Computers and Electrical Engineering 102 (2022) 108190

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm

Judy Simon, N. Kapileswar, Phani Kumar Polasi, M. Aarthi Elaveini *

Department of ECE, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Sensor networks
Intrusion detection
Deep learning
Convolutional Neural Network
Decision Tree

ABSTRACT

The intense growth of wireless communication and the digital revolution have increased the utilization of Internet of Things (IoT) applications. The number of internet users increase everyday which in turn increases the network traffic and data volume. The energy-limited sensor node resources in the IoT environment are vulnerable to attacks due to the networking procedures, open broadcast communication, etc. Intruders easily gain access to the network and perform different types of attacks which degrades the overall performance and quality of services. Intrusion detection systems are developed to detect different kinds of attacks that cannot be detected by the firewalls. Based on the features, the intrusion detection system classifies the normal and abnormal characteristics of the system. Various intrusion detection systems based on machine learning models have evolved so far. However, the feature selection process is much important to enhance the classification performance. Thus, in this research work, a deep learning-based feature selection procedure is presented to select the optimal features. The decision tree algorithm is utilized as a classifier to classify the deep features and detect attacks in the IoT network. Benchmark NSL-KDD dataset has been used for experimentation and the parameters like precision, recall, f1-score, and accuracy are evaluated for the proposed model and the conventional models to validate the superior performance. With maximum accuracy of 99.49%, the proposed hybrid model performs better than the conventional intrusion detection systems.

1. Introduction

The Internet of Things (IoT) connects millions of devices and integrates different services under a single network. A group of small, powered devices create a network that communicates through wired or wireless infrastructure. This group of devices is called as sensor networks and when connected to the internet or computer network to transfer data for further analysis, it is termed as an Internet of Things (IoT) environment. Smart devices connected in the IoT environment collect information from different sources and communicate with other devices at high speed. The intelligent healthcare system, smart industries, smart cities, smart ecosystem, and vehicular networks, etc., are some of the functional areas of IoT networks. The devices in the IoT network utilize different communication procedures and provide services. Artificial intelligence algorithms are widely used to process the collected information.

Besides the benefits of IoT, various security threats and attacks are the major issues in the IoT environment [1]. The data from the IoT applications is quite an area of huge interest for intruders. Various attacks are performed to acquire the data. As a result, the entire system is at stake in terms of the data security which consequently reduces the system performance [2]. Denial of service (DoS) and

* Corresponding author.
E-mail address: aarthim@srmist.edu.in (M.A. Elaveini).

https://doi.org/10.1016/j.compeleceng.2022.108190
Received 28 December 2021; Received in revised form 9 June 2022; Accepted 17 June 2022
Available online 1 July 2022

Distributed Denial of Service (DDoS) attacks are some of the familiar attacks in IoT networks [3,4]. To ensure device and data security in IoT networks, different security procedures should be followed for each device which is a tedious process. The security features of IoT devices are insufficient to handle threats and attacks. So, intrusion detection systems are introduced to detect different attacks and enhance network security, privacy, and confidentiality [5]. In simple terms, intrusion detection system is a network-related technology developed to detect vulnerabilities in the target computer or application.

Intrusion detection systems based on machine learning approaches [6] have evolved since the last decade. The detection process starts from selecting the features from the network data and classifying them based on the user-defined conditions or learning procedures [7]. However, the improper feature selection and processing of redundant or irrelevant data increases the computational complexity of the system which also degrades the overall quality of service. To overcome this, various optimization models are introduced. Nature-inspired heuristic and metaheuristic optimization models are utilized to select optimal features for the intrusion detection system. However, the optimization model performance degrades due to the local optima solution. The global solutions take more time to compute which increases the overall computation time and detection accuracy.

Recently, deep learning has gained increasing attention in various domains like image processing, signal processing, and data mining applications [8,9]. Deep learning belongs to the class of machine learning algorithms. Its architecture invokes multiple neural networks to simulate the behavior of the human brain. The benefits of the deep learning model are its feature selection procedure and classification performance. The optimal features obtained from the deep learning network enhance the classification accuracy as well as the overall quality of services. Considering these ideologies, this research work is aimed to develop an intrusion detection system based on a deep learning technique. As a summary, the contribution of this proposal is given as follows.

- A hybrid intrusion detection system is presented using deep learning and a machine learning algorithm. A convolutional neural network and decision tree algorithm are combined to obtain the proposed intrusion detection system.
- The fully connected neural network in conventional deep learning model is replaced with a decision tree algorithm to enhance the detection accuracy.
- Simulation analysis has been presented using benchmark NSL-KDD dataset and the network parameters like precision, recall, f1-score and accuracy are evaluated.
- The performance metrics of the proposed model and the existing conventional models are compared to claim the benefits of the proposed approach.

The remaining chapters in this research work are summarized as follows. The literature analysis is given in Section 2, which presents the features of the existing intrusion detection system. The proposed hybrid intrusion detection model is explained in Section 3. The results and discussions are presented in Section 4 and the conclusion is detailed in Section 5.

2. Related works

A brief literature analysis of various intrusion detection systems that have evolved in recent years is presented in this section. The Internet of Things interconnects multiple objects for data exchange, and most of the time, the communication channel is a wireless medium, which means it gets affected due to security factors. Moreover, due to the limited energy devices used in the IoT environment, the possibility of introducing security measures is lower, which makes it an easy target for intruders. Various intrusion detection systems have been introduced to detect intrusions in IoT networks. Machine learning algorithms are widely used for intrusion detection systems. However, the absence of labeled data makes the detection process challenging for machine learning algorithms. To overcome this limitation, the features should be selected and labeled properly. The generative adversarial network model presented in [10] detected cyber-attacks in fog architecture. The approach estimated the reconstruction loss by considering the data samples mapped to the latent space to attain high detection rates compared to the existing detection models.

A wireless network intrusion detection system presented in [11] efficiently detected Wi-Fi network attacks using machine learning models. Since most of the IoT applications accessed by the users utilize Wi-Fi networks for connectivity, the attack possibility on Wi-Fi networks has been discussed in detail in the model. The Wi-Fi traffic flow was classified using machine learning models to detect normal and malicious events in the network with a low false-positive rate, which is the observed merit of the presented model. The machine learning-based intrusion detection model presented in [12] detected intrusions in physical IoT systems. With the objective of detecting DoS attacks, the machine learning approach processed the unique metadata and identified the intrusions efficiently. A double hidden Markov model presented in [13] reduced the computational complexity of the intrusion detection system. The discrete single network abnormal behaviors were identified by the lower-level Hidden Markov Model (HMM), whereas the upper level was used to detect multiple abnormal events. The model showed a better detection rate for terminal abnormal behavior detection.

Intrusion detection in vehicular ad-hoc networks presented in [14] used machine learning techniques. DoS and DDoS attacks were detected by testing machine learning techniques for binary and multiscale classification. The feature selection for the machine learning models was performed using the chi-square technique and balanced using the Synthetic Minority Oversampling Technique (SMOTE) algorithm. Experimental results revealed the best performance of the XGboost algorithm with maximum detection accuracy compared to other machine learning techniques. A similar comparative analysis of deep recurrent neural networks with machine learning algorithms for intrusion detection is presented in [15]. The presented approach was experimented with the internet of medical things data, which handled sensitive information. Machine learning models such as random forest, KNN, decision tree, and ridge classifier were used in the comparative analysis. Maximum detection accuracy was the merit of the presented model; however, the computation complexity was a bit high compared to the state-of-the-art techniques.

Table 1
Summary of literature review.

Reference	Methodology	Dataset	Application	Remarks
[10]	Generative Adversarial Networks	Secure Water Treatment (SWaT) and the Water Distribution (WADI) datasets for CPSs, and the NSL-KDD dataset for network cyber-attacks	Cyber–Physical Systems	Maximum detection rate of 95%
[11]	Machine learning	University of Arizona and AWID family of datasets	Wi-Fi networks	Low false positives (0.0174)
[12]	K-Nearest Neighbors, Quadratic discriminant analysis (QDA), Iterative Dichotomiser 3(ID3), Random Forest (RF), Adaptive Boosting, Multilayer Perceptron, Naive Bayes,	Bot-IoT metadata	Cyber–Physical Systems	Random forest method outperformed other ML methods.
[14]	Logistic Regression (LR), naive Bayes (NB), decision tree (DT), support vector machine (SVM), k-nearest neighbor (kNN), random forest (RF), and XGBoost	NSL-KDD or KDD-CUP99 datasets	VANETs	XGBoost method outperformed other ML methods.
[15]	Particle swarm optimization with SVM, RF, NB, and RNN,	NSL-KDD	Cyber threats	Random forest method outperformed other ML methods.
[18]	Software Defined Networking	CAIDA, KDD Cup 1999, UNSW-NB15	IoT networks	95.5% average of detection rate
[22]	Gradient-based linear Support Vector Machine (SVM)	Aegean Wi-Fi Intrusion Dataset	Cyber-physical-social systems	98.22% accuracy

The intrusion detection model reported in [16] combines a Bayesian model with trust management for intrusion detection in wireless sensor networks. The hierarchical structure categorized the abnormal events and overcame the limitations of the packet-based trust management process. The approach was more efficient, even for heavy traffic environments, and reduced the computation complexity while detecting insider attacks. A mobile agent-based intrusion detection system reported in [17], incorporated machine learning and regression algorithms to detect intrusions. The network-level intrusion detection model identified the malicious event in the network as well as in sensor data. The minimum computation overhead and better detection accuracy are the merits of the approach.

An intrusion detection model for Software-Defined Networking (SDN) based cloud IoT networks is presented in [18]. A combination of SDN, machine learning, and network function virtualization was utilized to resolve cybersecurity issues in IoT systems. The hierarchical intrusion detection system (IDS) nodes detected the abnormalities and defined a policy for the software-defined network to prevent malicious traffic effectively. Detection of selective forwarding attacks in wireless IoT networks by analyzing the noise properties and the error probability is reported in [19]. The sentinel-based intrusion detection approach differentiated between common noise and other intrusion noises effectively using packet error probability. The approach had practical wireless IoT networks based on the IEEE standard. Though machine learning-based intrusion detection systems efficiently detected cyberattacks in IoT networks, sometimes, the machine learning model used for intrusion detection may also be subjected to cyberattack, which is termed as adversarial machine learning. These adversarial machine learning procedures manipulated network traffic and data that pass through the IoT devices, which creates confusion in the decision process. A rule-based approach presented in [20] generated adversarial machine learning samples and explored the performance of machine learning models for DoS attack detection. The results indicate that adversarial effects reduced the performance of machine learning models. A Bald-Eagle Search (BES) algorithm proposed in [21] was divided into three levels such as initialization, construction phase, and transmission phase for data transmission IoT networks. Performance was recorded with delay at 0.81s and efficiency of 97%.

A hybrid intrusion detection model presented in [22] incorporated the deep autoencoder and gradient support vector machine to detect intrusions in the IoT network. The stacked autoencoder extracted the network data features. From the selected features, optimal features were extracted using mutual information and a c4.8 wrapper. The presented intrusion detection system reduced the computation complexity of the network and detected impersonation attacks with a minimum false alarm rate. In [23], the features of deep learning architecture were utilized for intrusion detection as a deep migration learning model and to detect anomalies in the IoT network. The migration learning-based detection procedure attained better detection efficiency and minimum detection time compared to the conventional machine learning-based intrusion detection systems. A deep learning-based adaptive and resilient network intrusion detection model presented in [24] detected wireless network intrusions using deep learning techniques. The learning features of the network model were utilized to recognize the behavioral features of the environment and removed the intruder to reduce the security threats. Some of the research findings are summarized in Table 1.

From the above literature analysis, it is clear that machine learning-based intrusion detection models lag in performance due to feature selection procedures. The computational complexity of machine learning-based intrusion detection models increases due to the absence of data labels. Deep learning models exhibit better performance in feature selection, which can be utilized along with machine learning models for better intrusion detection in IoT networks. Considering this research summary, a hybrid intrusion detection model is presented to detect intrusions in wireless IoT networks.

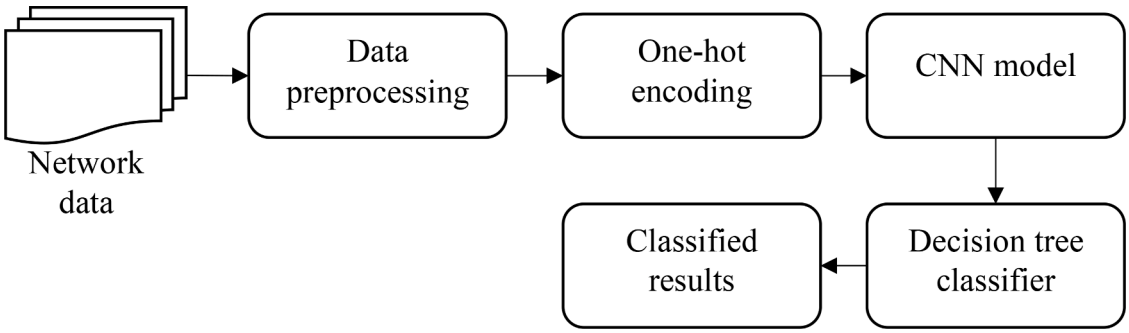

Fig. 1. Overview of the proposed intrusion detection system.

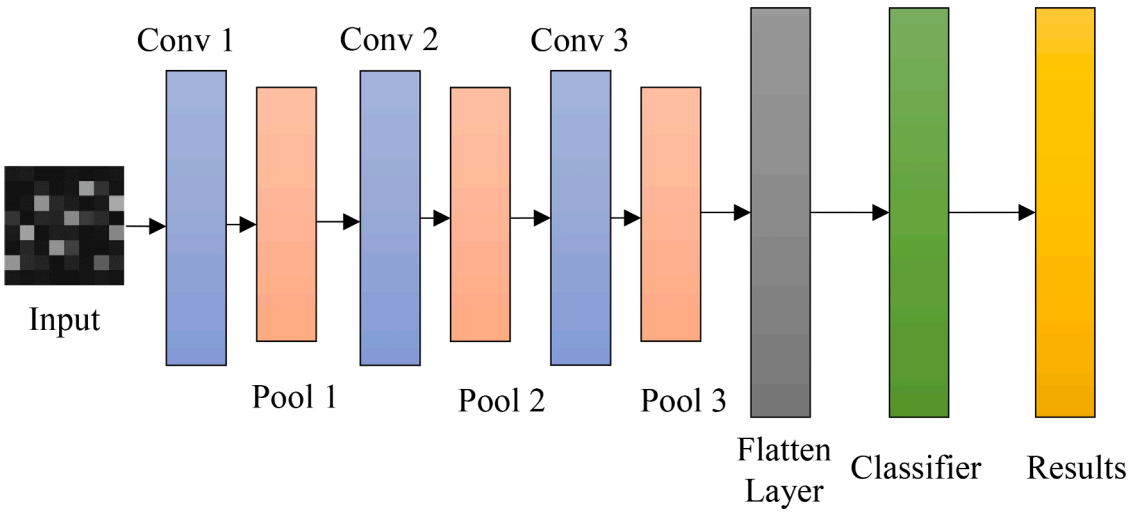

Fig. 2. Deep learning architecture.

3. Proposed work

The proposed deep learning-based intrusion detection system for wireless IoT networks using a Convolutional Neural Network (CNN) with a decision tree classifier is presented in this section. The novelty of the research work is present in the combination of classifier models used in the deep learning network. Instead of a fully connected neural network, the decision tree algorithm is used as a classifier in the proposed architecture. Conventional deep learning networks utilize a fully connected feed-forward network for classification purposes. The major limitation of a fully connected network is its neighborhood information loss. Also, it requires more parameters to optimize, and it is not translation invariant. Therefore, to utilize the features from the CNN model in an efficient manner for intrusion detection, a decision tree is employed as a classifier in the proposed model.

Decision tree is a simple and efficient machine learning classifier that is easy to interpret without any statistical knowledge. Decision trees require less data cleaning and can be used to solve both regression and classification problems. Different types of decision tree models available are ID3, BFtree, LMT, J48, etc. The proposed model utilizes the J48 decision tree model, as it provides maximum accuracy compared to other decision tree models. An overview of the proposed intrusion detection model is presented in Fig. 1. The process starts with data preprocessing in which, normalization is performed to reduce the differences in the feature values in dimensions. Since the data features are not even, it is essential to normalize by reducing the computational complexity. The standard min-max normalization is employed in the preprocessing step which maps the input data without altering the linear relationships. The normalization process is formulated as:

$$y = \frac{y - min}{max - min} \tag{1}$$

where, the minimum and maximum attribute are represented as *min* and *max* and the attribute value is represented as *y*. Followed by normalization, label numeration is performed which identifies the classes for the label records numerically. This numerical labeling simplifies the conversion of data features into images in the one-hot encoding process. One hot encoding encodes the binary vectors into a grayscale pixel. By adding empty pixels with the remaining pixel values, a complete image is obtained for analysis. A simple

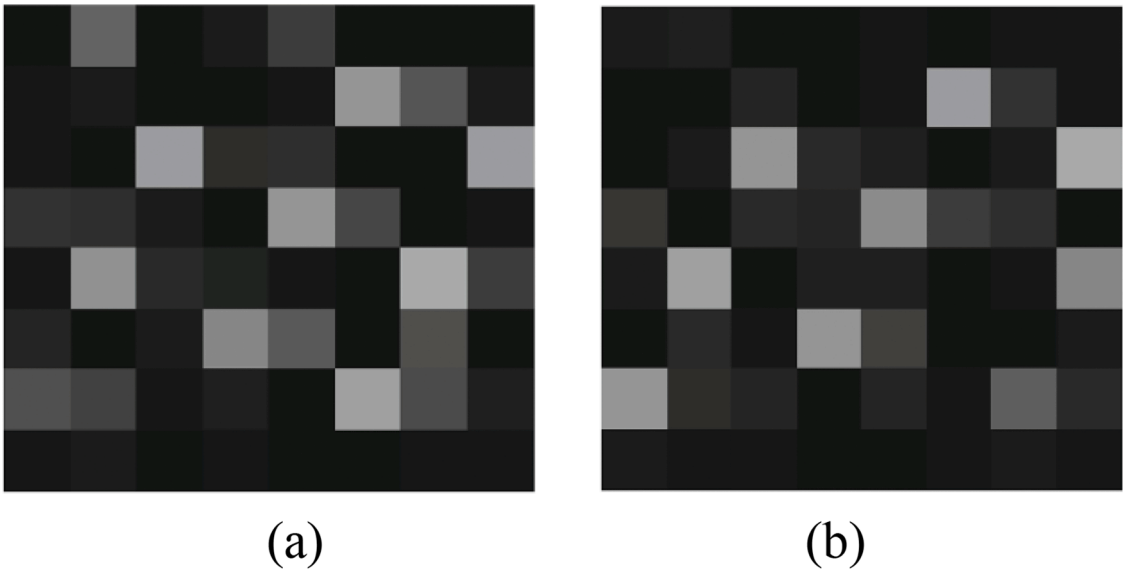

Fig. 3. Preprocessed data (a) Normal data (b) DoS attack data.

image scaling procedure is also incorporated to make sure the input images satisfy the entry conditions of the deep learning architecture.

The proposed hybrid intrusion detection system depicted in Fig. 2, processes the preprocessed data as shown in Fig. 3 through the convolution and pooling layers. The vectors are converted as an encoded binary image using one-hot encoding and the encoded image convolutes the features and provides to the pooling layer. Three convolution layers and three pooling layers are used in the architecture. These layers extract the optimal features from the input to output classifier and avoid data overfitting. Instead of the max-pooling layer, the average pooling layer is used in the proposed model to preserve the features of input data.

The convolution layer convolutes the features obtained from the previous layer and the process is mathematically defined as follows.

$$y_m^{i,j} = f\left(b_m^{i,j} + \sum_{s=1}^{S} w_{s,m}^{i,j} * l_{m+s-1}^{i-1,j}\right) \tag{2}$$

where, the output of the m^{th} neuron in layer i is represented as $y_m^{i,j}$, the function $f()$ indicates the activation function, the offset of the neuron for layer i is represented as $b_m^{i,j}$ and the output of the neuron for layer $i-1$ is represented as $l_{m+s-1}^{i-1,j}$ and the convolution kernel for i^{th} layer is represented as $w_{s,m}^{i,j}$. Followed by each convolution layer, a pooling layer is included in the architecture which reduces the dimensions of the features obtained from the convolution layer. This pooling operation reduces the network complexity by reducing the dimension and avoids data overfitting. Mathematically, the pooling layer function is expressed as:

$$\mathscr{O}_m^{i,j} = f\left(\delta_m^{i,j} pool\ \left(l_m^{i-1,j}\right) + b_m^{i,j}\right) \tag{3}$$

where, the m^{th} neuron output for layer i is represented as $\mathscr{O}_m^{i,j}$, the function $f()$ indicates the activation function, the offset of the neuron for layer i is represented as $b_m^{i,j}$, the sampling weight coefficient is represented as $\delta_m^{i,j}$, the pooling function is represented as $pool()$ and the output of the $i-1$ is represented as $l_m^{i-1,j}$. The process of convolution and pooling is performed three times as the architecture has three sets of convolution and pooling layers. Finally, before converting the features to flatten layer, a dropout function is introduced. This dropout layer helps the network to enhance the generalization ability and avoids overfitting.

The stride rate followed for all the convolution and pooling layers is '1' and the size of the input feature grayscale image is $60 \times 60 \times 2$. The dimensions of the first convolution and pooling layers are $56 \times 56 \times 2$ and $28 \times 28 \times 2$ respectively. The dimensions are reduced gradually in the successive layers. The dimensions of second convolution and pooling layers are $24 \times 24 \times 4$ and $12 \times 12 \times 4$ respectively. Similarly, the third layer dimensions are $8 \times 8 \times 8$ and $4 \times 4 \times 8$ for convolution and pooling layers respectively. The activation function used in the proposed architecture is Rectified Linear Unit (ReLU), which is computationally efficient than other activation functions. The dropout rate used in the proposed architecture is 0.25 and the flatten layer has 32 features which is fed as input to the classifier model. As mentioned in the initial discussion, fully connected neural network is replaced with decision tree classifier for better classification performances. Instead of regression model, the reason for selecting decision tree is due to the nature of the intrusion. As the intrusions are dynamic and do not occur continuously, regression models are avoided, and classification models are employed in the proposed architecture.

Table 2
NSL-KDD dataset training and testing records.

Attack	Train	Test
Normal	61642	15411
DoS	42708	10677
Probe	11262	2816
R2L	3106	776
U2R	95	24
Total	**118814**	**29703**

Decision tree algorithm classifies the features based on the attribute's behavior at several instances. Based on the training instances, new instances and its classes are obtained in the classification model. Moreover, the rule generation for the prediction process differentiates decision tree classifier from other classification models. The J48 is an ID3 extension which efficiently handles the missing values, continuous attribute ranges, rule derivation and decision tree pruning etc. The other algorithms perform classification recursively till the last leaf which requires a complete perfect data. Whereas J48 generates rules for the classification which increases the generalization ability of the decision tree model and provides more flexibility with enhanced accuracy in feature classification. The information gain mentioned in the algorithm is calculated based on the number of cases and subsets for the attributes. Mathematically, the information gain for attribute (z) is formulated as follows.

$$Gain = info(S) - \sum_{m=1}^{t} \frac{|S_i|}{|S|} \times info(S_i) \tag{4}$$

where, the set of cases is represented as S, the subset is represented as S_i, the set has distinct value for attribute (z), and the entropy function $info(S_i)$ is given as,

$$info\ (S_i) = -\sum_{i=1}^{M\ class} \frac{freq(c_i, S)}{|S|} \log_2 \left(\frac{freq(c_i, S)}{|S|} \right) \tag{5}$$

where, the entropy function is represented as *info*(.), frequentist probability of class in data is represented as *freq*(.) and c_i represents the class. In practical, if the generated decision tree is large, the confidence level of the decision tree is adjusted to simplify the decision tree classification process. The summarized pseudocode for the decision tree classifier used in the proposed deep learning-based intrusion detection model is given as follows.

Pseudocode for decision tree classifier for intrusion detection

```
Initialize root node M, testing attribute (ta)
If (N belongs to same category S)
{
Leaf node + M
Mark M as class S
Return M
}
For j=1 to m
Obtain the information gain
If (ta, M == continuous)
Obtain the threshold value
Split S based on the threshold
For each S
If (S is empty)
Select the child of M is a leaf node
Else
Select the child M = tree
Obtain the classification error rate of node M
Return M
End if
End for
End
```

4. Result and discussion

The performance analysis of the proposed hybrid intrusion detection system for wireless IoT network is verified through simulation performed in MATLAB R2017b. The simulation environment operating system is Windows 10 installed in an intel i5 processor with 16GB memory. Benchmark NSL-KDD dataset is used to validate the performance of proposed intrusion detection model. The dataset is used to train and test the model in 80:20 ratio. A five-fold cross validation technique is used to split the data for training and testing. For

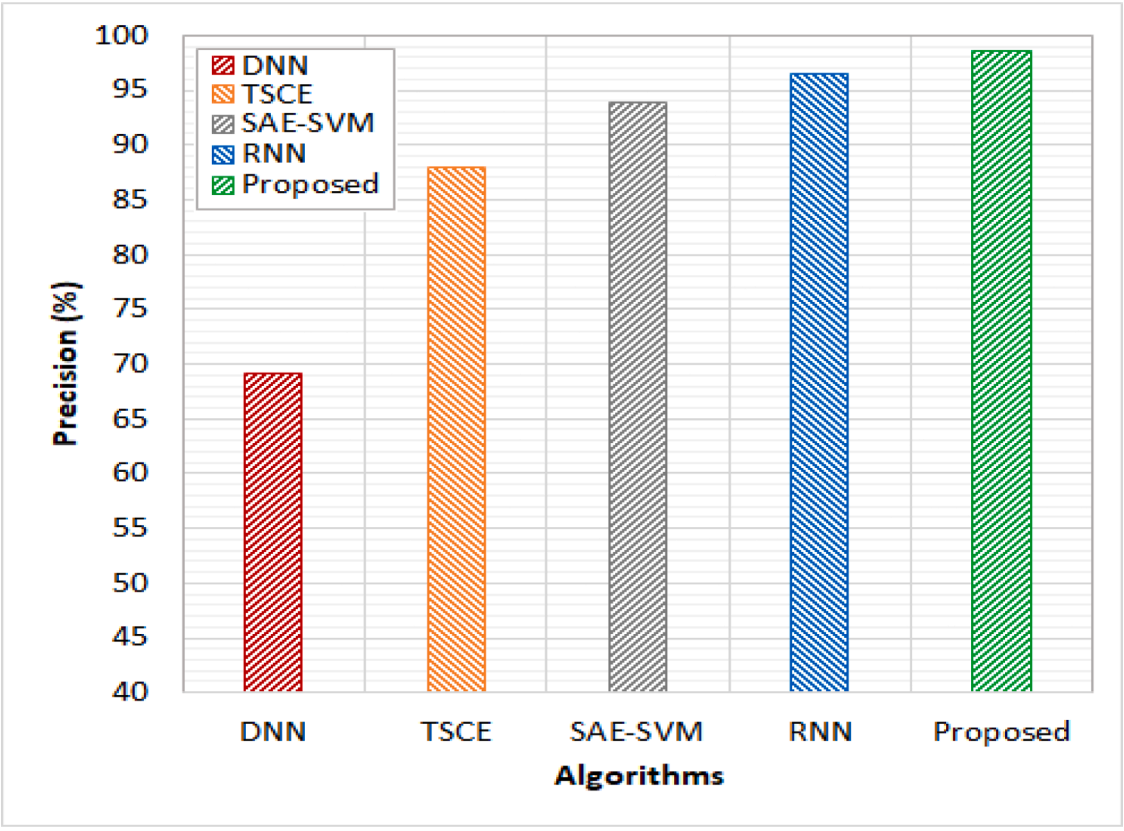

Fig. 4. Comparison of Precision parameter.

deep learning model, the hyperparameters are obtained from the architecture. The number of convolution and pooling layers are three and the optimizer function used in the experimentation is Adam optimizer. The kernel function selected is [5] and the activation function is ReLU. The details of dataset used for training and testing is depicted in Table 2.

The dataset has four types of attack data and normal data. The attacks are categorized into Denial-of-Service attack (DoS), probing attack (Probe), root to local attack (R2L) and user to remote attack (U2R). A total of 41 features is comprised of 38 numeric and 3 non-numeric features. Amongst these, 34 features are continuous, and 7 features are discrete in nature, and the features are arranged based on the content, traffic and basic characteristics. The one hot encoding used in the preprocessing step, converts the non-numeric features into numeric features. The attributes in the protocol type are User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Internet Control Message Protocol (ICMP), and it is encoded as (0,1,0), (1,0,0) and (0,0,1) respectively. The converted features are presented as feature map image to the deep learning model for further feature selection, and the decision tree classifies the features to detect the attack type. A confusion matrix is obtained based on the experimental parameters like True Positive (TP), True Negative (TN), False Negative (FN) and False positive (FP). Based on the these values the performance of the proposed model is evaluated in terms of accuracy, precision, recall and f1-score.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

$$Falsepositiverate = \frac{FP}{FP + TN} \tag{8}$$

$$FalseNegativerate = \frac{FN}{FN + TP} \tag{9}$$

$$Precision = \frac{TP}{TP + FP} \tag{10}$$

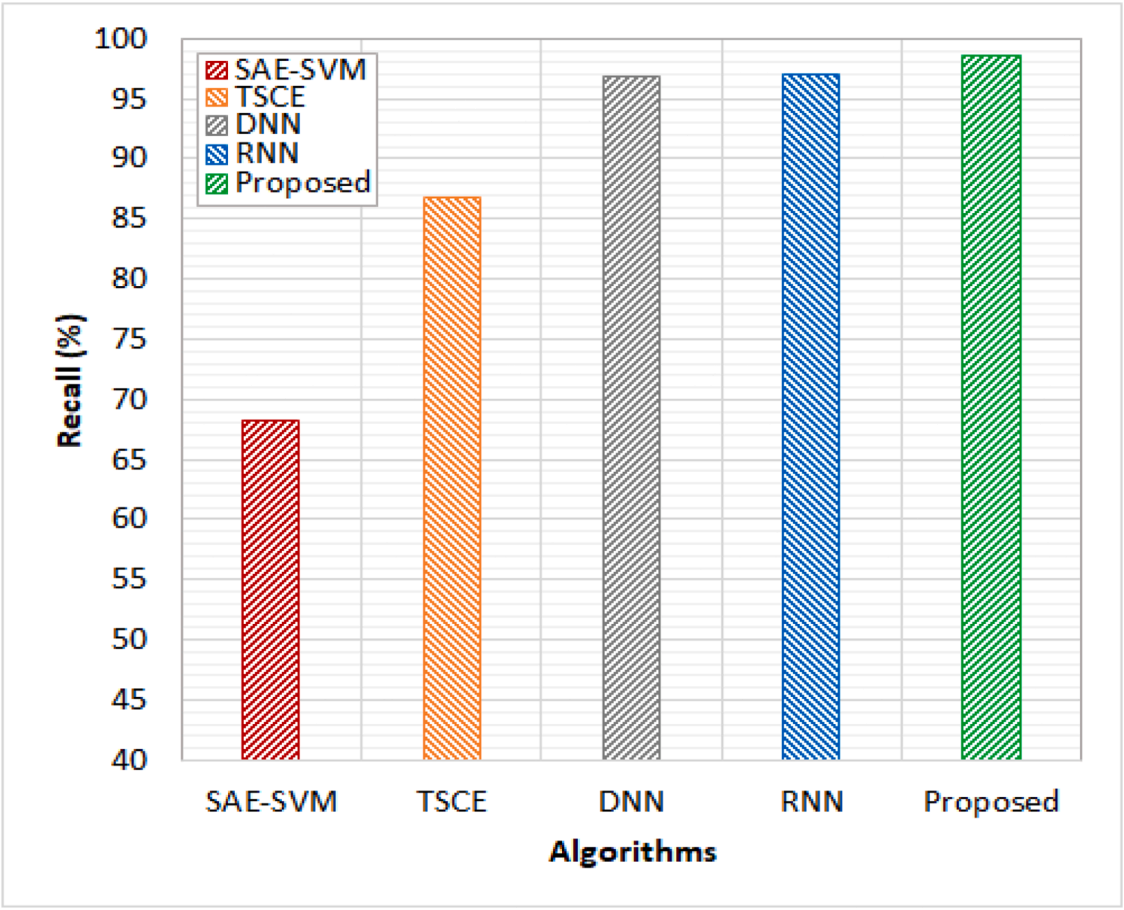

Fig. 5. Comparison of Recall parameter.

$$f1\ score = 2 \times \left(\frac{Precision\ \times Recall}{Precision + Recall} \right) \tag{11}$$

To validate the superior performance of the proposed hybrid intrusion detection model, existing techniques like Deep Neural Network (DNN) [25], Sparse Autoencoder with SVM (SAE-SVM) [24], Recurrent Neural Networks (RNN) [22] and Two-Stage Classifier Ensemble (TSCE) [23] models that utilize the same benchmark dataset, are used in the comparative analysis.

Fig. 4 depicts the comparative of analysis of the proposed model and the existing models in terms of precision parameter. The precision parameter is obtained based on the ratio of the number of attacks detected by the system to the number of attack scenario provided as input to the system. By formulation, it is simply defined based on the total number of true positive to the sum of false positive and true positive values obtained in the confusion matrix. It is observed from the Fig. 5 that, the maximum precision value is attained by the proposed hybrid intrusion detection model. The performance of RNN is slightly lesser in the proposed model, whereas other models exhibit huge difference in precision factor compared to the proposed detection model.

The recall is the ratio of the number of attacks detected by the system to the total number of attacks. Mathematically, it is ratio of true positive to the sum of true positive and false negative. It is observed from the results that, the maximum recall value of 98.24% is obtained by the proposed hybrid intrusion detection model which is 30% greater than that of the SAE-SVM model and 11 % greater than that of the TSCE model. Other deep learning models like DNN and RNN exhibits minor deviations in recall of nearly 1%, when compared to that of the proposed model.

Based on the precision and recall values, F1-score for the proposed model and existing models are calculated and depicted in Fig. 6. Higher F1-score indicates the better performance of the proposed model in the intrusion detection process. The maximum precision and recall values increase the F1-score of the proposed model. It can be observed from Figs. 4 and 5, that the maximum value is attained by the proposed model for precision and recall. Thus, the proposed model f1-score attains the maximum compared to other methods. Numerically, the F1-score obtained by the proposed model is 98.45 % which is 20% greater than that of the SAE-SVM model, 17% greater than that of the DNN model, 11% greater than that of the TSCE model and 2% greater than that of the RNN model.

The detection accuracy of the proposed model is measured based on the actual attacks detected to the total number of attacks. Mathematically based on the true positive values, the detection accuracy of the system has been evaluated. It is observed from the

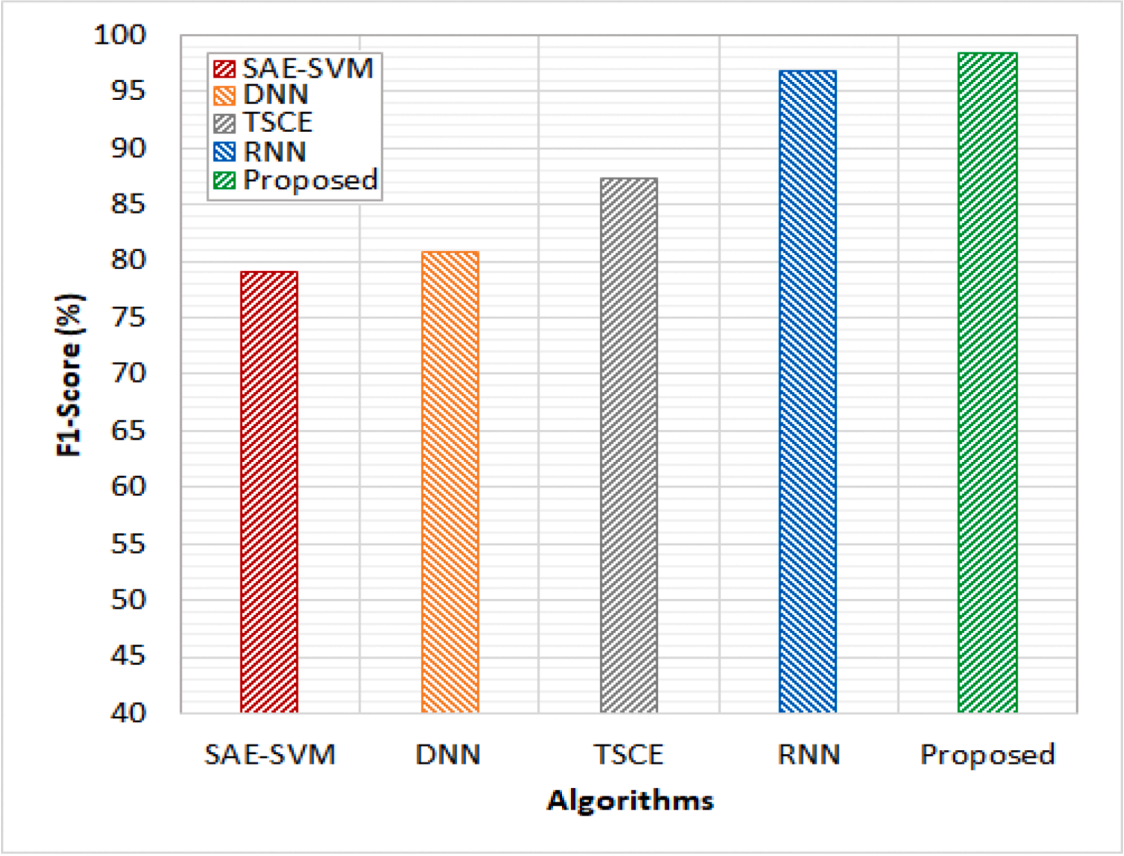

Fig. 6. F1-score comparison.

results depicted in Fig. 7 that the maximum accuracy of 99.49% is attained by the proposed model, and it detects most of the attacks as listed in the dataset. On comparison, the performance of the proposed model is 20% greater than that of the DNN and SAE-SVM models, 16% greater than that of the RNN model, and 13% greater than that of the TSCE model. The error rate for the proposed model can be evaluated from the obtained accuracy values. The general error rate is formulated as,

$$Error\ rate\ = 1 - Accuracy \tag{12}$$

Based on the above equation, it is observed that the error rate for the proposed model is 0.006, whereas the error rate for TSCE model is 0.143, error rate of RNN is 0.167, error rate of SAE-SVM is 0.1952 and DNN exhibits the error rate of 0.199.

The results obtained in the experimental analysis are summarized for better understanding in Table 3. It is observed that, due to the utilization of optimal feature selection using the hybrid model in place of conventional feed forward neural network, the intrusion detection performance is increased. The maximum performance attained by the proposed model for all the parameters, clearly indicates that this model is suitable for IoT networks to detect different types of intrusions. Though the performances are measured for benchmark dataset, the performance of proposed model will be same for real time data also. However, there will be small deviations in detection accuracy due to network characteristics and data diversity.

5. Conclusion

A hybrid intrusion detection model for wireless IoT networks using deep learning and machine learning techniques, has been presented in this research work. The deep network feature characteristics are utilized to select the essential features in the intrusion detection process. Further, to improve the classification accuracy, decision tree algorithm is used to classify the selected features from convolution layers. The experimentation is carried out with the benchmark NSL-KDD dataset and is compared with the existing intrusion detection systems like Deep Neural Network (DNN), Recurrent Neural Networks (RNN), Two-Stage Classifier Ensemble (TSCE), and Sparse Autoencoder with SVM (SAE-SVM). Experimental results confirm the better performance of proposed model in terms of precision, recall, F1-score and accuracy. With maximum detection of 99.49%, the proposed hybrid intrusion detection model detects maximum attacks in the dataset. Further, this research work can be extended by introducing concatenated deep learning architectures for multiple attack detection.

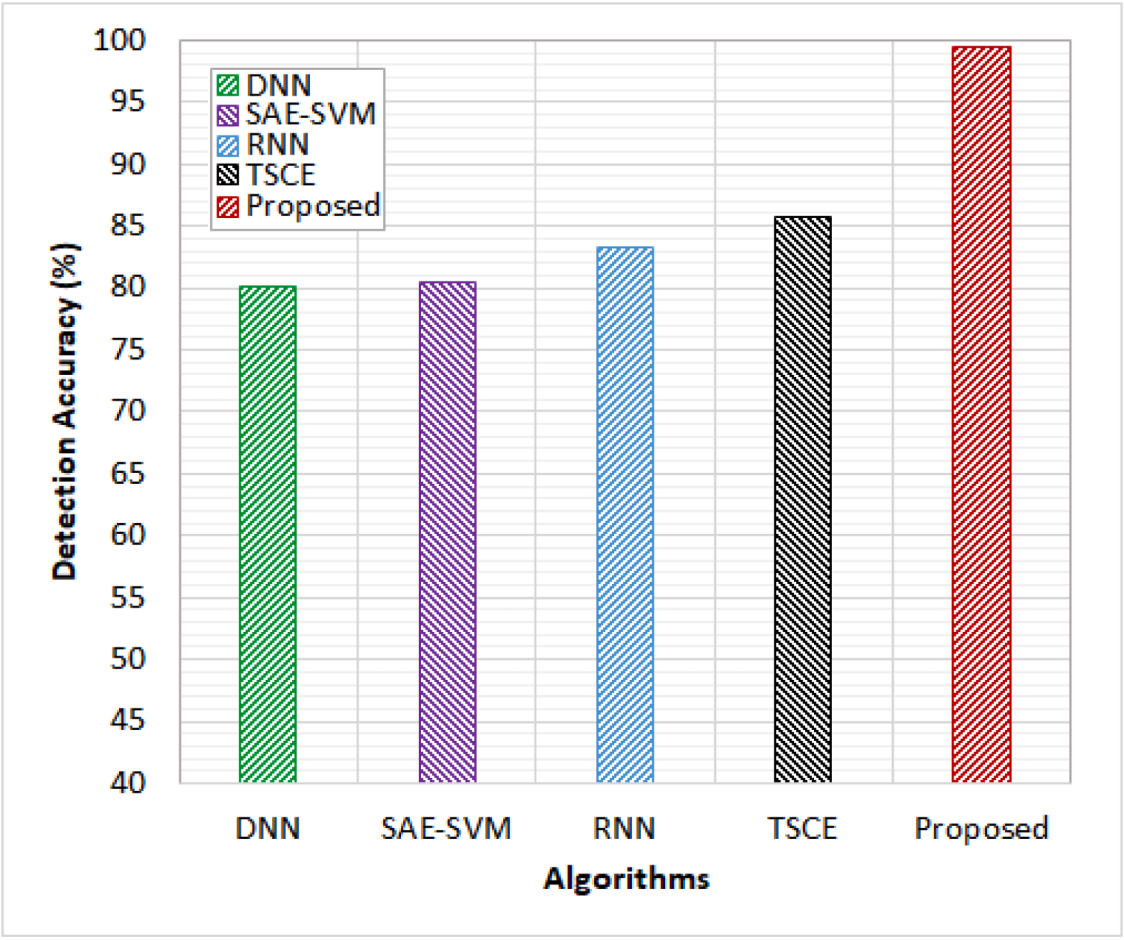

Fig. 7. Accuracy comparison.

Table 3
Performance comparative analysis.

Algorithms	Precision(%)	Recall(%)	F1-Score(%)	Accuracy(%)
DNN [22]	69.20	96.90	80.74	80.1
SAE-SVM [23]	93.92	68.28	79.07	80.48
RNN [24]	96.50	97.09	96.79	83.28
TSCE [25]	88.00	86.80	87.40	85.79
Proposed	**98.66**	**98.24**	**98.4496**	**99.49**

Declaration of Competing Interest

All author states that there is no conflict of interest.

Data Availability

No data was used for the research described in the article.

References

[1] Atul Dhanke Jyoti, Kamalraj R, Khasim Syed. A machine learning based IoT for providing an intrusion detection system for security. Microprocess Microsyst 2021;82:1–10.
[2] Benkhelifa Elhadj, Welsh Thomas, Hamouda Walaa. A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems. IEEE Commun Surv Tut 2018;20(4):3496–509.

[3] Pundir Sumit, Wazid Mohammad, Singh Devesh Pratap, Das Ashok Kumar, Rodrigues Joel JPC, Park Youngho. Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges. IEEE Access 2020;8:3343–63.
[4] Butun Ismail, Österberg Patrik, Song Houbing. Security of the internet of things: vulnerabilities, attacks, and countermeasures. IEEE Commun Surv Tut 2020;22 (1):616–44.
[5] Hajiheidari Somayye, Wakil Karzan, Navimipour Nima Jafari. Intrusion detection systems in the Internet of things: a comprehensive investigation. Comput Netw 2019;160:165–91.
[6] Kiran Sai, Devisetty RNKamakshi, Karthi R. Building a intrusion detection system for IoT environment using machine learning techniques. Procedia Comput Sci 2020;171:2372–9.
[7] Yoon John. Deep-learning approach to attack handling of IoT devices using IoT-enabled network services. Internet Things 2020;11:1–21.
[8] Jacob IJeena, EbbyDarney P. Design of deep learning algorithm for IoT application by image based recognition. J ISMAC 2021;3(3):276–90.
[9] Chen Joy Iong-Zong, Lai Kong-Long. Deep convolution neural network model for credit-card fraud detection and alert. J Artif Intell 2021;3(02):101–12.
[10] Araujo-Filho Paulo Freitas de, Kaddoum Georges, Campelo Divanilson R, Santos Aline Gondim, Macêdo David, Zanchettin Cleber. Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment. IEEE Internet Things J 2021;8(8):6247–56.
[11] Satam Pratik, Hariri Salim. WIDS: an anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) Protocol. IEEE Trans Netw Serv Manage 2021;18(1): 1077–91.
[12] Malathi C, Naga Padmaja I. Identification of cyber-attacks using machine learning in smart IoT networks. Mater Today: Proc 2021:1–6. https://doi.org/10.1016/j.matpr.2021.06.400.
[13] Wu Kehe, Li Jiawei, Zhang Bo. Abnormal detection of wireless power terminals in untrusted environment based on double Hidden Markov model. IEEE Access 2021;9:18682–91.
[14] Gad Abdallah R, Nashat Ahmed A, Barkat Tamer M. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access 2021;9:142206–17.
[15] Saheed Yakub Kayode, Arowolo Micheal Olaolu. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access 2021;9:161546–54.
[16] Meng Weizhi, Li Wenjuan, Su Chunhua, Zhou Jianying, Lu Rongxing. Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. IEEE Access 2018;6:7234–43.
[17] Thamilarasu Geethapriya, Odesile Adedayo, Hoang Andrew. An intrusion detection system for internet of medical things. IEEE Access 2020;8:181560–76.
[18] Baraneetharan E. Role of machine learning algorithms intrusion detection in WSNs: a survey. J Inf Technol 2020;2(03):161–73.
[19] Karuppusamy Dr P. Machine learning approach to predictive maintenance in manufacturing industry-a comparative study. J Soft Comput Paradigm 2021;2(4): 246–55.
[20] Chen Joy Iong Zong, Lai Kong-Long. Machine learning based energy management at internet of things network nodes. J Trends Comp Sci Smart Technol 2020; (3):127–33. September 2020.
[21] Li Daming, Deng Lianbing, Wang Haoxiang. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int J Inf Manag 2019;49:533–45.
[22] Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S. Deep learning approach for intelligent intrusion detection system. IEEE Access 2019;7:41525–50.
[23] Al-Qatf M, Lasheng Y, Al-Habib M, Al-Sabahi K. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access 2018;6:52843–56.
[24] Yin C, Zhu Y, Fei J, He X. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 2017;5:21954–61.
[25] Tama BA, Comuzzi M, Rhee KH. TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. IEEE Access 2019;7: 94497–507.

Judy Simon received the M.E. (Applied Electronics) and Ph D from Sathyabama University Chennai in 2012 and 2021 respectively. She is currently Assistant Professor in Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India. Her research interests include Wireless Communication Systems, Sensor Networks, and Internet of Things.

Nellore Kapileswar received the B.Tech. ECE from JNTU Hyderabad in the year 2007 and the M.Tech in Nanotechnology from VIT University, Vellore, India in 2009. He is working and currently pursuing his Ph.D in ECE Department, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India. His research interests include Communication Systems, Wireless Sensor Networks and Internet of Things.

Phani Kumar Polasi received the Ph.D in ECE from Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India in 2017. He is currently working as Professor and Head of ECE Department SRM Institute of Science and Technology (formerly known as SRM University), Ramapuram Campus, Chennai, Tamil Nadu, India. His research interests include Wireless Communication Systems, Signal Processing and sensor networks.

Aarthi Elaveini received her M.E degree in Embedded Systems Technologies from Anna University, in 2012. She is currently pursuing her Ph. D at SRM University. She is currently working as an Assistant Professor in the department of ECE, SRM Institute of Science and Technology, India. Her research interests are in the areas of wireless communication systems, Image processing, visible light communication.