Received: 10 April 2024 | Revised: 12 June 2024 | Accepted: 30 June 2024 | Published online: 9 July 2024

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2024, Vol. 00(00) 1–10
DOI: 10.47852/bonviewJCCE42023061

BON VIEW PUBLISHING

BSA-SGRU-A Novel Deep Learning Framework for Alleviate the Multiple Attacks in IoT-Cloud Environment

P. Jagdish Kumar[1,*] and Neduncheliyan Subbu[1]

[1]*Bharath Institute of Higher Education and Research, India*

Abstract: The Internet of Things (IoT) has emanated as an innovative technology that grants users to establish connections to external servers located in the cloud and the uninterrupted Internet, allowing them to live more comfortably. As the number of users increases, security and privacy breaches also increase exponentially, as it invests the greatest threats to the IoT networked devices and cloud storage. Though machine and deep learning algorithms have paved the bright light toward the design of intelligent systems to mitigate the attacks, creating effective defenses against numerous assaults remains a significant design challenge for researchers, and accurately predicting these attacks continues to pose an ongoing hurdle. To solve this problem, this paper proposes a hybrid learning model that ensembles the skip connection-based gated recurrent units (Skip-GRU) and bi-layered self-attention networks to predict and mitigate the different attacks. First, Skip-GRU is constructed using residual connections that remove redundant information and capture only global features. Second, novel bi-layered privacy-preserving networks are combined to obtain the spatial and temporal attributes. Finally, softmax is utilized to obtain the prediction results of sample labels. Performance parameters including accuracy, precision, recall, and F1-score are assessed and evaluated during the comprehensive eradication exploration that is conducted utilizing the NSL-KDD and UNSW datasets. By comparing how it performs to other cutting-edge approaches to learning, the one recommended demonstrates its superiority. The technique has proven its efficacy in providing enough security versus various threats, as seen by the results, which show that it has obtained 0.97 accuracy, 0.96 precision, 0.96 recall, and 0.96 F1-score.

Keywords: Internet of Things (IoT), cloud, security and private breaches, skip connection, GRU, self-attention, NSL-KDD datasets

1. Introduction

An industrial management tool known as the Internet of Things (IoT) is a network of gadgets that has revolutionized the surveillance and automation procedure context [1–4]. Many industries, including home, healthcare, automobiles, and even defense, use this diverse array of gadgets with complicated designs and varying functionality.

These devices are a combination of different stages such as electronic processing, sensors, actuators, and connectivity. The human expenditure of pervasive technology increases when IoT technologies are employed more widely, boosting the possibility of hackers and intruders exploiting networking safety and confidentiality as a result of network advancement.

Differing between dangerous and lawful network data can be challenging due to attackers' unexpected behavior [5–7]. IoT apps often operate on the notion of anywhere, anytime, and anything, interacting autonomously with a variety of appliances or gadgets. Due to the ease with which malevolent agents might get gadgets, harm to them is going to be inevitable and will be seen as an intrinsic danger.

Attack toolkits are also widely available on the Internet these days, having been produced [8–11]. However, with the least amount of work, hackers may use these technologies to further launch attacks. In order to create a security framework against IoT-cloud threats, more intelligent research is being focused on in the present day by utilizing myriad strategies. However, the numerous issues with these conventional systems include a lack of processing capacity, limited performance, and vulnerability to unforeseen attacks.

Security is considered as one of the crucial challenges in the IoT-cloud ecosystems. Challenges like feeble authentication and the absence of robust encryption and the absence of a non-intelligent cloud authorization mechanism can lead to the rise of many problems such as data breaches and leakage breaches. To defend against the attacks, several network measures are integrated into the IoT devices and cloud also. Artificial intelligence (AI) algorithms endeavor to tackle these security obstacles without the limitations of pre-established regulations.

Deep learning (DL), a facet of machine learning (ML), facilitates enhancement in performance, providing defensive characteristics against the multiple attacks in the present scenario. Methods based on "conventional deep neural networks, convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM), and even hybrid gated recurrent neural networks (HGRNN) (self-attention)" are used to design the intelligent systems to safeguard the IoT devices and data against the multiple attacks [12–14]. CNN are used to extract the spatial information, whereas LSTM and HGRNN algorithms are employed to

***Corresponding author:** P. Jagdish Kumar, Bharath Institute of Higher Education and Research, India. Email: pjagadishdcs19@bharathuniv.ac.

attain the temporal characteristics to aid in the better prediction of the attacks in the cloud environment.

However, these algorithms reflect their own disadvantages such as class imbalance problems, overfitting, and complexity overhead while handling the unpredictable behavior of attackers and consuming more computations that lead to the overhead in producing high performances. Therefore, it is imperative to solve the problems inherent in the above methods.

Motivated by the aforementioned problem, this paper proposes a novel combination of Skip-connected gated recurrent units (Skip-GRU) and bi-layered attention layers to cater to the needs for designing a defensive system that is both computationally effective and capable of high-performance prediction of multiple attacks such as DoS (denial of services). DDoS (distributed DoS) and MIM (man-in-middle) attacks. In order to mitigate numerous assaults, the paper's contribution involves using the positive aspects of the suggested approach, as shown below.

HGRNN based on residual principles are introduced in GRNN to succeed in better feature selection by removing the redundant features that aid for better feature selection.

Bi-layered attention maps are proposed and combined with the Skip-GRU networks to enhance better feature extraction that aids for better prediction of attacks.

Softmax-based feedfoward learning layers are familiarized in the place of the conventional training networks to accomplish low latency with high prediction ratio.

Extensive ablation studies and experiments are conducted and compared with the other state of DL frameworks in which the suggested framework has beaten the other frameworks.

The remainder of the piece is systematized as pursues: Section 2 furnishes contextual details and pertinent references, while Section 3 delineates the dataset particulars, data preprocessing techniques, and recommended methodologies. Section 4 provides an elaboration of the findings from the experiments. Section 5 concludes with recommendations for further enhancements.

2. Related Works

Using deep neural networks and conventional ML techniques, Ai et al. [15] created a secure cloud-based architecture. IoT devices and sensors are used by the system to gather patient readings, which are then safely sent to cloud storage via public key encryption. Subsequently, the predictive algorithm uses real-time data prediction to determine if the patient anticipates developing diabetes or not. The UCI Pima Indian diabetes dataset was used to evaluate the prediction methods. Based on the outcome, it outperforms 98% of the classic ML approaches. That being said, the primary shortcoming of this system is that it increased computational expenses.

Zhang et al. [16] have proposed an intelligent intrusion detection system (IDS) to counterfeit cloud attacks using swarm-optimized DL algorithms. The swarm methodologies are utilized to enhance the skip connection of the deep neural networks. The framework uses the 2D-CNN as classification networks to classify the network attacks. The authors used the Net-flow-based datasets for analyzing the framework and achieved a considerable good performance. Though the model yields good performance, computational complexity remains to be a challenge in deploying the system for obtaining better performances.

In order to allow devices to perform activities jointly by utilizing proximity and resource complementarity, Cañedo and Skjellum [17] introduced a "deep reinforcement learning (DRL)"-based data analytics framework. Data scheduling optimization is used to optimize data input in parallel and enhance the management of overall communication overhead. The findings of the simulation indicate that the suggested method does not require a priori IoT node information and instead leverages DRL to maximize execution speed and accuracy. In addition, the cost of awards, failure rate, and average delay time are calculated. However, data leaking in real-time situations is this framework's main flaw.

A novel IoT-enabled intelligent agriculture system for safe data exchange among its numerous actors is proposed by Wang et al. [18] in 2023, taking advantage of DL and smart contracts. To guarantee safe data transfer in IoT-enabled AI, this framework first created a new authentication and key management system. After then, the cloud server uses a cutting-edge DL architecture to analyze and find other breaches using the encrypted transactions. Yet, a real-time setting is not appropriate for this architecture.

Chakraborty et al., Kwabena et al., and Sekhar et al. [19–21] have proposed the deployment of artificial neural networks in the cloud to provide high-end security against network attacks. The framework was evaluated using NSL-KDD datasets, and performance metrics such as accuracy and false alarm rates were measured and analyzed. Though the accuracy of 0.97 is achieved, still the deployment complexity is high, which resists the system to safeguard the cloud data against intruding attacks.

The integration of ML and DL techniques into IDSs has significantly enhanced their ability to detect attacks on IoT networks. However, the opaque nature of ML/DL decision-making processes poses a challenge for cybersecurity experts who need to understand and act upon these decisions. To address this issue, recent studies have focused on explainable AI (XAI) to provide transparency and interpretability in ML/DL-based IDSs. Abou El Houda et al. [22] proposed a novel framework that combines deep neural networks with XAI models like RuleFit and SHapley Additive exPlanations (SHAP), demonstrating improved detection and explanation of IoT attacks, thereby enhancing trust and usability for cybersecurity professionals.

Awajan [23] introduces a DL-based IDS specifically designed for IoT networks, addressing the critical need for real-time detection of cyberattacks. The proposed IDS utilizes a four-layer fully connected deep neural network architecture that effectively identifies various types of malicious traffic, such as Blackhole, DDoS, Opportunistic Service, Sinkhole, and Workhole attacks. This system, independent of communication protocols, aims to simplify deployment and enhance security measures for IoT devices. Experimental results demonstrate its high performance, achieving an average detection accuracy of 93.74% and consistent precision, recall, and F1-scores of 93.71%, 93.82%, and 93.47%, respectively, thereby proving its efficacy in safeguarding IoT networks.

Mohan Das et al. [24] present a novel approach to enhancing security within the Social Internet of Things (SIoT), where IoT devices interact through social platforms, raising concerns about privacy and data security. The authors propose a multi-hop CNN with an attention mechanism to effectively detect attacks from malicious nodes within the network. This innovative model aims to categorize safe nodes and identify various types of fraudulent activities, addressing the shortcomings of previous methods that struggled to distinguish between different attack forms. The proposed system's performance is validated through comprehensive metrics, including accuracy, precision, recall, F1-score, and mean absolute error, showing significant improvements over existing techniques in safeguarding the SIoT environment.

Kowsalyadevi and Balaji [25] introduce IoBTSec-RPL, a hybrid DL-based model designed to enhance the security of the Internet of Battlefield Things (IoBT) by detecting routing protocol (RPL) attacks. Recognizing the low-security features of RPL

in IoBT environments, this model aims to address vulnerabilities due to device heterogeneity and open wireless communications. The IoBTSec-RPL framework includes preprocessing through min-max normalization and missing value imputation, feature selection via an enhanced pelican optimization algorithm, data augmentation with an auxiliary classifier gated adversarial network, and attack detection using a combination of LSTM and Deep Belief Network (DBN). Experimental results demonstrate the model's effectiveness, achieving a recall of 98.93% and outperforming other models like LGBM, LSTM, and DBN by 2.16%, 5.73%, and 6.06% in accuracy for 200,000 traffic samples, thereby providing robust security for IoBT environments.

An approach to securing the architecture of intelligent transportation systems that preserves privacy and is based on security was given by Kumar et al. [26] in 2022. The "long-hyperparameters memory-auto encoder (LSTM-AE)" approach is incorporated into this DL module of the framework to encode cloud data into a new format and thwart inference assaults. Though not appropriate for dense networks, this architecture performs better in terms of attack detection.

With the introduction of the "Deep Blockchain Framework (DBF)" by Alkadi et al. [27] in 2021, the goal is to enable security-based distributed intrusion detection and privacy-based blockchain technology in IoT networks using smart contracts. In terms of consecutive network data, the "UNSW-NB15 and BoT-IoT" datasets are used to assess the intrusion detection approach. One DL algorithm that makes use of it is called bidirectional LSTM. The framework may be used as a tool for decision-making to assist clients and cloud service suppliers in migrating their data securely, swiftly, and consistently. Nevertheless, there is a lot of computational complexity.

Li et al. [28] created a CNN inference system that depends on IoT-edge-cloud cooperation. By adopting an encryption technique, sensor information and parameters for models are shielded from tampering and disclosure. Model parameters are lowered for transmission and encryption using a seed-filter-based approach, without sacrificing interpretation efficiency. Based on the security evaluation, we can utilize our cryptography approaches to defend against MIM attacks. However, there are serious temporal complexity issues with this system in a real-time situation.

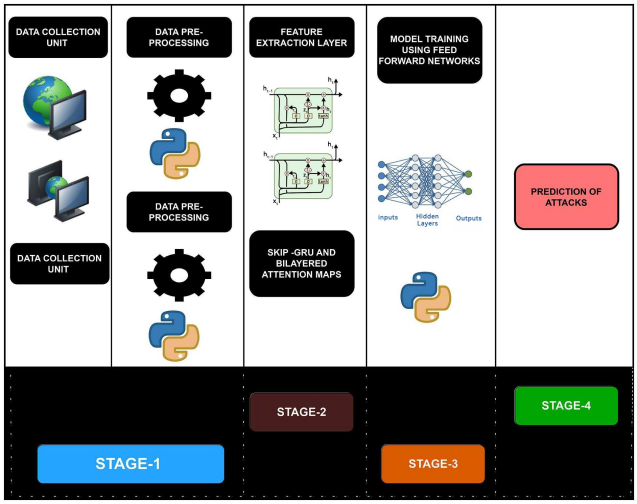
3. Research Methodology

Figure 1 depicts the suggested structure for anticipating assaults in an IoT-cloud constellation. Three phases make up the proposed structure. In the first stage, multiple attacks and normal data are collected using the data collection unit. Data Short-Term was implemented in the second stage, followed by feature extraction using the proposed Skip-gated units ensemble with bi-layered attention maps. Finally, softmax-based feedforward layers were deployed to predict the multiple attacks. The suggested system predicts the following in the case of an assault. (1) Are these nodes malicious or normal? (2) What kind of assaults took place? The following lists every step's comprehensive description:

3.1. Materials and methods

Additionally, we ran our trials on the recently released UNSW-NB15 dataset, which is accessible to the public [29]. There are one class characteristic and 49 features in the dataset. UNSW_NB15_Train and UNSW_NB15_Test, two smaller datasets, are utilized as train and test sets, respectively. The validation of classifiers is then carried out using the NSL-KDD dataset as well. There are one class attribute and 41 features in the dataset. This work

Figure 1
Proposed framework used for prediction of multiple attacks in IoT-cloud environment



makes use of the "NSL_KDD [30] dataset's KDDTrain+ (training) and KDDTest+ (testing) sets".

3.2. Proposed training network

This division delves into the operational mechanism of the gated RNNs and proposed ensemble model.

3.3. Gated recurrent units

"LSTM" is thought to have its most fascinating variation in GRU. To merge the input vector and forget gate into a single vector, Pandya et al. [31] presented this concept. Long-term memory and sequencing are sustained by this network. Comparing the complication to the LSTM network, there is a significant decrease.

Chung introduced the following equations to represent the distinctive attributes of GRU:

$$h_t = (1 - x_t) \odot h_{t-1} + x_t \odot h_t \tag{1}$$

$$\tilde{h}_t = g(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \tag{2}$$

$$z_t = \sigma(W_h x_t + U_z h_{t-1} + b_z) \tag{3}$$

$$r_t = \sigma(W_h x_t + U_r h_{t-1} + b_r) \tag{4}$$

The overall GRU's characteristics are represented by the following equation:

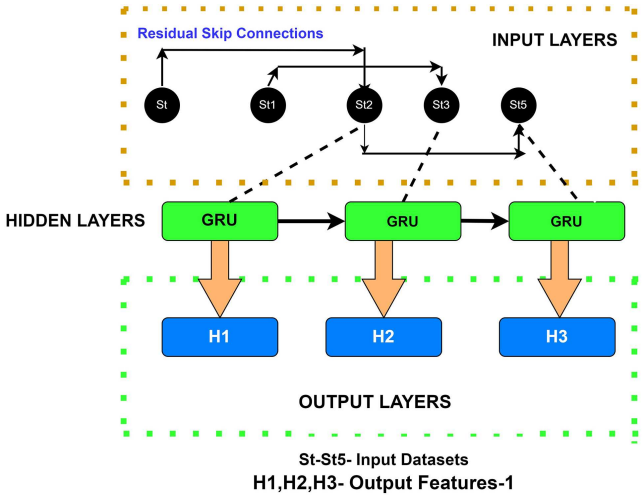
$$P = \mathrm{GRU}(\sum_{t=1}^{n} [x_t, h_t, z_t, r_t(W(t), B(t), \eta(\tanh))]) \tag{5}$$

where "x_t represents the current input feature, y_t denotes the output state, h_t signifies the module's output at the current moment, while Z_t and r_t stand for the update and reset gates, respectively. Additionally, $W(t)$ refers to the current instant's weights, and $B(t)$ represents the bias weights".

3.4. Skip-connected GRU networks

As mentioned in Taheri et al. [32], skip connections play an important role in U-NETS, which directly maps the features of different structures. The role of skip connections in the proposed model is to calculate the probability of skipping (Pk) to determine the redundant information and reserve the important feature in GRU networks. Figure 3 illustrates the proposed Skip-GRU architecture. The skip connection network is embedded in the standard GRU. In this model, skip connection consists of two convolutional layers followed by batch normalization, residual block, and an activation function Leaky ReLU layers (LReLU). The proposed skip connection uses a residual block to remove the vanishing gradient problem and remove the repeated information. The data needs to be input into the proposed skip connection, and the *Pk* is calculated based on the blocks involved in designing the proposed Skip-GRU networks as shown in Figure 2.

Figure 2
Proposed Skip-GRU architecture for the feature extraction



Mathematically, the Skip-GRU networks are expressed as

$$H(t) = \mathrm{LReLU}(\mathrm{Res}(W1.S1 * b1)) \tag{6}$$

$$Pk = \mathrm{Softmax}(\mathrm{Res}(W2.H(t) * b2)) \tag{7}$$

where $W1$, $W2$, $b1$, and $b2$ are weights and biases of the convolutional layers and $H(t)$ is the hidden state.

3.5. Self-attention maps

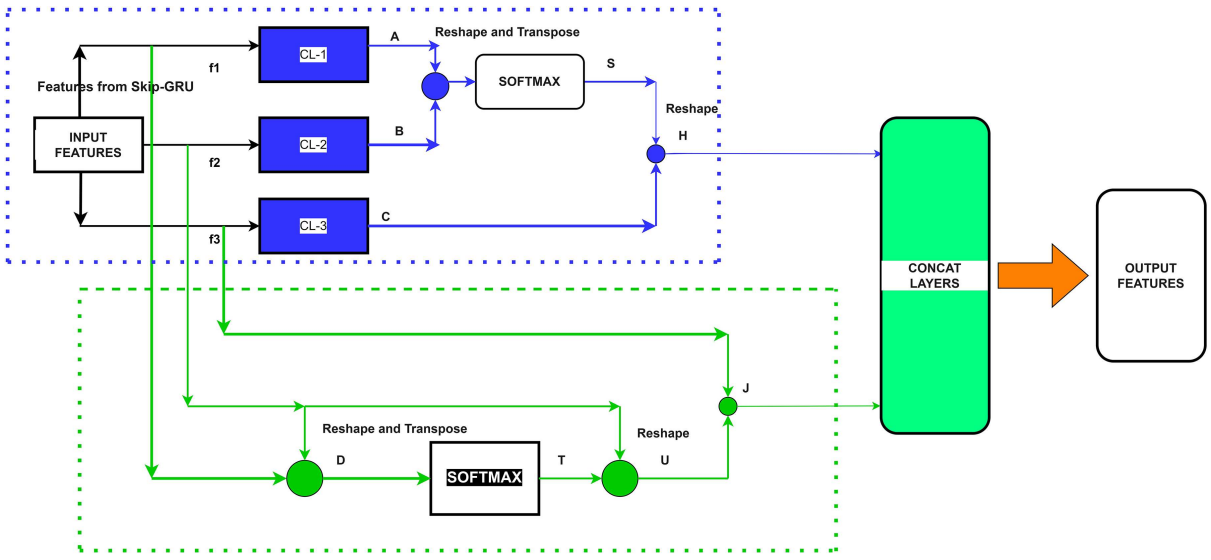
For the purpose of improving the selection of appropriate words in sequence-to-sequence design, the attention map was introduced in 2014. The addition of attention layers to simulate repetitive attributes that can support accurate categorization mechanisms has been a current trend in most research. "Producing the three vectors *Q, K*, and *V* for each input sequence is how the preprocessing mechanism, sometimes directed to the intra-attention mechanism, operates. This results in the output sequences being changed from the input patterns of each layer. To put it another way, this strategy utilizes scaled dot operations to map the query to the collection of key pairs. The following is the computational calculation of the dot product for self-attention".

$$F(K, Q) = ((K), Q^{\mathrm{T}})/(V_{\mathrm{K}})\text{^}0.5 \tag{8}$$

3.6. Bi-layered attention maps

Figure 3 depicts the proposed "bi-layered attention (BLA)" maps. The proposed BLA consists of position self-attention (PSA) and channel attention (CA). The combination of these attention networks aids for an effective feature extraction that aids for better prediction of attacks. The input temporal features from Skip-GRU are fed to the proposed BLA networks. The PSA layer consists of three convolutional layers with the softmax activation layers and uses unique strategies for the generation of attention maps as shown in Figure 4. The softmax activation layer receives input from the channel attention network, which performs operations such as multiplication and addition. The output from the two attention layers is finally concatenated to form the final attention maps. Equations (8),

Figure 3
Construction diagram for the proposed bi-channel attention maps



(9), and (10) details the mathematical process carried out on the PSA and CA networks, whereas Equation (4) displays the entire mathematical operations performed in the BLA module.

$$Y = H + J \tag{9}$$

$$H = S(\mathrm{x}) = \mathrm{Softmax}\,(\mathrm{Transpose}\,(A) + (B)) \tag{10}$$

$$Y = S(x) = \mathrm{Softmax}\,(\mathrm{Transpose}(A + B) + J) \tag{11}$$

$$J = T + U \tag{12}$$

$$T = \mathrm{Softmax}\,(\mathrm{Transpose}(A.B)) \tag{13}$$

$$J = \mathrm{Softmax}\,(\mathrm{Transpose}(A.B.C) + U) \tag{14}$$

where *"Y"* is the bi-layered attentions' feature maps, f): H is PSAs' feature maps, J: CAs' feature maps, *A, B, C*): feature maps of three parallel convolutional operations, $U(x)$: The process involves the multiplication of feature maps obtained from reshaped and transposed input feature maps. The operations of "." and "+" represent element-wise product and addition, respectively, of these feature maps.

3.7. Softmax-based feedforward classification networks

Ultimately, the "fully linked feedforward network" receives these characteristics for final categorization. Based on extreme learning machines (ELM) theory, the completely linked layers are created. Working on the premise of auto-tuning property, the ELM operates with great speed and minimal computing overhead; a thorough discussion of its operation may be found in Aldweesh et al. [33]. Pursuing the "attention maps, the input feature maps of the ELM are depicted" as

$$X = F(Y) \tag{15}$$

where Y gives the features from SKIP-GRU-BLA,

Denoting the output ELM function is

$$Y(n) = X(n)\,\beta = X(n)\,X^T\left(\frac{1}{\mathrm{C}}XX^T\right)^{-1}\mathrm{O} \tag{16}$$

The general instruction for ELM is provided through

$$T = \alpha(\sum_{n=1}^{N}(Y(n),\, B(n),\, W(n))) \tag{17}$$

Lastly, in order to attain the highest accuracy, the softmax activation layers have been added to the feedforward layers mentioned before. Algorithm 1 presents the working principle of the proposed model as shown in Table 1.

4. Execution Process

The complete algorithm was developed using the "Intel Workstation with I7 CPU with NVIDIA GPU, 16GB RAM, and 3.2 GHZ frequency". The initial framework design was crafted utilizing Keras with TensorFlow as its underlying framework.

Table 1
Algorithm 1: Working principle of the proposed model

Steps	Algorithm 1/Suggested framework's pseudocode
1	Input: Data From the IoT networks
2	Output: Malicious /Attack Prediction
3	For n = 1 to Nmax
4	Feature Extraction Process using Equation (15)
5	Train the network using Equation (18)
6	If (T == 1)
7	/Normal Condition Exists
8	Else if (T == 2)
9	/Malicious Attack is found
10	Else
11	Redirect to Step 6
12	End
13	End
14	End
15	End

4.1. Performance metrics

Deep feedforward training networks that categorize the appropriate classifications into "normal, sensitive, and attack data" are used in the experiments to validate the design that was suggested. Evaluation metrics such as "recall, sensitivity, accuracy, specificity, and F1-score" are measured to assess the proposed scheme's productivity. Table 2 displays the mathematical procedures for measuring the metrics that were employed to assess the advised structure. Table 3 also shows the study's hyperparameters that were employed to train the advised framework by using the 50 trial and error experimentation.

Table 2
Formulae of evaluation metrics for the suggested framework

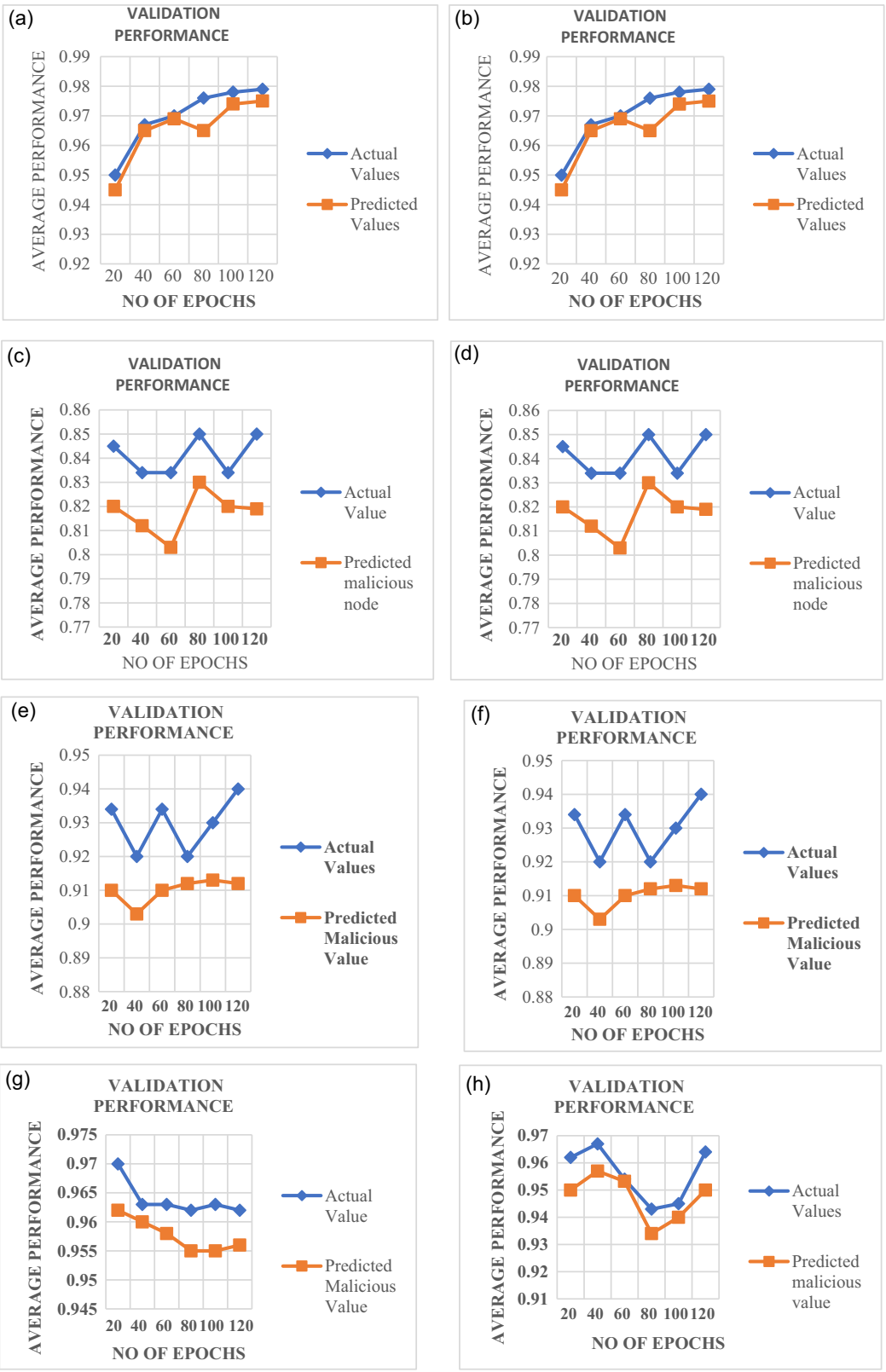
SL.NO	Evaluation boundaries	Formulae
01	Accuracy (Acc)	$\frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$
02	Sensitivity or recall (Sens)	$\frac{\mathrm{TP}}{\mathrm{TP+FN}}$ x100
03	Specificity (Scy)	$\frac{\mathrm{TN}}{\mathrm{TN+FP}}$
04	Precision (Pcsn)	$\frac{\mathrm{TN}}{\mathrm{TP+FP}}$
05	F1-score (Fscr)	$2.\frac{\mathrm{Precison*Recall1}}{\mathrm{Precision+Recall1}}$

Note: "TP is true positive values, TN is true negative values, FP is false positive, and FN is false negative".

Table 3
Hyperparameters during the suggested framework's training phase

Sl.no	Hyperparameters	Specifications
1	No of GRU cells	10
2	Epochs count	129
3	Total batch size	32
4	Rate of learning	0.001
5	Momentum	0.2
6	Dropouts	0.2

Figure 4
Validation performance of different models in handling the NSL-KDD and UNSW datasets. (a) and (b) Proposed model, (c) and (d) LSTM model, (e) and (f) H-GRU, (g) optimized GRU, and (h)A-BiGRU



4.2. Results and discussion

The testing is conducted using component architectures that have the same specifications as the suggested framework. Specifications of the residing frameworks included "one-dimensional LSTM [34], hybrid GRU [35], optimized LSTM [36], and attention-based BiGRU(A-BiGRU) [37]". For validating the algorithm, a comparative analysis has been conducted utilizing four distinct datasets.

Figure 4 shows how well the various models performed during validation while dealing with the NSL-KDD and UNSW datasets.

It is clear from Figure 4(a) and (b) that the suggested system's "root mean square error (RMSE)" is 0.0124, while the RMSE of the other versions ranged from 0.0290 to 0.0450, respectively (Figure 4(c)–(h)). The inclusion of the BLA models in the Skip-GRU has produced less error of prediction that is evident from Figure 4(a and b). The average performance metrics of the proposed model and other models are listed in Tables 4, 5 and 6.

Table 4
Performance measures using UNSW2019 datasets for various algorithms

Algorithms	Evaluation boundaries				
	Acc	Pcsn	Sens	Scy	Fscr
LSTM	0.823	0.812	0.864	0.150	0.86
Hybrid GRU	0.912	0.90	0.89	0.110	0.91
Optimized-GRU	0.902	0.91	0.90	0.100	0.92
A-BIGRU	0.964	0.945	0.92	0.101	0.934
Proposed model	0.975	0.98	0.974	0.011	0.983

Table 5
Evaluations of performance with NSL-KDD+(training) datasets for various approaches

Algorithms	Evaluation boundaries				
	Acc	Pcsn	Sens	Scy	Fscr
LSTM	0.874	0.87	0.864	0.150	0.86
Hybrid GRU	0.902	0.90	0.89	0.110	0.91
Optimized-GRU	0.910	0.91	0.90	0.100	0.92
A-BIGRU	0.964	0.945	0.92	0.101	0.934
Proposed model	0.983	0.98	0.974	0.011	0.983

Table 6
Evaluations of performance with NSL-KDD+(test) datasets for various approaches

Algorithms	Evaluation boundaries				
	Acc	Pcsn	Sens	Scy	Fscr
LSTM	0.874	0.87	0.864	0.150	0.86
Hybrid GRU	0.902	0.90	0.89	0.110	0.91
Optimized-GRU	0.910	0.91	0.90	0.100	0.92
A-BIGRU	0.964	0.945	0.92	0.101	0.934
Proposed model	0.983	0.98	0.974	0.011	0.983

The suggested algorithm's and other approaches' performance in managing the various datasets is shown in Tables 4, 5 and 6. Based on the data, it is evident that the recommended approach has surpassed the other approaches with regard to "recall, F1-score, high accuracy, and high precision".

4.3. Statistical performance

Statistical performance outcomes have been added and compared with the other existing models. In this experimentation, several existing meta-heuristic algorithms are taken into consideration. To prove the excellence of the proposed model, several meta-heuristic algorithms integrated with the CNN+GRU have been experimented with in which the outcomes are in-cultivated and compared with the proposed model. The meta-heuristic algorithms used for experimentation are particle swarm optimization (PSO) [38], genetic algorithm (GA) [39], whale optimization algorithm(WOA) [40], spotted hyena optimization (SHO) [41], and hybrid-reptile search optimization (HRSO) [42–44]. These well-performing optimizers are included in the proposed DL architectures, and validation is carried out by comparing them with the proposed architecture in the model. Tables 7 and 8 illustrate the statistical performance of the different models.

From the above Tables 7 and 8, it is very clear that the proposed model is statistically fit for optimizing the features that can aid for the best classification mechanism.

4.4. Time complexity analysis

Time complexity analysis has been analyzed using the model building time (MBT). Table 9 illustrates the different MBT analyses of the different algorithms in training the different datasets.

Table 9 lists out model building time (MBT) of different classifiers across four datasets with holdout validation. The main reason behind computing MBT is that it is very important to consider the training time a model takes, as it would directly impact the resources usage and also the performance of the model in detecting the various attacks. Thus, MBT helps in making a good trade-off between the computational overhead and classification performance of a classifier. From the above table, the average MBT of the proposed model is 0.37 s for training the different datasets, whereas hybrid-LSTM has consumed 0.61 s, GRU consumes 0.76 s, and LSTM consumes 0.89, respectively. From the analysis, it can be concluded that the proposed model consumes only 0.37 s and finds its strong place in designing the defense system against the multiple attacks.

Table 7
Fitness function-based outcomes for the different combinations of optimizers

Algorithm	Best	Worst	Mean	Median	SD	Variance
PSO	0.72	0.693	0.702	0.0201	0.0343	5.84×10^{-6}
GA	0.72	0.703	0.6754	0.0210	0.0533	5.900×10^{-6}
WOA	0.73	0.719	0.6348	0.0267	0.0632	6.90×10^{-5}
SHO	0.76	0.745	0.7464	0.0933	0.06563	3.390×10^{-4}
HRSO	0.83	0.805	0.4563	0.0435	0.03893	3.78×10^{-4}
Proposed model	0.97	0.903	0.8433	0.0453	0.03032	3.03×10^{-4}

Table 8
Indicator function-based outcomes for the different combinations of optimizers

Algorithm	Best	Worst	Mean	Median	SD	Variance
PSO	0.752	0.6930	0.702	0.02019	0.0343	5.84×10^{-6}
GA	0.743	0.703	0.6754	0.02102	0.0533	5.900×10^{-6}
WOA	0.762	0.719	0.63489	0.02675	0.0632	6.90×10^{-5}
SHO	0.772	0.745	0.7464	0.09333	0.06563	3.390×10^{-4}
HRSO	0.8292	0.8054	0.45637	0.04353	0.03893	3.78×10^{-4}
Proposed model	0.9654	0.903	0.8433	0.04536	0.03032	3.03×10^{-4}

Table 9
MBT for the different algorithms using different datasets

Datasets	(MBT)-secs			
	LSTM	GRU	Hybrid -LSTM	Proposed model
UNSW	0.89	0.79	0.60	0.39
NSL-KDD++ Train	0.902	0.703	0.63	0.38
NSL-KDD++ Test	0.902	0.756	0.66	0.40
Average MBT	0.89	0.76	0.61	0.37

5. Conclusion and Future Enhancement

An innovative Skip-GRU ensemble with self-attention BLA maps is presented in this research to protect cloud and IoT devices against the growing number of threats. The BLA in Skip-GRU is essential for removing nonoptimal features and reducing computational load, both of which have an impact on classification performance. Once more, the entire algorithm is trained using cutting-edge softmax-based feedforward layers in order to get a higher performance ratio. Two different datasets, UNSW and NSL-KDD++, are used in the comprehensive testing, and performance indicators are analyzed and assessed. The advantage of the proposed method is demonstrated by a performance evaluation with other DL strategies. The recommended model has outperformed in terms of minimal overhead and high detection ratio. As the suggested paradigm expands, its effectiveness must be confirmed using real-time statistics and more robust encryption techniques (bidirectional models) to manage resource-constrained IoT and cloud gadgets.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data available on request from the corresponding author upon reasonable request.

Author Contribution Statement

P. Jagdish Kumar: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Neduncheliyan Subbu:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

References

[1] Kolhar, M., & Aldossary, S. M. (2023). A deep learning approach for securing IoT infrastructure with emphasis on smart vertical networks. *Designs, 7*(6), 139. https://doi.org/10.3390/designs7060139

[2] Nizamudeen, S. M. T. (2023). Intelligent intrusion detection framework for multi-clouds–IoT environment using swarm-based deep learning classifier. *Journal of Cloud Computing, 12*(1), 134. https://doi.org/10.1186/s13677-023-00509-4

[3] Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., ..., & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet, 14*(3), 89. https://doi.org/10.3390/fi14030089

[4] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering, 99,* 107810. https://doi.org/10.1016/j.compeleceng.2022.107810

[5] Yan, Z., Yang, G., He, R., Yang, H., Ci, H., & Wang, R. (2023). Ship trajectory clustering based on trajectory resampling and enhanced birch algorithm. *Journal of Marine Science and Engineering, 11*(2), 407. https://doi.org/10.3390/jmse11020407

[6] Liu, X., Liu, Y., Liu, A., & Yang, L. T. (2018). Defending ON–OFF attacks using light probing messages in smart sensors for industrial communication systems. *IEEE Transactions on Industrial Informatics, 14*(9), 3801–3811. https://doi.org/10.1109/TII.2018.2836150

[7] Guo, Y., Wang, Y., Khan, F., Al-Atawi, A. A., Abdulwahid, A. A., Lee, Y., & Marapelli, B. (2023). Traffic management in IoT backbone networks using GNN and MAB with SDN orchestration. *Sensors, 23*(16), 7091. https://doi.org/10.3390/s23167091

[8] Sivaramakrishnan, R., & SenthilKumar, G. (2024). Workload characterization in embedded systems utilizing hybrid intelligent gated recurrent unit and extreme learning machines.

International Journal of Intelligent Systems and Applications in Engineering, 12, 233–243.

[9] Jagadeesan, J., Subashree, D., & Kirupanithi, D. N. (2023). An optimized ensemble support vector machine-based extreme learning model for real-time big data analytics and disaster prediction. *Cognitive Computation, 15*(6), 2152–2174. https://doi.org/10.1007/s12559-023-10176-x

[10] Dixit, P., Kohli, R., Acevedo-Duque, A., Gonzalez-Diaz, R. R., & Jhaveri, R. H. (2021). Comparing and analyzing applications of intelligent techniques in cyberattack detection. *Security and Communication Networks, 2021*(1), 5561816. https://doi.org/10.1155/2021/5561816

[11] Sriranjani, R., Bharath Kumar, M., Paramesh, A. K., Saleem, M. D., Hemavathi, N., & Parvathy, A. (2023). Machine learning based intrusion detection scheme to detect replay attacks in smart grid. In *IEEE International Students' Conference on Electrical, Electronics and Computer Science,* 1–5. https://doi.org/10.1109/SCEECS57921.2023.10063021

[12] Jothi, B., & Pushpalatha, M. (2023). WILS-TRS—A novel optimized deep learning based intrusion detection framework for IoT networks. *Personal and Ubiquitous Computing, 27*(3), 1285–1301. https://doi.org/10.1007/s00779-021-01578-5

[13] Qureshi, T. N., Khan, Z. A., Javaid, N., Aldegheishem, A., Rasheed, M. B., & Alrajeh, N. (2023). Elephant herding robustness evolution algorithm with multi-clan co-evolution against cyber attacks for scale-free internet of things in smart cities. *IEEE Access, 11,* 79056–79072. https://doi.org/10.1109/ACCESS.2023.3298559

[14] Mahajan, N., Chauhan, A., Kumar, H., Kaushal, S., & Sangaiah, A. K. (2022). A deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems. *Mobile Networks and Applications, 27*(4), 1423–1443. https://doi.org/10.1007/s11036-022-01973-z

[15] Ai, Z., Zhang, W., Li, M., Li, P., & Shi, L. (2023). A smart collaborative framework for dynamic multi-task offloading in IIoT-MEC networks. *Peer-to-Peer Networking and Applications, 16*(2), 749–764. https://doi.org/10.1007/s12083-022-01441-1

[16] Zhang, C., Yang, S., Mao, L., & Ning, H. (2024). Anomaly detection and defense techniques in federated learning: A comprehensive review. *Artificial Intelligence Review, 57*(6), 150. https://doi.org/10.1007/s10462-024-10796-1

[17] Cañedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. In *14th Annual Conference on Privacy, Security and Trust,* 219–222. https://doi.org/10.1109/PST.2016.7906930

[18] Wang, X., Han, Y., Leung, V. C. M., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(2), 869–904. https://doi.org/10.1109/COMST.2020.2970550

[19] Chakraborty, A., Kumar, M., & Chaurasia, N. (2023). Secure framework for IoT applications using Deep Learning in fog Computing. *Journal of Information Security and Applications, 77,* 103569. https://doi.org/10.1016/j.jisa.2023.103569

[20] Kwabena, O. A., Qin, Z., Zhuang, T., & Qin, Z. (2019). MSCryptoNet: Multi-scheme privacy-preserving deep learning in cloud computing. *IEEE Access, 7,* 29344–29354. https://doi.org/10.1109/ACCESS.2019.2901219

[21] Sekhar, J. N. C., Domathoti, B., & Santibanez Gonzalez, E. D. R. (2023). Prediction of battery remaining useful life using machine learning algorithms. *Sustainability, 15*(21), 15283. https://doi.org/10.3390/su152115283

[22] Abou El Houda, Z., Brik, B., & Senouci, S. M. (2022). A novel IoT-based explainable deep learning framework for intrusion detection systems. *IEEE Internet of Things Magazine, 5*(2), 20–23. https://doi.org/10.1109/IOTM.005.2200028

[23] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers, 12*(2), 34. https://doi.org/10.3390/computers12020034

[24] Mohan Das, R., Arun Kumar, U., Gopinath, S., Gomathy, V., Natraj, N. A., Anushkannan, N. K., & Balashanmugham, A. (2023). A novel deep learning-based approach for detecting attacks in social IoT. *Soft Computing.* https://doi.org/10.1007/s00500-023-08389-1

[25] Kowsalyadevi, K., & Balaji, N. V. (2023). IoBTSec-RPL: A novel RPL attack detecting mechanism using hybrid deep learning over battlefield IoT environment. *International Journal of Computer Networks and Applications, 10*(4), 637–650. https://doi.org/10.22247/ijcna/2023/223317

[26] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Kumar, N., & Hassan, M. M. (2022). A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. *IEEE Transactions on Intelligent Transportation Systems, 23*(9), 16492–16503. https://doi.org/10.1109/TITS.2021.3098636

[27] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2021). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal, 8*(12), 9463–9472. https://doi.org/10.1109/JIOT.2020.2996590

[28] Li, J., Li, Y., Ding, C., Yu, J., & Ren, Y. (2022). Identity-based secure and efficient intelligent inference framework for IoT-cloud system. In *IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming,* 1–6. https://doi.org/10.1109/PAAP56126.2022.10010411

[29] Karri, C., & Naidu, M. S. R. (2020). Deep learning algorithms for secure robot face recognition in cloud environments. In *IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking,* 1021–1028. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00154

[30] Wang, W., Du, X., Shan, D., Qin, R., & Wang, N. (2022). Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. *IEEE Transactions on Cloud Computing, 10*(3), 1634–1646. https://doi.org/10.1109/TCC.2020.3001017

[31] Pandya, S. B., Kalita, K., Jangir, P., Ghadai, R. K., & Abualigah, L. (2024). Multi-objective Geometric Mean Optimizer (MOGMO): A novel metaphor-free population-based math-inspired multi-objective algorithm. *International Journal of Computational Intelligence Systems, 17*(1), 91. https://doi.org/10.1007/s44196-024-00420-z

[32] Taheri, R., Ahmed, H., & Arslan, E. (2023). Deep learning for the security of software-defined networks: A review. *Cluster Computing, 26*(5), 3089–3112. https://doi.org/10.1007/s10586-023-04069-9

[33] Aldweesh, A., Kodati, S., Alauthman, M., Aqeel, I., Khormi, I. M., Dhasaratham, M., & Lakshmana Kumar, R. (2024). Mlora-CBF: Efficient cluster-based routing protocol against

resource allocation using modified location routing algorithm with cluster-based flooding. *Wireless Networks, 30*(2), 671–693. https://doi.org/10.1007/s11276-023-03506-2

[34] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Transactions on Network and Service Management, 16*(3), 924–935. https://doi.org/10.1109/TNSM.2019.2927886

[35] Kalaivani, M., & Padmavathi, G. (2023). Ensembling of attention-based recurrent units for detection and mitigation of multiple attacks in cloud. *International Journal of Advanced Computer Science and Applications, 14*(10), 86–92. https://doi.org/10.14569/IJACSA.2023.0141010

[36] Kalpana, P., Anandan, R., Hussien, A. G., Migdady, H., & Abualigah, L. (2024). Plant disease recognition using residual convolutional enlightened Swin transformer networks. *Scientific Reports, 14*(1), 8660. https://doi.org/10.1038/s41598-024-56393-8

[37] Kalpana, P., & Anandan, R. (2023). A capsule attention network for plant disease classification. *Traitement du Signal, 40*(5).

[38] Kalpana, P., Chanti, Y., Ravi, G., Regan, D., & Pareek, P. K. (2023). SE-Resnet152 model: Early corn leaf disease identification and classification using feature based transfer learning technique. In *International Conference on Evolutionary Algorithms and Soft Computing Techniques,* 1–6. https://doi.org/10.1109/EASCT59475.2023.10392328

[39] Gurrola-Ramos, J., Hernàndez-Aguirre, A., & Dalmau-Cedeño, O. (2020). COLSHADE for real-world single-objective constrained optimization problems. In *IEEE Congress on Evolutionary Computation,* 1–8. https://doi.org/10.1109/CEC48606.2020.9185583

[40] LaTorre, A., Molina, D., Osaba, E., Poyatos, J., Del Ser, J., & Herrera, F. (2021). A prescription of methodological guidelines for comparing bio-inspired optimization algorithms. *Swarm and Evolutionary Computation, 67,* 100973. https://doi.org/10.1016/j.swevo.2021.100973

[41] Jovanovic, L., Jovanovic, D., Bacanin, N., Jovancai Stakic, A., Antonijevic, M., Magd, H., ..., & Zivkovic, M. (2022). Multi-step crude oil price prediction based on LSTM approach tuned by salp swarm algorithm with disputation operator. *Sustainability, 14*(21), 14616. https://doi.org/10.3390/su142114616

[42] Kalpana, P., Almusawi, M., Chanti, Y., Kumar, V. S., & Rao, M. V. (2024). A Deep reinforcement learning-based task offloading framework for edge-cloud computing. In *International Conference on Integrated Circuits and Communication Systems,* 1–5. https://doi.org/10.1109/ICICACS60521.2024.10498232

[43] Abualigah, L., Al-Ajlouni, Y. Y., Daoud, M. S., Altalhi, M., & Migdady, H. (2024). Fake news detection using recurrent neural network based on bidirectional LSTM and GloVe. *Social Network Analysis and Mining, 14*(1), 40. https://doi.org/10.1007/s13278-024-01198-w

[44] Bacanin, N., Jovanovic, L., Zivkovic, M., Kandasamy, V., Antonijevic, M., Deveci, M., & Strumberger, I. (2023). Multivariate energy forecasting via metaheuristic tuned long-short term memory and gated recurrent unit neural networks. *Information Sciences, 642,* 119122. https://doi.org/10.1016/j.ins.2023.119122

How to Cite: Jagdish Kumar, P., & Subbu, N. (2024). BSA-SGRU-A Novel Deep Learning Framework for Alleviate the Multiple Attacks in IoT-Cloud Environment. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE42023061