Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

An Avant-Garde African Vulture Optimization (A^2VO) based Deep RNN-LSTM Model for 5G-IoT Security

Gopalakrishnan Ramasubramanian[1,*], Singaravelu Rajaprakash[2]

[1] Faculty of Arts and Science, Vinayaka Missions Research Foundation, Salem, Tamilnadu State-636308, India
[2] Department of Computer Science and Engineering, Aarupadaiveedu Institute of Technology, Vinayaka Missions Research Foundation, Paiyanoor, Chengalpattu District. TamilNadu State-613104, India

ARTICLE INFO

Article history:
Received 8 May 2023
Received in revised form 27 July 2023
Accepted 4 August 2023
Available online 18 August 2023

Keywords:
Intrusion Detection System (IDS); 5G Wireless Networks; Internet of Things (IoT); security; Avant-Garde African Vulture Optimization (A^2VO); Recurrent Neural Network (RNN) – Long Short Term Memory (LSTM)

ABSTRACT

In current days, 5G is more essential for the Internet of Things (IoT) systems, since it offers a quicker network with more capacity to address communication needs. The frequency range that mobile communication technologies employ to transfer data is expanded by the 5G spectrum. However, it also broadens the presence of attacks within the core network, increasing the corporate system's susceptibility to security intrusions. Hence, various Intrusion Detection System (IDS) frameworks are developed in the conventional works for 5G-IoT network security. However, the significant challenges of the existing studies are complexity burden, high processing time, and ineffective intrusion detection. Therefore, the proposed work intends to implement a novel Avant-Garde African Vulture Optimization (A^2VO), and Recurrent Neural Network (RNN) – Long Short-Term Memory (LSTM) mechanism of 5G-IoT security. The min-max normalization technique is used to preprocess the attributes and fields in the dataset. In addition, a precise and effective deep Recurrent Neural Network (RNN) - Long Short Term Memory (LSTM) based classification algorithm is used to categorize normal and attacking data with high accuracy and low complication. The most significant features from the normalized dataset are chosen for classification using the Avant-Garde African Vulture Optimization (A^2VO) method. For demonstrating the superiority of the suggested security model, the performance results are verified and compared using several benchmarking datasets.

1. Introduction

Internet of Things (IoT) is more susceptible to the different types of intrusions or attacks, due to its tremendous growth in present days [1,2]. The effectiveness of sensitive devices may affect end users, increases cyber threats and identity theft, which also has an adverse effect on income since problems produced by IoT network are unnoticed for extended periods of time [3-5]. Moreover, attacks on IoT interfaces must be closely monitored in real time for ensuring safety and security. Since, 5G is essential for IoT systems, even though it offers a speedier network with more capacity

* *Corresponding author.*
E-mail address: rram2005@hotmail.com

https://doi.org/10.37934/araset.32.1.117

to address connectivity needs. The frequency range that mobile communication technologies employ to transfer data is expanded by the 5G spectrum [6]. A full bandwidth of mobile networks increases as a result of the large usable range, allowing for the connection of additional devices. To address current challenges, 5G will undoubtedly necessitate command over the network's response time and network architecture. The integrated infrastructure of 5G often refreshes network endpoints and components to take into account new circumstances [7, 8]. Moreover, the service providers frequently use the cutting-edge technology to quickly take benefit of the value-added services. Yet, the up gradation is based on the cognitive radio technology, which has a number of significant features, including the capacity for devices to recognize their precise location, signals, monitoring devices, environment, and etc. [9]. Cognitive radio equipment functions as a transceiver in its operating environment that perceptually gathers the radio signals with proper response.

Moreover, the cognitive radio function can recognize the environmental changes and reacts to ongoing community. In order to meet the demands of customers and settle disputes in the 5G environment, a fundamental shift in the development of 5G wireless mobile technology is required [10]. One of the key problems with the 5G network is that every component used during the design and deployment phases must be authenticated with every other component in the network architecture before any operation can be started. In contrast, the components must also be developed using reliable network components during the physical layer phase of the network. There are several security flaws that can be readily impacted by intrusion-based attacks as internet traffic continues to increase and the industry updates 5G and IoT technology. In the existing studies, a variety of security mechanisms are implemented to protect the 5G-IoT systems against the intrusions. Intrusion detection necessitates the observation and analysis of active networks and networking traffic in order to detect potential computer assaults. For this goal, the Intrusion Detection System (IDS) [11, 12] is developed, which is a combination of techniques and tools that often have typical network security capabilities. The collection of information from the observed incidents is where an IDS originates. It performs thorough logging and contrasts actions with event-related information from many networks.

The detector uses a variety of approaches and related methodologies depending on the circumstance, which is the heart of an IDS. Additionally, mitigation would be possible, and the procedure for identifying intrusions and avoiding them begins here. Numerous IDS methodologies [13,14] are discussed in the literature as solutions to the IoT security issue. In a standard IDS frameworks, sensors gather data, which is then delivered to an analysis engine that scans the information and looks for intrusions. The reporting system alerts the network administrator if an intrusion is found [15]. The learning techniques are extensively used in the conventional works for improving the security of 5G-IoT systems [16-18]. However, the most challenging issues correlated to the existing studies are high processing time, low efficiency, lack of attack detection accuracy, and lack of reliability. Therefore, the proposed work intends to use a novel intelligence mechanism for protecting 5G-IoT systems. The dataset used for implementation in this study includes the different types of attacks, which is practical for both IoT-based systems and 5G networks. Hence, a novel method to identify these kinds of attacks is developed in this research work, which has the following contributions:

i. The min-max normalization algorithm is applied after dataset acquisition for normalize the attributes and fields.
ii. The 5G-IoT security framework's attack detection performance is enhanced by the implementation of the Avant-Garde African Vulture Optimization (A^2VO) algorithm, which selects the most pertinent features from the normalized dataset for classification.

iii. Moreover, a precise and efficient deep Recurrent Neural Network (RNN) – Long Short Term Memory (LSTM) based classification algorithm is applied to categorize normal and attacking data with high accuracy and low complexity.
iv. The performance results are validated and compared by using several benchmarking datasets for proving the betterment of the proposed security model.

The other portions are structured into the subsequent sections: Section 2 presents the literature review of the existing IDS methodologies related in 5G-IoT systems, where the benefits and limitations of each methodology have been discussed. Section 3 provides the clear explanation for the proposed IDS framework with its workflow and algorithms. Section 4 validates the performance and results of proposed framework by using a variety of benchmark datasets, and the outcomes are compared using several evaluation measures. In section 5, the conclusions, findings, and potential applications of the paper are summarized.

2. Related Works

This section reviews some of the current methods for intrusion detection and categorization in 5G-IoT systems, as well as some of their positive and negative aspects.

A system for intrusion detection based on several kernels was created by Hu *et al.,* [19] to secure 5G-IoT networks. Here, the authors offered a multiple kernel clustering algorithm-based analysis strategy to tackle the problem of selecting traffic features in anomaly detection. This approach increases clustering efficacy by combining multiple base kernels made from different feature properties, which lessens the susceptibility of the effectiveness of anomaly detection to the choice of individual features. In most traditional solutions, the techniques of average replacement or empty value replacement are used, and in certain cases, these lacking qualities are even ignored, which may lead to a reduced detection rate. The suggested multi-kernel method inserts the estimated values that are computed using sample data with the base kernel. Rezvy *et al.,* [20] used a deep auto-encoded dense neural network approach for 5G-IoT network security. In order to distinguish between regular and disruptive events from the AWID dataset, the authors of this work present an intrusion detection system with a hybrid approach that makes use of data mining techniques. Here, the five-fold cross validation is performed to validate and assess the performance of the suggested mechanism. This system provides advantages including faster training and higher attack prediction accuracy. Wazid *et al.,* [21] investigated about the major issues, challenges and future scope in 5G-IoT networks. This study indicates that the due to its vulnerability to multiple sorts of assaults, the 5G-enabled IoT ecosystem has a variety of security and privacy-related problems. Sicari *et al.,* [22] provided a detailed overview about various privacy and security challenges in 5G-IoT networks. Due to the significant influence 5G will undoubtedly have on Internet-based applications, academics are becoming more and more interested in the technology. Specifically, it might be essential for the development of environments associated to the Internet of Things. Recently, a lot of study surveys have been put forward in the field, largely concentrating on the characteristics and difficulties of the 5G protocol. The conversation that follows reveals how little focus is being made on the 5G wireless communication standard's security and privacy standards so far.

Bocu *et al.,* [23] designed a real time IDS for protecting 5G software defined networks from assaults. High throughput data lines are used in the 5G data networks. However, the wide range of supported mobile devices and the associated compatible applications are what primarily decide the added value that these unique data networks produce. Fu *et al.,* [24] introduced an automata

based IDS for IoT security. Many challenging situations can be described and addressed using automata theory. The uniform description challenge of heterogeneous IoT networks was solved in this research by the authors using a variant of the Input Output Labelled Transition System, and they also provide a matching intrusion detection mechanism for IoT networks. A collection of methods, such as collected information organization, packet information translation, anomalous information detection, and attack categorization are devised and suggested to accomplish this goal. Additionally, the authors created GUI tools to automatically examine, visually portray, and identify potential intrusions in generic activity processes. Samarakoon *et al.,* [10] investigated the different types of active, self-adaptive and real time security mechanisms for 5G wireless networks. Since AI-based security algorithms may identify hidden patterns in massive amounts of data, the great majority of data created within the network is very significant. The lack of comprehensive, reliable datasets that demonstrate complex network behaviors, particularly 5G network behaviors, is a persistent issue in AI-based security studies. The overall quality of the collected data and how well the data's behavior mimics a real network scenario have a substantial impact on the accuracy and efficacy of ML-based intrusion detection.

Rodriguez *et al.,* [25] utilized a transfer learning based IDS for improving the cyber-security of IoT networks. The deep learning algorithms have shown their ability to extract complicated patterns. In IoT systems, there isn't a significant collection of labelled data for both undiscovered assaults and recognized groupings of attacks. These networks frequently lack, or at least need a significant amount of effort to get, new training data. Furthermore, it takes a lot of time and computational resources to completely retrain DL models with the fresh data when a new incursion is discovered. IoT networks with sparse and uneven datasets and computing-constrained devices as a result make it challenging for DL-based IDSs to function. For the purpose of detecting known and unknown attacks in IoT networks, the authors introduced a novel approach based on transfer learning. Mobile Network is a significant concept of wireless networks which comprises of thousands of nodes that are mobile as well as autonomous and they do not requires any existing network infrastructure. Kim *et al.,* [26] suggested an effective feature selection mechanism for minimizing the complexity of IDS in 5G core networks. The authors emphasized the significance of eliminating auxiliary features to detect IoT DDoS in the 5G core network path with minimal latency. The results of the tests demonstrate that by choosing features that have a significant impact on learning and detection, the feature selection process can produce classification models that are faster and more accurate. Furthermore, the authors constructed a new simulation environment and collected data using a range of consumer devices. Extraction of features is sometimes time-consuming and difficult because previous machine learning algorithms mainly rely on feature engineering. Therefore, using typical machine learning techniques like DT [27], ensemble models [28], ANN [29], AE [30], RNN [31], KNN [3], and DNN [32] in real-time applications is impractical for detecting threats. Table 1 presents the review of various IDS methodologies used for protecting 5G-IoT networks.

Table 1
Review on existing IDS methodologies

Ref	Methods	Pros	Cons
[27]	Decision Tree (DT)	Simple to understand and easy interpretation	Un stability, overfitting and resampling
[28]	Ensemble models	Better prediction and performance	Complex to interpret, and increased training cost
[29]	Artificial Neural Network (ANN)	Better generalization capability, and prediction performance	Not suitable for large applications, and high computational burden
[30]	Auto Encoder (AE)	Better accuracy and less overfitting	Ineffective training and high time consumption
[31]	Recurrent Neural Network (RNN)	Well-suited for large scale application, and more accurate in prediction	Slow in process, difficult training, and computational complexity
[3]	K-Nearest Neighbor (KNN)	Well-suited for both classification & regression, and ability to handle multi-class problems	Computationally ineffective, and resource constraints
[32]	Deep Neural Network (DNN)	High accuracy and better detection performance	Computationally expensive, and requires large amount of data for training

3. Proposed Methodology

The proposed deep learning-based IDS architecture is fully explained in this part, along with a description of the overall work flow and individual stages. The purpose of this research is to present a unique intrusion detection framework with minimal computational expense and time for safeguarding 5G-IoT systems. For this purpose, a combination of Avant-Garde African Vultures Optimization (A^2VO) incorporated with a deep Recurrent Neural Network – Long Short Term Memory (RNN-LSTM) models are proposed in this work. For system validation and assessment, a common and popular cyber-attack datasets like NSL-KDD, AWID, and UNSW-NB15 have been used in this study. After dataset acquisition, the preprocessing is carried out to normalize the attributes with the use of min-max normalization scheme. During this process, the given dataset is properly organized for an effective and accurate classification. Since, the preprocessed data could be more useful for attaining an improved classification performance. After that, an A^2VO technique is deployed to choose the features from the normalized dataset with increased convergence speed. Consequently, the obtained features are trained by the RNN-LSTM for an accurate intrusion detection and classification. The workflow model of the proposed A^2VO-RNN-LSTM based IDS framework is shown in Figure 1, which comprises the following stages of operations:

i. Dataset acquisition
ii. Preprocessing based min-max normalization
iii. A^2VO based feature selection
iv. RNN-LSTM classification
v. Performance evaluation

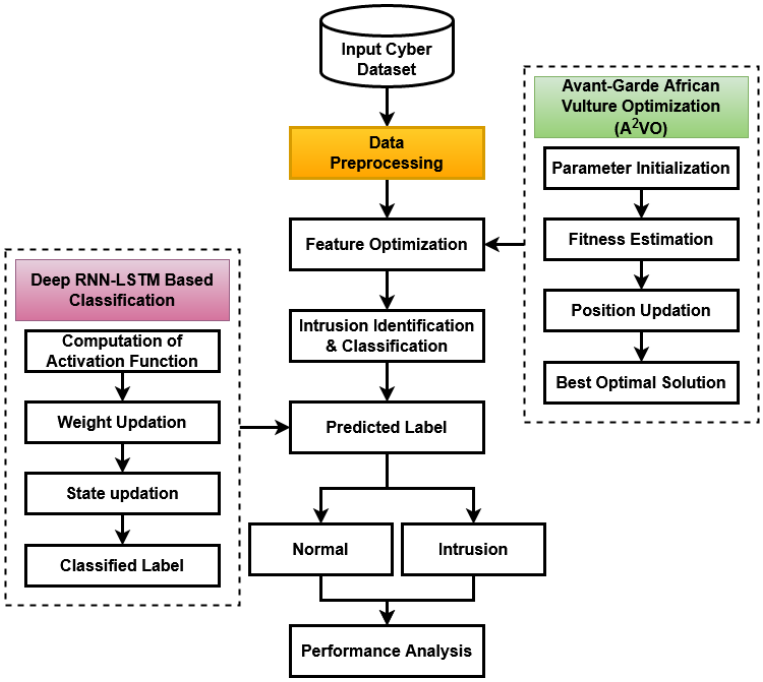

Fig. 1. Proposed work flow model

3.1 Avant-Garde African Vultures Optimization (AVO)

Here, the optimization algorithm is mainly used to obtain the most suitable solution for choosing the relevant features from the given datasets. In the existing studies, a lot of optimization approaches are developed for feature optimization or selection. Nevertheless, the major drawbacks of the existing mechanisms are low convergence rate, not highly efficient, and requires maximum time to reach the solution in the searching space. Therefore, the proposed work aims to use a highly efficient optimization algorithm, named as, Avant-Garde African Vultures Optimization (A^2VO) [33] for feature selection. Typically, the African vultures are unusual animals that feed on the herd and are shown to become quite defensive when failed to snag their prey. Additionally, they primarily hunt for dead animals or artefacts left by other animals. By including the rotational motion surrounding what is eaten in the cosmos, the observation of the food is furthered, and after that, they move in some unusual pattern in the direction of the prey. Based on their capacity for defending when chasing prey and their searching skills, they are nonetheless divided into bigger and smaller vultures. In order to get the best results for the fitness function, the vultures are essentially divided into two groups based on how well they can find food and how prominent they are. The amount of famine or level of contentment is taken into account while modelling the AV's behavior in this stage. The creatures can explore the best place to get food if they have enough food in their control, but on the other hand, being starved may make them more hostile. Moreover, the effectiveness of optimization is validated based on its exploitation and exploration capabilities.

The initial population is formed at the beginning of optimization, and each solution's fitness is assessed. The population as a whole is updated for each fitness generation, as represented in below:

$$P(i) = \begin{cases} Q_1 & if \quad t_i = \alpha \\ Q_2 & if \; t_i = \beta \end{cases} \tag{1}$$

where, $P(i)$ indicates the initial set of population, Q_1 and Q_2 are the probability parameters ranging from 0 to 1. When each of the best solutions is determined from each group, the vultures are chosen based on probability using equation (1). Then, the best optimal parameters are selected based on the Roulette wheel selection method as represented in below:

$$b_i = \frac{S_i}{\sum_{i=1}^{n} S_i} \tag{2}$$

In the Avant-Garde African Vultures Optimization technique, the Roulette wheel selection mechanism has been used to obtain the best optimal parameters, which is based on the rate of starvation and bias value.

Where, b_i indicates the best solution, and S_i represents the rate of starvation. Vultures often hunt for food, and when they feel fulfilled, they are more likely to move farther in their search than when they are starving, which makes them hostile. However, when they are starving, they lack the strength required to fly far or join the more powerful vultures in their hunt for prey. Moreover, the vulture's location updation $L(i+1)$ is performed by using the following model:

$$L(i+1) = P(i) - K(i) \times S \tag{3}$$

$$K(i) = |\delta \times P(i) - L(i)| \tag{4}$$

where, δ indicates the position of vulture, S denotes the rate of vulture, and $L(i)$ represents the position vector. According to its movement, the optimal position is determined based on the following model:

$$L(i+1) = P(i) - S + w_2 \times ((U_b - L_b) \times w_3 + L_b \tag{5}$$

where, w_2 and w_3 are the random numbers, U_b is the upper bound, and L_b is the lower bound. When many vultures congregate at a single food supply, serious fights over food acquisition may occur. Strong vultures during such times prefer not to eat together with other vultures, as shown below:

$$L(i+1) = K(i) \times (S + w_4) - d(g) \tag{6}$$

$$d(g) = P(i) - L(i) \tag{7}$$

By using the following model, the vector position of vultures is updated:

$$P(i+1) = \frac{\omega 1 + \omega 2}{2} \tag{8}$$

$$\omega 1 = Q_1(i) - \frac{Q_1(i) \times P(i)}{Q_1(i) \times P(i)^2} \times S \tag{9}$$

$$\omega 2 = Q_2(i) - \frac{Q_2(i) \times P(i)}{Q_2(i) \times P(i)^2} \times S \tag{10}$$

where, $Q_1(i)$ and $Q_2(i)$ are the best vultures from each group, and $P(i)$ indicates the current position of vulture and is updated as follows:

$$P(i+1) = \frac{\omega 1 + \omega 2}{2} \quad (11)$$

On the other side, some vultures also behave aggressively when pursuing prey. They approach the head vulture from a variety of angles, as demonstrated below:

$$P(i+1) = P(i) - |d(g)| \times S \times Levy(d) \quad (12)$$

According to $P(i+1)$, the best solution is identified from the optimization process, which is considered as the best optimal solution for the given problem. It is further for selecting the most appropriate characteristics from the normalized dataset is produced by applying this technique.

Algorithm I – AVO based Feature Selection

Input: ***Preprocessed dataset;***
Output: ***Selected features;***
Begin
Step 1: Initialize population and optimization parameters;
Step 2: Compute fitness value using Eq. (1);
Step 3: Select the best optimal parameters using Eq. (2);
Step 4: Perform vulture location updation $L(i+1)$ using Eq. (3) and Eq. (4);
Step 5: Update the vector position $P(i+1)$ according to the strong vultures using Eq. (8) to Eq.(10);
Step 6: Find the current position and get the best optimal solution $P(i+1)$;

3.2 RNN-LSTM

After choosing the essential features from the dataset, the classifier training is carried out to predict the intrusions in 5G-IoT systems. For this purpose, a simple and effective deep learning model, called, as Recurrent Neural Network – Long Short Term Memory (RNN-LSTM) [34] for precisely categorizing the class of intrusions. The current classification models face particular difficulties in terms of high error rates, time-consuming data training and testing, and low model prediction rates. The RNN-LSTM is a widely employed advanced deep learning classifier for multi-class intrusion detection and classification problems in various application systems. The simplicity of implementation, good detection accuracy, decreased complexity, and effective data training are the main benefits of employing this technique. The proposed study aims to construct a RNN-LSTM model for detecting the assaults from the cyber-attack dataset. Figure 2 depicts the proposed RNN-LSTM technique's integrated architecture model, which has layers of input, LSTM, GRU, time distribution, and output. In this scenario, the input layer is utilized to gather the features for the classifier's training, and the output layer generates the final label for the classification as either normal or attack class. In this model, the network's current condition is depicted as follows:

$$\sigma_k = f(\sigma_{k-1}, I_k) \quad (13)$$

where, σ_k represents the current hidden state of network, and I_k denotes the input. According to the weight value, the activation function is estimated by using the following model:

$$\sigma_k = \tanh(W_\sigma \times \sigma_{k-1} + W_I \times I_k) \quad (14)$$

Then, the output value is estimated based on the updated weight value as indicated in the following equation:

$$Q_k = W_Q \times \sigma_{k-1} \tag{15}$$

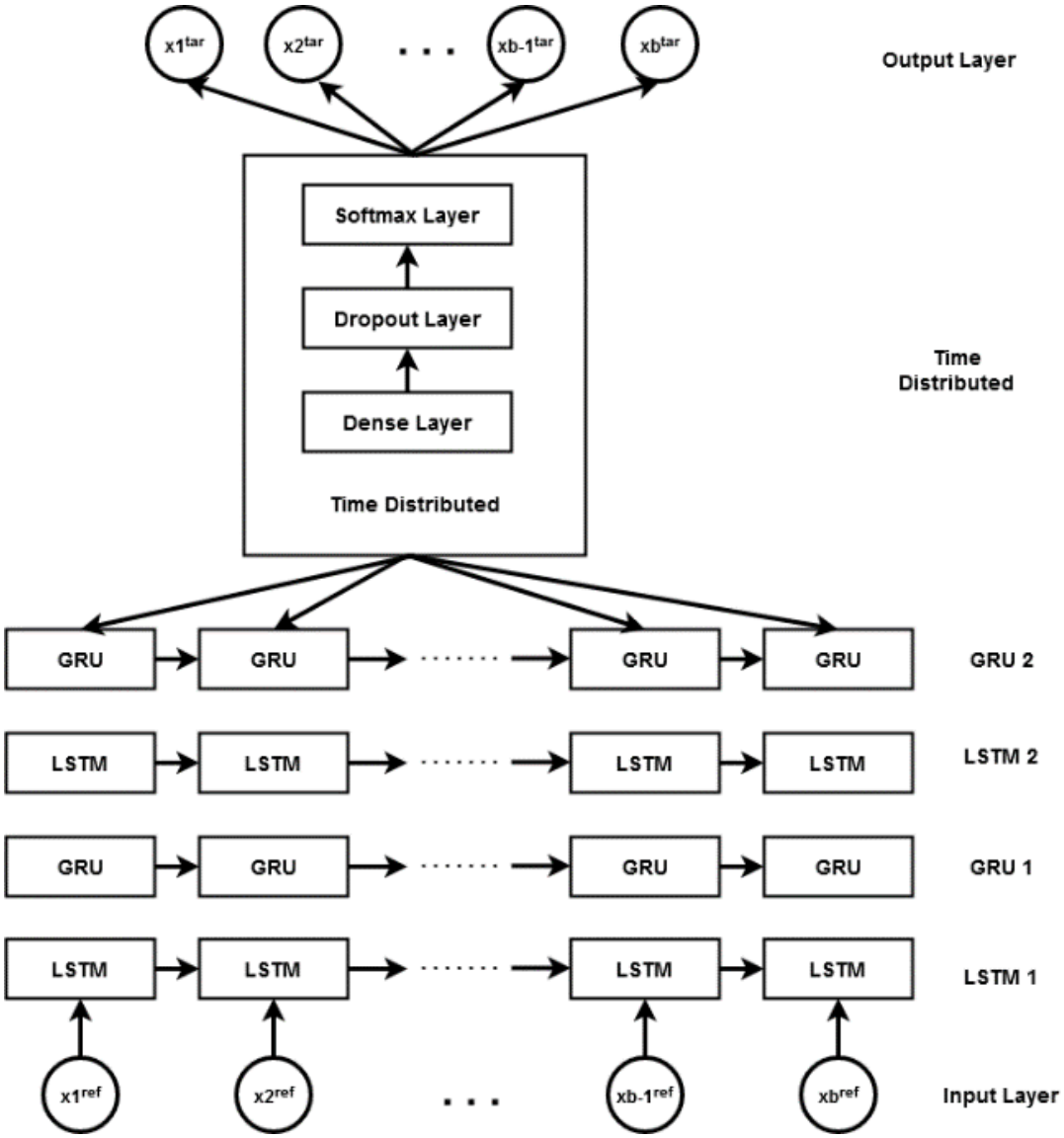

Fig. 2. Structure of RNN-LSTM

Each LSTM cell has three separate gates, including an input gate, a forget gate, and an output gate. The input gate is in charge of attaching new data to a cell. Here, the current inputs are obtained by the sigmoid layer, and the result produced by the forget gate is shown in the following form:

$$E_k = I(W_E \times [\sigma_{k-1}, I_k] + B_E) \tag{16}$$

where, E_k is the result of forget gate, and B_E denotes the bias value. Finally, the output gate produces the final prediction output based on the following model:

$$O_k = I(W_0 \times [\sigma_{k-1}, I_k] + B_0) \tag{17}$$

The update gate and reset gate constitute two different gates in GRU that are utilized to handle the data. The reset gate in this case manages the GRU's secret state, as seen below:

$$k = I(W \times \sigma_{k-1} \times I_k) \tag{18}$$

Therefore, the updated gate τ_k as indicated below maintains the long term memory of GRU:

$$\tau_k = I(W_\tau \times \sigma_{k-1} + I_k) \tag{19}$$

By using this algorithm, the final prediction results are obtained as the output, which helps to accurately categorize the normal and intrusions from the given cyber datasets.

4. Results and Discussion

By using a range of well-known datasets, this section compares and validates the outcomes and attack detection performance of the existing and proposed IDS techniques. Additionally, a number of assessment indicators are utilized to evaluate the results including the following:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{20}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{21}$$

$$\text{Recall or TPR} = \frac{TP}{TP+FN} \tag{22}$$

$$\text{F1} - \text{measure} = 2 * \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{23}$$

$$\text{FPR} = \frac{FP}{FP+TN} \tag{24}$$

where, TP – true positives, TN – true negatives, FP – false positives, and FN – false negatives. Moreover, the popular benchmarking datasets such as NSL-KDD, UNSW-NB15 and AWID are considered in this study for performance evaluation and comparison. The attacks exist in these datasets are common for both 5G and IoT networks. Here, the A^{2}VO-RNN-LSTM model is validated and tested by using these datasets. Table 2 and Figure 3 compares the standard and proposed IDS approaches used for securing 5G-IoT networks, where the performance is compared using the standard NSL-KDD dataset. The overall attack detection performance and security level of the IDS framework can be validated according to its improved accuracy and reduced false predictions. Also, the obtained results indicate that the proposed A^{2}VO-RNN-LSTM outperforms other algorithms with improved performance results.

Table 2
Comparative analysis using NSL-KDD

Methods	TPR (%)	FPR (%)	Precision (%)	Accuracy (%)	F1-score (%)
MKKM-IC	89	5	81.65	93.80	85.17
Density peaks	75	8.75	68.18	88	71.43
K-Means	68	11.75	59.13	84.20	63.26
GMM	80	6.25	76.19	91	78.05
Proposed	99	2.3	98.9	99	98.9

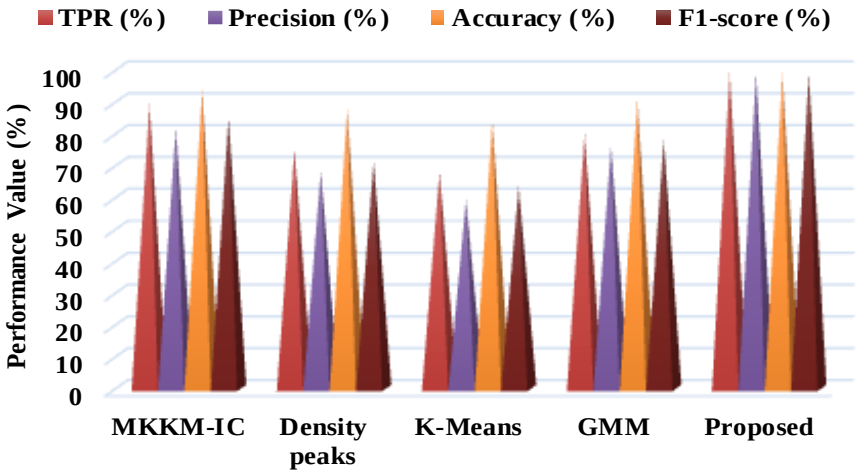

Fig. 3. Performance analysis using NSL-KDD dataset

Table 3 and 4 presents the comparative analysis of existing and proposed mechanisms by using UNSW-NB 15 and AWID datasets respectively, and they are graphically shown in Figure 4 and Figure 5. Then, Figure 6 shows the FPR of existing and proposed attack detection methodologies for different datasets. The efficiency of the AI-powered algorithms are validated and compared in this study based on the parameters of TPR, FPR, precision, accuracy and f1-score. These measures can determine the performance and attack detection efficiency of entire security framework, hence which must be highly improved for assuring better system performance. According to the results, it is noted that the proposed A^{2}VO-RNN-LSTM technique increases an average accuracy to 99.1% for all datasets, which is highly superior to the existing techniques. Due to the dimensionality reduction of features by A^{2}VO, the classifier's training and testing complexity has been effectively minimized, which helps to obtain an increased performance rate.

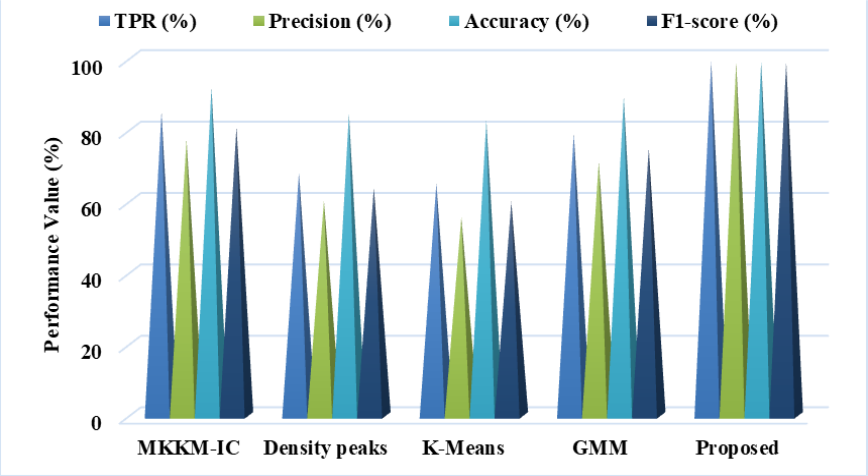

Fig. 4. Performance analysis using UNSW-NB 15 dataset

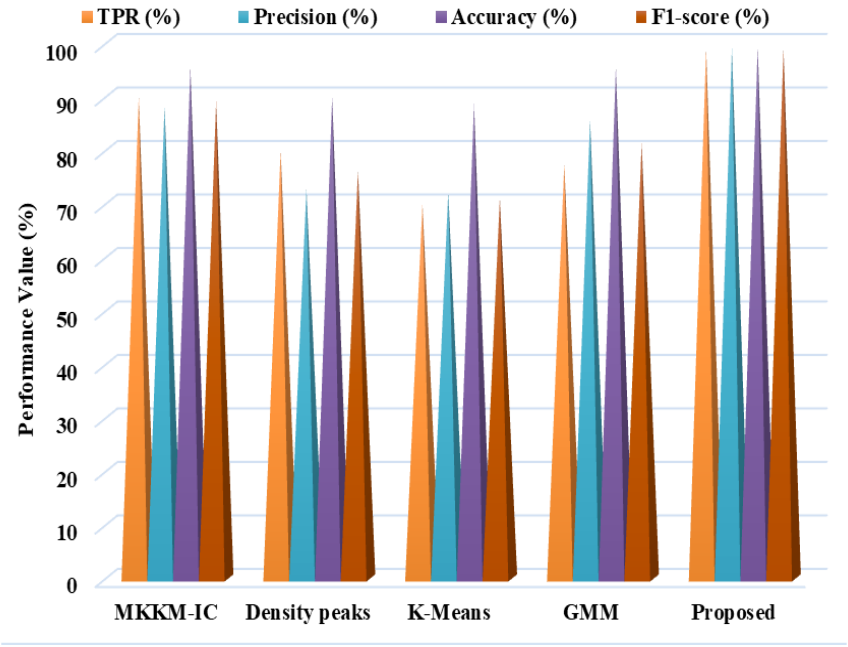

Fig. 5. Performance analysis using AWID dataset

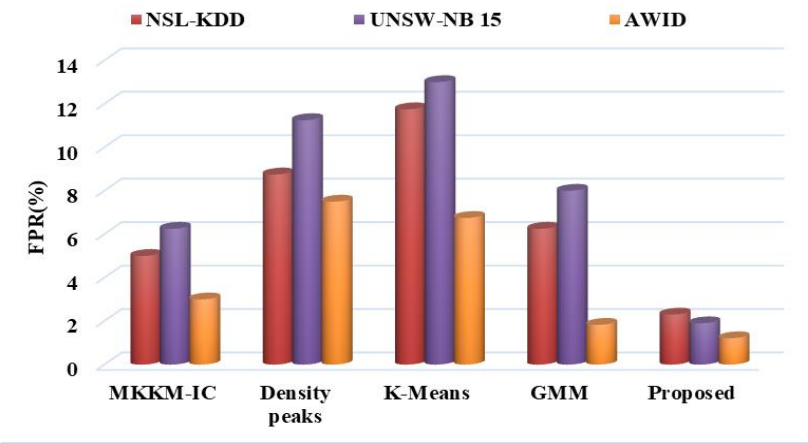

Fig. 6. Comparative analysis based on FPR

For determining the improved performance and superiority of the proposed model, some of the existing IDS methodologies such as MKKM-IC, Density peaks, K-Means, GMM are considered in this study. The Multiple Kernel K-Means Clustering (MKKM-IC) is a single kernel model used for categorizing the normal and attacking instances from the given data. Similarly, the density peaks, K-Means, and Gaussian Mixture Modeling (GMM) are also the widely used machine learning techniques, which predicts the attacking instances according to the characteristics of the dataset.

Table 3
Comparative analysis using UNSW-NB 15

Methods	TPR (%)	FPR (%)	Precision (%)	Accuracy (%)	F1-score (%)
MKKM-IC	85	6.25	77.27	92	80.95
Density peaks	68	11.25	60.18	84.60	63.85
K-Means	65	13	55.56	82.60	59.91
GMM	79	8	71.17	89.40	74.88
Proposed	99.1	1.9	99	99.2	99

Table 4
Comparative analysis using AWID dataset

Methods	TPR (%)	FPR (%)	Precision (%)	Accuracy (%)	F1-score (%)
MKKM-IC	90	3	88.24	95.60	89.11
Density peaks	80	7.5	72.73	90	76.19
K-Means	70	6.75	72.16	88.6	71.07
GMM	77.42	1.83	85.71	95.60	81.36
Proposed	99	1.21	99.1	99.3	99

Using the AWID dataset, as shown in Figure 7, the total detection accuracy of the current [20] and suggested classification approaches is tested and compared. Moreover, Figure 8 to Figure 10 validates the precision, recall and f1-score of existing deep learning [35] and proposed RNN-LSTM techniques with respect to the different types of attacks in the NSL-KDD dataset. The findings indicate that the proposed A^{2}VO-RNN-LSTM technique highly improves the precision, recall, and f1-score measures by precisely locating the intrusions from the dataset. With proper classifier's training, the classifier results the better predictions with low error outcomes.

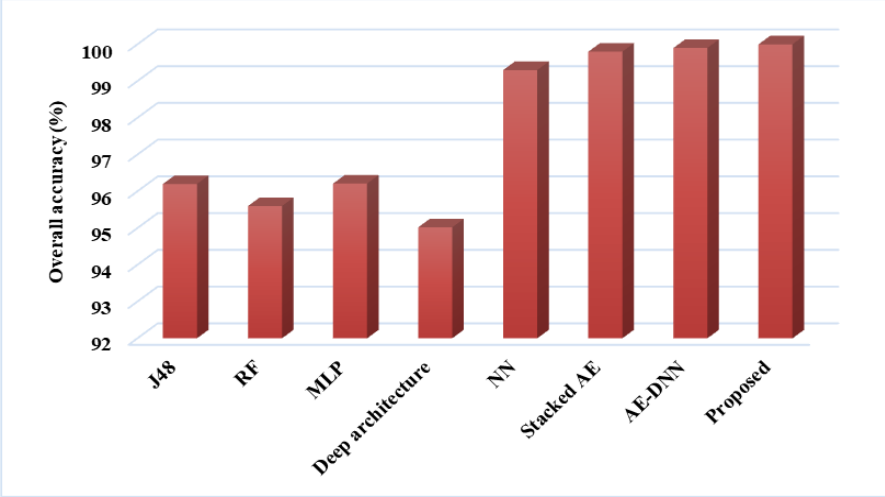

Fig. 7. Overall attack detection accuracy using AWID dataset

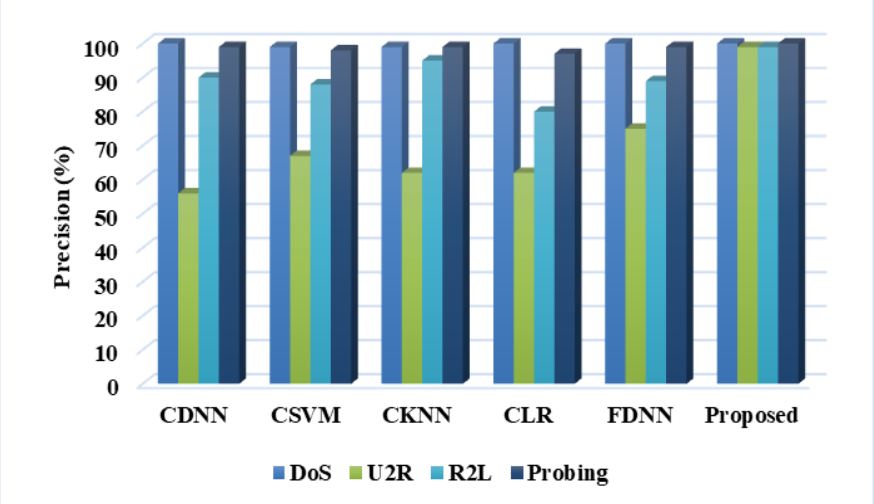

Fig. 8. Comparative analysis based on precision with respect to different types of attacks

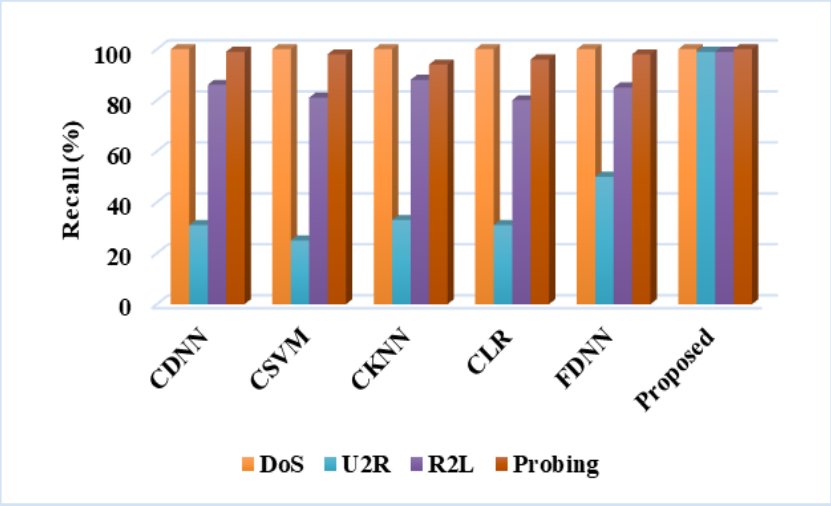

Fig. 9. Comparative analysis based on precision with respect to different types of attacks

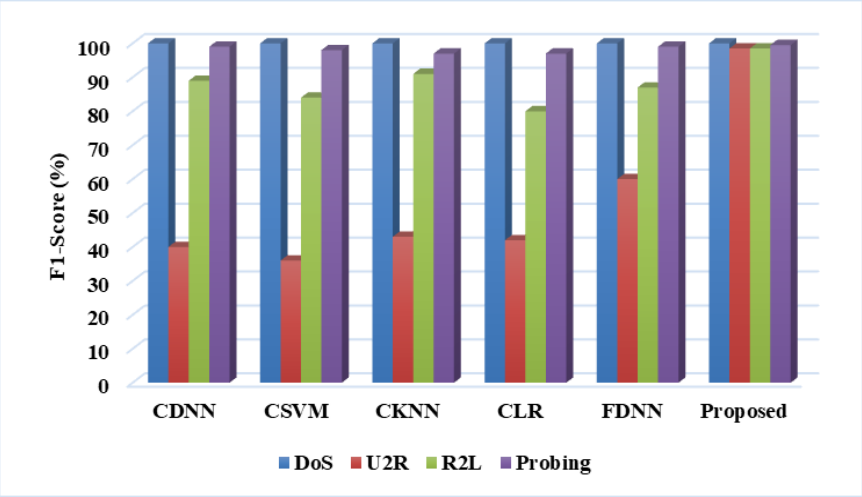

Fig. 10. Comparative analysis based on precision with respect to different types of attacks

When compared to the other machine learning and deep learning techniques such as SVM, KNN, LR, FDNN, GMM, K-Means, and etc, the proposed A^{2}VO-RNN-LSTM could effectively predict the vulnerabilities in the 5G-IoT systems by analyzing the attributes or characteristics of the given cyber threat data. Moreover, the feature analysis and optimization processes are carried out in this research for highly enhancing the detection rate of classifier. Also, the proposed model has the unique properties of low system complexity, better accuracy, and optimized performance outcomes.

5. Conclusion

This paper proposed a novel A^{2}VO-RNN-LSTM technique for increasing the security of 5G-IoT networks. The contribution of this work is to develop a lightweight and precise security framework for protecting 5G-IoT system from cyber-attacks. This security system comprises the modules of min-max normalization based preprocessing, A^{2}VO based feature optimization, and RNN-LSTM based attack prediction. In this study, the popular and recent cyber-attack datasets are used for analysis and interpretation, which comprises the intrusions that are common for both 5G and IoT

networks. After acquiring the dataset, preprocessing is done using the min-max normalization strategy to normalize the characteristics. The given dataset is correctly organized during this phase to allow for an efficient and precise classification. As a result, preprocessed data might be more beneficial for achieving better classification performance. The features are then selected from the normalized dataset with accelerated convergence using an A2VO approach. By using the acquired features, the RNN-LSTM is trained for precise intrusion detection and classification. For performance evaluation, the results of the proposed A^2VO-RNN-LSTM model is validated and compared by using a variety of evaluation metrics. Finally, the findings indicate that the proposed A^2VO-RNN-LSTM increases the average accuracy to 99% for all datasets by precisely predicting the type of intrusions according to their characteristics.

In future, the present work can be improved by deploying a new classification model for 5G wireless security. Moreover, various security vulnerabilities in 5G and 6G wireless communication systems are addressed in the upcoming work with the use of AI algorithms. Also, we planned to develop a new authentication protocol for developing 5G/6G enabled cyber physical systems.

Acknowledgement
This research was not funded by any grant

References

[1] Sousa, Breno, Naercio Magaia, and Sara Silva. "An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles." *Electronics* 12, no. 8 (2023): 1757. https://doi.org/10.3390/electronics12081757

[2] Sood, Keshav, Mohammad Reza Nosouhi, Dinh Duc Nha Nguyen, Frank Jiang, Morshed Chowdhury, and Robin Doss. "Intrusion detection scheme with dimensionality reduction in next generation networks." *IEEE Transactions on Information Forensics and Security* 18 (2023): 965-979. https://doi.org/10.1109/TIFS.2022.3233777

[3] Nguyen, Dinh Duc Nha, Keshav Sood, Yong Xiang, Longxiang Gao, Lianhua Chi, and Shui Yu. "Towards IoT Node Authentication Mechanism in Next Generation Networks." *IEEE Internet of Things Journal* (2023). https://doi.org/10.1109/JIOT.2023.3262822

[4] Shobowale, K. O., Z. Mukhtar, B. Yahaya, Y. Ibrahim, and M. O. Momoh. "Latest advances on security architecture for 5G technology and services." *International Journal of Software Engineering and Computer Systems* 9, no. 1 (2023): 27-38. https://doi.org/10.15282/ijsecs.9.1.2023.3.0107

[5] Redelijkheid, M. N. F. "Monitoring network traffic and responding to malicious traffic for IoT devices in 5G network slices." Master's thesis, University of Twente, 2023.

[6] Cook, Jonathan, Sabih Ur Rehman, and M. Arif Khan. "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions." *IEEE Access* (2023). https://doi.org/10.1109/ACCESS.2023.3268064

[7] Ding, Shanshuo, Liang Kou, and Ting Wu. "A GAN-based intrusion detection model for 5G enabled future metaverse." *Mobile Networks and Applications* 27, no. 6 (2022): 2596-2610. https://doi.org/10.1007/s11036-022-02075-6

[8] Rajasoundaran, S., A. V. Prabu, Sidheswar Routray, Prince Priya Malla, G. Sateesh Kumar, Amrit Mukherjee, and Yinan Qi. "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks." *Computer Communications* 187 (2022): 71-82. https://doi.org/10.1016/j.comcom.2022.02.004

[9] Kumudavalli, Thenmozhi Rayan, and S. C. Sandeep. "Machine learning IDS models for 5G and IoT." *Secure Communication for 5G and IoT Networks* (2022): 73-84. https://doi.org/10.1007/978-3-030-79766-9_5

[10] Samarakoon, Sehan, Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, Sang-Yoon Chang, Jinoh Kim, Jonghyun Kim, and Mika Ylianttila. "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network." *arXiv preprint arXiv:2212.01298* (2022).

[11] Bhati, Bhoopesh Singh, Chandra Shekhar Rai, Balamurugan Balamurugan, and Fadi Al-Turjman. "An intrusion detection scheme based on the ensemble of discriminant classifiers." *Computers & Electrical Engineering* 86 (2020): 106742. https://doi.org/10.1016/j.compeleceng.2020.106742

[12] Dey, Saurabh, Qiang Ye, and Srinivas Sampalli. "A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks." *Information Fusion* 49 (2019): 205-215. https://doi.org/10.1016/j.inffus.2019.01.002

[13] Sathesh, Dr A. "Enhanced soft computing approaches for intrusion detection schemes in social media networks." *Journal of Soft Computing Paradigm* 1, no. 2 (2019): 69-79. https://doi.org/10.36548/jscp.2019.2.002
[14] Lansky, Jan, Saqib Ali, Mokhtar Mohammadi, Mohammed Kamal Majeed, Sarkhel H. Taher Karim, Shima Rashidi, Mehdi Hosseinzadeh, and Amir Masoud Rahmani. "Deep learning-based intrusion detection systems: a systematic review." *IEEE Access* 9 (2021): 101574-101599. https://doi.org/10.1109/ACCESS.2021.3097247
[15] Zhang, Jielun, Fuhao Li, and Feng Ye. "An ensemble-based network intrusion detection scheme with bayesian deep learning." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020. https://doi.org/10.1109/ICC40277.2020.9149402
[16] Lu, Guanyu, and Xiuxia Tian. "An efficient communication intrusion detection scheme in AMI combining feature dimensionality reduction and improved LSTM." *Security and Communication Networks* 2021 (2021): 1-21. https://doi.org/10.1155/2021/6631075
[17] Bandecchi, Susan, and Nicoleta Dascalu. "Intrusion Detection Scheme in Secure Zone Based System." *Journal of Computing and Natural Science* (2021): 19-25. https://doi.org/10.53759/181X/JCNS202101005
[18] Manan, Jamila, Atiq Ahmed, Ihsan Ullah, Leïla Merghem-Boulahia, and Dominique Gaïti. "Distributed intrusion detection scheme for next generation networks." *Journal of Network and Computer Applications* 147 (2019): 102422. https://doi.org/10.1016/j.jnca.2019.102422
[19] Hu, Ning, Zhihong Tian, Hui Lu, Xiaojiang Du, and Mohsen Guizani. "A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks." *International Journal of Machine Learning and Cybernetics* (2021): 1-16. https://doi.org/10.1007/s13042-020-01253-w
[20] Rezvy, Shahadate, Yuan Luo, Miltos Petridis, Aboubaker Lasebae, and Tahmina Zebin. "An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks." In *2019 53rd Annual Conference on information sciences and systems (CISS)*, pp. 1-6. IEEE, 2019. https://doi.org/10.1109/CISS.2019.8693059
[21] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel JPC Rodrigues. "Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap." *IEEE Access* 9 (2020): 4466-4489. https://doi.org/10.1109/ACCESS.2020.3047895
[22] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "5G In the internet of things era: An overview on security and privacy challenges." *Computer Networks* 179 (2020): 107345. https://doi.org/10.1016/j.comnet.2020.107345
[23] Bocu, Razvan, Maksim Iavich, and Sabin Tabirca. "A real-time intrusion detection system for software defined 5G networks." In *International Conference on Advanced Information Networking and Applications*, pp. 436-446. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-75078-7_44
[24] Fu, Yulong, Zheng Yan, Jin Cao, Ousmane Koné, and Xuefei Cao. "An automata based intrusion detection method for internet of things." *Mobile Information Systems* 2017 (2017). https://doi.org/10.1155/2017/1750637
[25] Rodríguez, Eva, Pol Valls, Beatriz Otero, Juan José Costa, Javier Verdú, Manuel Alejandro Pajuelo, and Ramon Canal. "Transfer-learning-based intrusion detection framework in IoT networks." *Sensors* 22, no. 15 (2022): 5621. https://doi.org/10.3390/s22155621
[26] Kim, Ye-Eun, Yea-Sul Kim, and Hwankuk Kim. "Effective feature selection methods to detect IoT DDoS attack in 5G core network." *Sensors* 22, no. 10 (2022): 3819. https://doi.org/10.3390/s22103819
[27] Kalaivaani, P. T., Raja Krishnamoorthy, A. Srinivasula Reddy, and Anand Deva Durai Chelladurai. "Adaptive Multimode Decision Tree Classification Model Using Effective System Analysis in IDS for 5G and IoT Security Issues." *Secure Communication for 5G and IoT Networks* (2022): 141-158. https://doi.org/10.1007/978-3-030-79766-9_9
[28] Cheng, Xiaochun, Chengqi Zhang, Yi Qian, Moayad Aloqaily, and Yang Xiao. "deep learning for 5G IoT systems." *International journal of machine learning and cybernetics* 12 (2021): 3049-3051. https://doi.org/10.1007/s13042-021-01382-w
[29] Nyangaresi, Vincent Omollo, Musheer Ahmad, Ahmed Alkhayyat, and Wei Feng. "Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things." *Expert Systems* 39, no. 10 (2022): e13126. https://doi.org/10.1111/exsy.13126
[30] Ieracitano, Cosimo, Ahsan Adeel, Francesco Carlo Morabito, and Amir Hussain. "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach." *Neurocomputing* 387 (2020): 51-62. https://doi.org/10.1016/j.neucom.2019.11.016
[31] Guan, Jianfeng, Junxian Cai, Haozhe Bai, and Ilsun You. "Deep transfer learning-based network traffic classification for scarce dataset in 5G IoT systems." *International Journal of Machine Learning and Cybernetics* 12, no. 11 (2021): 3351-3365. https://doi.org/10.1007/s13042-021-01415-4
[32] Yadav, Kusum, Anurag Jain, Yasser Alharbi, Ali Alferaidi, Lulwah M. Alkwai, Nada Mohamed Osman Sid Ahmed, and Sawsan Ali Saad Hamad. "A secure data transmission and efficient data balancing approach for 5G-based IoT

data using UUDIS-ECC and LSRHS-CNN algorithms." *IET communications* 16, no. 5 (2022): 571-583. https://doi.org/10.1049/cmu2.12336

[33] Vashishtha, Govind, Sumika Chauhan, Anil Kumar, and Rajesh Kumar. "An ameliorated African vulture optimization algorithm to diagnose the rolling bearing defects." *Measurement Science and Technology* 33, no. 7 (2022): 075013. https://doi.org/10.1088/1361-6501/ac656a

[34] Gill, Harmandeep Singh, Osamah Ibrahim Khalaf, Youseef Alotaibi, Saleh Alghamdi, and Fawaz Alassery. "Multi-Model CNN-RNN-LSTM Based Fruit Recognition and Classification." *Intelligent Automation & Soft Computing* 33, no. 1 (2022). https://doi.org/10.32604/iasc.2022.022589

[35] Mirzaee, Parya Haji, Mohammad Shojafar, Zahra Pooranian, Pedram Asefy, Haitham Cruickshank, and Rahim Tafazolli. "Fids: A federated intrusion detection system for 5g smart metering network." In *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*, pp. 215-222. IEEE, 2021. https://doi.org/10.1109/MSN53354.2021.00044