lévy flight and mutation operator for feature selection," *Neural Computing and Applications*, vol. 34, no. 10, pp. 7437–7472, 2022.

[15] S. Ullah, J. Ahmad, M. A. Khan, E. H. Alkhammash, M. Hadjouni *et al.,* "A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering," *Sensors*, vol. 22, no. 10, pp. 1–16, 2022. https://doi.org/10.3390/s22103607

[16] R. Lohiya, A. Thakkar and A. Thakkar, "Intrusion detection using deep neural network with antirectifier layer," in *Applied Soft Computing and Communication Networks: Proc. of ACN 2020*, Singapore, vol. 187, pp. 89–105, 2021.

[17] L. Yanmiao, X. Yingying, Z. Liu, H. Hou, Y. Zheng *et al.,* "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, no. 1, pp. 1–10, 2020.

[18] S. Singh Panwar, Y. P. Raiwani and L. S. Panwar, "Evaluation of network intrusion detection with features selection and machine learning algorithms on CICIDS-2017 Dataset," in *Int. Conf. on Advances in Engineering Science Management & Technology (ICAESMT)*, Dehradun, India, Uttaranchal University, pp. 1–10, 2019.

[19] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg *et al.,* "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, no. 1, pp. 55–68, 2022. https://doi.org/10.1016/j.jpdc.2022.01.030

[20] V. Priyanka and T. G. Kumar, "Performance assessment of IDS based on CICIDS-2017 dataset," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020) ICT: Applications and Social Interfaces*, Singapore, pp. 611–621, 2022.

[21] Y. Xue, A. Aouari, R. F. Mansour and S. Su, "A hybrid algorithm based on PSO and GA for feature selection," *Journal of Cybersecurity*, vol. 3, no. 2, pp. 117–124, 2021.

[22] M. Poongodi, S. Bourouis, A. N. Ahmed, M. Vijayaragavan, K. G. S. Venkatesan *et al.,* "A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework," *Computer Communications*, vol. 192, no. 1, pp. 48–56, 2022.

[23] S. A. Changazi, A. D. Bakhshi, M. Yousaf, M. H. Islam, S. M. Mohsin *et al.,* "GA-based geometrically optimized topology robustness to improve ambient intelligence of future internet of things," *Computer Communications*, vol. 154, no. 1, pp. 109–117, 2020.

[24] K. Cho, B. V. Merriënboer, D. Bahdanau and Y. Bengio, "On the properties of neural machine translation: Encoder-decoder approaches," *arXiv preprint arXiv*:1409.1259, pp. 1–9, 2014.

[25] P. Sun, P. Liu, Q. Li, C. Liu, X. Lu *et al.,* "DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–11, 2020.

[26] A. Henry, S. Gautam, S. Khanna, K. Rabie, T. Shongwe *et al.,* "Composition of hybrid deep learning model and feature optimization for intrusion detection system," *Sensors*, vol. 23, no. 2, pp. 890, 2023.