

# Hybrid intrusion detection model for hierarchical wireless sensor network using federated learning

Sathishkumar Mani<sup>1</sup>, Parasuram Chandrasekaran Kishoreraja<sup>2</sup>, Christeena Joseph<sup>3</sup>, Reji Manoharan<sup>4</sup>,  
Prasannavenkatesan Theerthagiri<sup>1</sup>

<sup>1</sup>Department of Computer Science and Engineering, GITAM School of Technology, GITAM University, Bengaluru, India

<sup>2</sup>School of Computer Science and Information Systems, Vellore Institute of Technology, Vellore, India

<sup>3</sup>Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India

<sup>4</sup>Department of Electronics and Communication Engineering, Rohini College of Engineering and Technology, Kanyakumari, India

## Article Info

### Article history:

Received Apr 18, 2024

Revised Aug 12, 2024

Accepted Aug 30, 2024

### Keywords:

Attacks

Federated learning

Global aggregator server

Intrusion detection systems

Wireless sensor network

## ABSTRACT

The applications of wireless sensor networks are vast and popular in today's technology world. These networks consist of small, independent sensors that are capable of measuring various physical quantities. Deployment of wireless sensor networks increased due to immense applications which are susceptible to different types of attacks in an unprotected and open region. Intrusion detection systems (IDS) play a vital part in any secured environment for any network. IDS using federated learning have the potential to achieve better classification accuracy. Usually, all the data is stored in centralized server in order to communicate between the systems. On the other hand, federated learning is a distributed learning technique that does not transfer data but trains models locally and transfers the parameters to the centralized server. The proposed research uses a hybrid IDS for wireless sensor networks using federated learning. The detection takes place in real-time through detailed analysis of attacks at different levels in a decentralized manner. Hybrid IDS are designed for node level, cluster level and the base station where federated learning acts as a client and aggregated server.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Parasuram Chandrasekaran Kishoreraja

School of Computer Science and Information Systems, Vellore Institute of Technology

Vellore, India

Email: kishoreraja.pc@vit.ac.in

## 1. INTRODUCTION

The wireless sensor network is extensively used in many applications like measuring the temperature of volcanoes. The network is simple, low-cost, energy-efficient, and distributed sensing and processing, which depicts the network to security attacks [1]. Traditional methods like cryptography methods are no longer used to defend the network. Instead, an intrusion detection system (IDS) detects all kinds of attacks. Considering all limitations in wireless sensor networks, IDS are specific to detect particular types of attacks [2]. Most attacks happened in sensor networks due to misbehavior of route updates. This research work uses different levels of IDS using federated learning. Most of the IDS use a distributed detection process in order to lessen the computational load, but another problem arises: communication overhead [3], [4]. The authors presented anomaly detection and communicated to a global model system. It uses estimators for its anomaly IDS [4]. There are various classifiers, co-variance parameters, and statistical tools used to [5]–[9] detect distributed anomalies. Hybrid algorithms are proposed using Quantum particle swarm optimization (PSO) and radial basis function neural network (RBFNN) [10]–[12]. Numerous neural network-based IDS are proposed, which give better approximation ability, good classification and fast convergence [13].

In recent years, machine learning (ML) and deep learning (DL) algorithms have been used in many domains, such as healthcare and image processing. IDS, using ML techniques, learns all kinds of traffic [14], [15]. The detection process is totally based on data collected and stored centrally in the server. It is found that the accuracy decreases due to large data sets with high packet loss rates [16], [17]. The problems can be addressed by federated learning. This algorithm learns data generated by the devices in a collaborative fashion without any centralized server. It works with decentralized data from devices which are communicated in either direction. The traditional centralized learning methods expect to follow local learning and attainment of privacy preservation and cost reduction [18]–[20]. This research proposed hybrid intrusion detection for wireless sensor networks using federated learning. The authors proposed a DL-based IDS with four different strategies [21]. Kwon *et al.* [20] reviewed only seven DL-based solutions for IDS.

There are different types of IDS available, which evaluate various information available on single or multiple hosts as well as analyzing from captured packets during transmission between the nodes. Signature-based intrusion detection uses patterns in the detection model, whereas the anomaly detection model looks for abnormality in network traffic. Anomaly detection techniques use statistical models, neural networks, data mining, and computational intelligence in the learning module. Today, DL models and artificial intelligence techniques gather a lot of interest in designing the intrusion detection model. One of the problems is feature selection, which affects the entire performance of the systems. There is a tradeoff between security and performance metrics while choosing an IDS technique.

There are different types of IDS for wireless sensor networks with respect to architectural design. One is centralized, and the other is distributed [14]. Today, most of the IDS are distributed where the detection is done in a local node. The problem is to spend a significant energy for coordination among all nodes. Further, the nodes are unable to detect certain attacks since it has knowledge about its neighborhood only. Single point failure occurs in centralized IDS due to communication problems between the nodes that create large communication overhead. The third type of IDS is the hybrid model, which is a combination of distributed and centralized IDS.

Learning algorithms like ML and DL are used in many domains, such as healthcare and image processing. IDS, using ML techniques, learns all kinds of traffic. The detection process is totally based on data collected and stored centrally in the server. It is found that the accuracy decreases due to a large data set with a high packet loss rate [20]. The problems can be addressed by federated learning. This algorithm learns data generated by the devices in a collaborative fashion without any centralized server [22]. It works with decentralized data from devices which are communicated in either direction. There are two stages: local learning and model transmission, which permit the accomplishment of privacy preservation and cost reduction. In the traditional method of intrusion detection, all information is maintained in a centralized server and also transferred this information between server and host, which are vulnerable to man-in-the-middle attacks [23]. Federated learning methods work in a decentralized manner with this information [24]. So, it is efficient and enforces a privacy policy for sensitive data. There are numerous approaches to intrusion detection using federated learning. Sunny *et al.* [25] proposes using mimic learning in combination with federated learning to protect against reverse engineering attacks. Most ML and DL models suffered from false negative alarms [26], [27].

This research proposed hybrid intrusion detection for wireless sensor networks using a federated learning algorithm. A typical artificial neural network has different phases. It uses supervised and unsupervised training algorithms. The pattern recognition problems can be solved by incorporating the supervised algorithms. The classification problems can be solved by incorporating unsupervised algorithms where the network learns without the knowledge of the desired output [28], [29]. The significance of the neural network is that it repeatedly learns the coefficients. The coefficients are adjusted to normal data and attack data during the training phase. The neural network approach improves the detection rate, and the false alarm is reduced [30], [31].

## 2. METHOD

The proposed model is layered and clustered with a hybrid IDS model. Each IDS is placed on the client side with sensor nodes. All are operated in a distributed manner. A hybrid Hierarchical network consists of a sensor node and a client which holds local IDS systems. It identifies the data anomaly with respect to the sensor node and client. Anomaly is detected based on the mean variance and data distribution is correlated with sensor node and client locally. After the selection of cluster heads among nodes, cluster-based IDS (CBIDS) is activated in order to detect different types of attacks such as selective forwarding, flooding, selfish misbehaviour, node replication attacks and sinkhole attacks. All behaviour analysis is done using federated learning architecture. The federated learning-based IDS for wireless sensor network architecture is given in Figure 1.

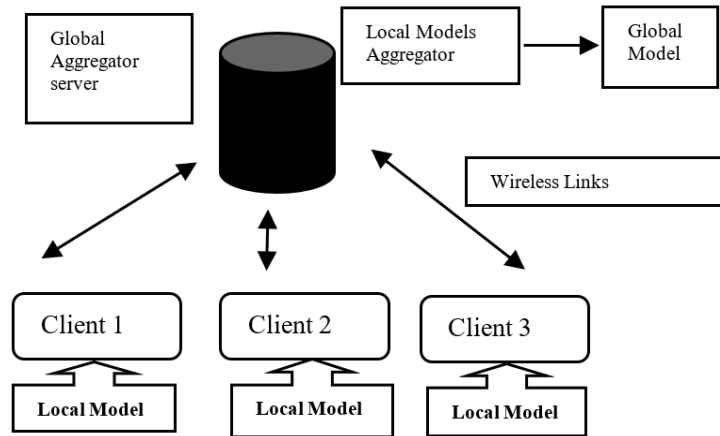


Figure 1. Federated learning-based IDS in wireless sensor network

The proposed architecture is divided into two parts—the client side and the server side. The client-side has local model data aggregation and sensor devices. The server side has a global aggregator server and a local model aggregator, which leads to the global model. In this architect, each local client model trains the data acquired from sensor devices with the local models shared by the server. Further, the IDS at the client end detects any unwanted attacks at the node level and cluster level. An analyzer is used to monitor and track their network traffic data as well as node data for subsequent analysis. Clients are trained locally and globally for data aggregation. The detection module aggregates all trained data from clients and analyse the data to check the abnormal behavior of the wireless sensor network. The use of a global aggregation server is to transform local learning into global learning. A client is able to detect intrusions by comparing behaviors obtained from global learning and improves the detection.

### 2.1. Implementation

The proposed work first client trains a local dataset and then shares the data with a global aggregator rather than on a central server. The global aggregation server interacts with all clients and looks for local IDS models. It creates an updated global model with all client's IDS models with optimal parameters. The equation uses the starting weights ( $w$ ) and number of federated learning rounds ( $R$ ); the convergence level can be achieved by changing weights and number of federated learning rounds again and again. At round  $t$ , each local client's weight is communicated and updated to the aggregation server (1) is used from the FedAvg algorithm [28] to update the model weights.

$$W_{t+1} = \sum_{k=1}^K n_k / n w_{t+1}^k \quad (1)$$

Where  $n$  is the total size of all client datasets, and  $n_k$  represents the size of each client dataset.  $w_{t+1}^k$  is the updated global model after the iteration.

### 2.2. Algorithm for local intrusion detection system on the client side

The algorithm for the local IDS on the client side is summarized in this section. The following algorithm is implemented on each client side, and the local analyzer evaluates sense data for abnormalities.

Step 1: Check the sensor data. create a table and store it

Step 2: Take the table. Check the size and compare it with a threshold. Compute variance

Step 3: Compute abnormalities in the table. Check the condition of data anomaly with a threshold value

Step 4: Otherwise, drop it. Forward to a global leader

The global aggregation server initiates a neural network model (NNM) from a global intrusion detection model. Each uses the global model. Each client creates local weights with their private data, and each client calculates a fresh set of local weights and works parallelly with the global model. The clients use sensor data collected locally and analyse with local analyser. The local client model works with the global aggregation model in order to improve the IDS and communicate with the global aggregation server. The global aggregation server adapts changes received from local clients and adds the weights from the various local node models in order to produce a new, improved model (1). The parameters are evaluated on the basis of dataset size at every node. Once again, updated model parameters are communicated with clients for the changes that occurred in

the centralized server. Every client routine the novel classical parameters and makes variations to them based on the novel data. The process is repeated for the improvement of learning.

Data packet information is given in the input of a neural network, which has one input layer, one hidden layer and an output layer. This neural network-based IDS is implemented in cluster head for detecting the attacks. So, four neurons have been given to the input of the neural network. Normal and abnormal condition is created in the training phase. Centre of activation function and spread factor is initiated and the spread factor. Performance is totally based on a number of parameters in a neural network. Hidden layer parameters and radius of the RDF function play crucial functions in the performance of the IDS system.

### 2.3. Algorithm for global intrusion detection system

The algorithm for the global IDS is summarized in this section. The input parameters to the federated learning structure are given. Different types of attacks can be detected.

Step 1: Initialize self-organisation map parameters

Step 2: Initialize the weights for the neural network

Step 3: Compute the output of every node and error Function4.

Step 4: Check the condition for error

Step 5: Otherwise, update the self-organization parameters and weights of the neural network. Calculate the output of every node.

The detection of attack and techniques is tabulated in Table 1.

Table 1. Detection and techniques

IDS	Technique
CBIDS	Federated learning methods
SBIDS	Federated learning methods
NBIDS	Rule-based

## 3. RESULTS AND DISCUSSION

Tensorflow and keras are used for ML and DL. Simulation is carried out in network simulator version 2 (NS2) in order to extract wireless sensor network parameters. Simulation parameters are listed in Table 2. Datasets are generated from NS2 and sensors to train and test IDS. The testbed was created for two types of attacks which are distributed denial-of-service (DDoS) attacks and man-in-the-middle (MIM) attacks. Initially, the data is preprocessed. The feature selection approaches were applied to reduce training and classification time. Table 3 displays the selected data for ML models. The tests were performed using federated learning. The efficacy of federated learning was evaluated with 2 or 3 clients.

Table 2. Simulation parameters

Parameters	Values
Area	600×600
Nodes (Number)	100
Simulation time in seconds	100
Protocol for routing	HIDS
Energy (Joules)	100
Interval	4 to 6
Number of attackers	- 4
Packet Size (bytes)	50 to 100

Table 3. Data set for ML model

Type	Total	Train	Test
Normal	11,222	8,856	2,466
DDoS_UDP Attack	5,508	4,478	3,299
DDoS_ICMP Attack	8,195	6,989	3,956
DDoS_HTTP Attack	9,789	7,221	3,777
DDoS_TCP Attack	8,358	6,136	3,546
MIM Attack	1,725	1,238	674

### 3.1. Performance evaluation

Network performance parameters were analyzed with different packet size e and interval. Performance is measured with two parameters. They are the detection ratio and false positive rate. The graphs are analyzed in Figure 2. Figure 2(a) depicts the packet size vs jitter, Figure 2(b) depicts the packet size vs

packets dropped, Figure 2(c) depicts the interval vs packets dropped, Figure 2(d) depicts the interval vs throughput, Figure 2(e) depicts the attacker vs throughput, and Figure 2(f) depicts the jitter vs attacker. The results show an improvement in the performance of the anomaly detection performance system with a reduction of false positive rate and high detection ratio. It shows the performance graph for hybrid IDS architecture. IDS performance can be evaluated by the following parameters. Correct positive (CP): the number of attack samples out is divided by accurately detected attacks in the total samples. Untrue positive (UP): the number of normal samples is divided by incorrectly identified as attacks in the normal samples. Correct negative (CN): the number of benign samples is divided accurately and classified as normal. Untrue negative (UN): the number of attack samples is divided by wrongly recognized as normal.

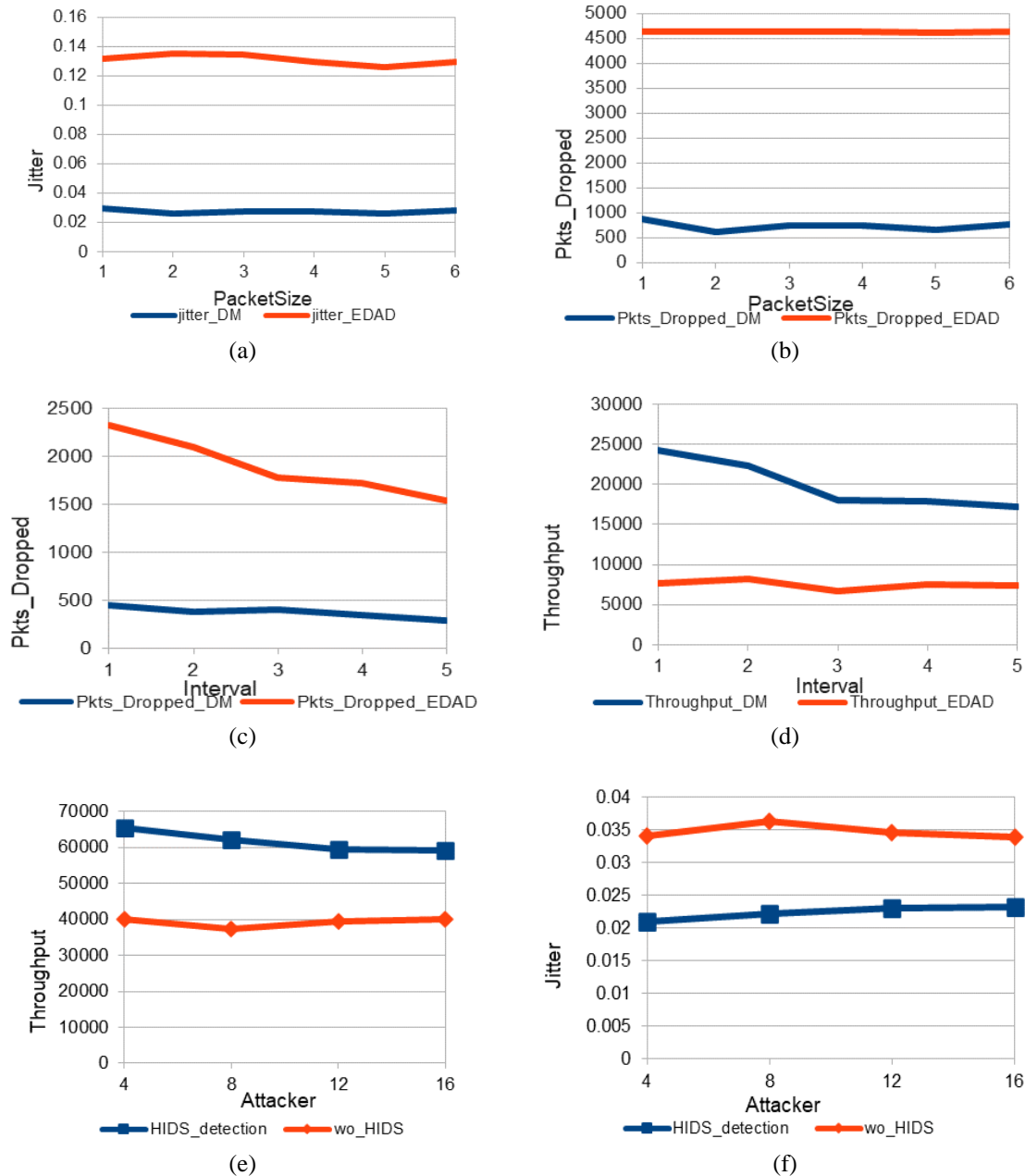


Figure 2. Performance graph for data anomaly in NBIDS: (a) packet size vs jitted, (b) packet size vs packets dropped, (c) interval vs packets dropped, (d) interval vs throughput, (e) attacker vs throughput, and (f) jitter vs attacker

The performance metrics are evaluated by two parameters. Detection ratio: the ratio between the number of correctly identified attacks and expected attacks. False alarm rate: it is the ratio between the identification of normal samples as attack with normal samples. Figures 3(a) and 3(b) shows the performance graph for hybrid IDS architecture. Table 4 shows the results of ML approaches for a centralized model in terms of detection ratio. This table gives information about how IDS differentiates attacks and benign classes in the dataset. The detection ratio for RNN and CNN approaches is reached at peak values of 93% and 95%, respectively. Table 5 shows the comparison of the detection ratio in global models.

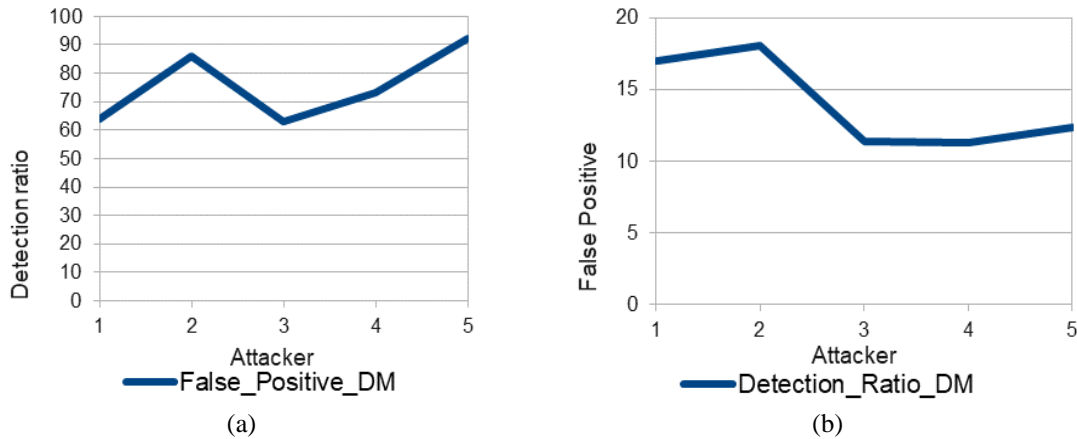


Figure 3. Performance graph for hybrid IDS architecture (a) attacker vs false positive and (b) attacker vs detection ratio

Table 4. Intrusion detection at global aggregation server

Class	Detection ratio	
	CNN	RNN
Normal	0.93	0.95
DDoS_UDP Attack	0.88	0.89
DDoS_ICMP Attack	0.80	0.81
DDoS_HTTP Attack	0.60	0.55
DDoS_TCP Attack	0.93	0.94
MIM Attack	0.93	0.95

Table 5 Comparison of detection ratio

Classifier	Clients	Federated learning model detection ratio
CNN	2	64.23
	3	61.88
RNN	2	60.39
	3	61.47

**4. CONCLUSION**

The IDS model is proposed in this research work using federated learning for wireless sensor networks. Three IDS models have been designed at three levels. One is at the sensor side, the second is at the client base, and the last is at the global aggregation server side. Three IDS aims to detect different types of attacks using a federated learning model. It is observed that the hybrid IDS model using federated learning gives a high detection ratio above 92 %—and a low false positive rate. Further, IDS can achieve a very low false positive rate by changing the parameters in the federated learning model.

**REFERENCES**




[1] Y. Maleh and A. Ezzati, “A review of security attacks and intrusion detection schemes in wireless sensor network,” *International Journal of Wireless & Mobile Networks*, vol. 5, no. 6, pp. 79–90, 2013, doi: 10.5121/ijwmn.2013.5606.

[2] H. Sedjelmaci and S. M. Senouci, “A lightweight hybrid security framework for wireless sensor networks,” *2014 IEEE International Conference on Communications (ICC)*, Sydney, Australia, 2014, pp. 3636-3641, doi: 10.1109/ICC.2014.6883886.




[3] Z. Yang, N. Meratnia, and P. Havinga, “An online outlier detection technique for wireless sensor networks using unsupervised quarter-sphere support vector machine,” in *2008 International Conference on Intelligent Sensors, Sensor Networks and Information*

- Processing*, 2008, pp. 151–156, doi: 10.1109/ISSNIP.2008.4761978.
- [4] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, “Quarter sphere based distributed anomaly detection in wireless sensor networks,” *2007 IEEE International Conference on Communications*, Glasgow, UK, 2007, pp. 3864–3869, doi: 10.1109/ICC.2007.637..
  - [5] N. Shahid, I. H. Naqvi, and S. B. Qaisar, “Quarter-sphere SVM: Attribute and spatio-temporal correlations based outlier & event detection in wireless sensor networks,” *IEEE Wireless Communications and Networking Conference, WCNC*, pp. 2048–2053, 2012, doi: 10.1109/WCNC.2012.6214127.
  - [6] Y. Zhang, N. A. S. Hamm, N. Meratnia, A. Stein, M. V. D. Voort, and P. J. M. Havinga, “Statistics-based outlier detection for wireless sensor networks,” *International Journal of Geographical Information Science*, vol. 26, no. 8, pp. 1373–1392, 2012, doi: 10.1080/13658816.2012.654493.
  - [7] M. A. Rassam, A. Zainal, and M. A. Maarof, “One-class principal component classifier for anomaly detection in wireless sensor network,” in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 2012, pp. 271–276, doi: 10.1109/CASoN.2012.6412414.
  - [8] J. Weng, Y. Zhang, and W. S. Hwang, “Candid covariance-free incremental principal component analysis,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 8, pp. 1034–1040, 2003, doi: 10.1109/TPAMI.2003.1217609.
  - [9] M. A. Rassam, A. Zainal, and M. A. Maarof, “An efficient distributed anomaly detection model for wireless sensor networks,” *AASRI Procedia*, vol. 5, pp. 9–14, 2013, doi: 10.1016/j.aasri.2013.10.052.
  - [10] Y. Liu, “QPSO-optimized RBF neural network for network anomaly detection,” *Journal of Information and Computational Science*, vol. 8, no. 9, pp. 1479–1485, 2011.
  - [11] Y. Peng, Y. Wang, Y. Niu, and Q. Hu, “Application study on intrusion detection system using IRBF,” *Journal of Software*, vol. 9, no. 1, pp. 177–183, 2014, doi: 10.4304/jsw.9.1.177-183.
  - [12] P. Yichun, N. Yi, and H. Qiwei, “Research on intrusion detection system based on IRBF,” in *2012 Eighth International Conference on Computational Intelligence and Security*, 2012, pp. 544–548, doi: 10.1109/CIS.2012.128.
  - [13] S. Devaraju and S. Ramakrishnan, “Performance analysis of intrusion detection system using various neural network classifiers,” in *International Conference on Recent Trends in Information Technology, ICRTIT 2011*, 2011, pp. 1033–1038, doi: 10.1109/ICRTIT.2011.5972289.
  - [14] M. Riecker, S. Biedermann, R. El Bansarkhani, and M. Hollick, “Lightweight energy consumption-based intrusion detection system for wireless sensor networks,” *International Journal of Information Security*, vol. 14, no. 2, pp. 155–167, 2015, doi: 10.1007/s10207-014-0241-1.
  - [15] U. Halici, “Radial basis function network,” in *Artificial Neural Networks*, Ankara, Turkey: METU Electrical and Electronics Engineering, 2005, pp. 139–147.
  - [16] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, “Shallow and deep networks intrusion detection system: a taxonomy and survey,” *arXiv-Computer Science*, pp. 1–43, 2017.
  - [17] F. Tang, B. Mao, Z. M. Fadlullah, and N. Kato, “On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 80–86, Sep. 2018, doi: 10.1109/MCOM.2018.1701227.
  - [18] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, “A survey on federated learning,” *Knowledge-Based Systems*, vol. 216, pp. 1–11, 2021, doi: 10.1016/j.knosys.2021.106775.
  - [19] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, “Federated-learning-based anomaly detection for IoT security attacks,” *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2022, doi: 10.1109/JIOT.2021.3077803.
  - [20] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, “A survey of deep learning-based network anomaly detection,” *Cluster Computing*, vol. 22, pp. 949–961, 2019, doi: 10.1007/s10586-017-1117-8.
  - [21] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues,” *Knowledge-Based Systems*, vol. 189, 2020, doi: 10.1016/j.knosys.2019.105124.
  - [22] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, “Federated wireless network intrusion detection,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 6004–6006, doi: 10.1109/BigData47090.2019.9005507.
  - [23] N. Bouacida and P. Mohapatra, “Vulnerabilities in federated learning,” *IEEE Access*, vol. 9, pp. 63229–63249, 2021, doi: 10.1109/ACCESS.2021.3075203.
  - [24] A. Thakkar and R. Lohiya, “A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges,” *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021, doi: 10.1007/s11831-020-09496-0.
  - [25] A. I. Sunny, A. Zhao, L. Li, and S. K. Sakiliba, “Low-cost IoT-based sensor system: A case study on harsh environmental monitoring,” *Sensors*, vol. 21, no. 1, pp. 1–12, 2021, doi: 10.3390/s21010214.
  - [26] N. A. A. Al-Marri, B. S. Ciftler, and M. M. Abdallah, “Federated mimic learning for privacy preserving intrusion detection,” in *2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2020, pp. 1–6, doi: 10.1109/BlackSeaCom48709.2020.9234959.
  - [27] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning,” *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.
  - [28] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017*, vol. 54, pp. 1–10, 2017.
  - [29] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, “DfIoT: a federated self-learning anomaly detection system for IoT,” in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 756–767, doi: 10.1109/ICDCS.2019.00080.
  - [30] R. Samrin and D. Vasumathi, “Review on anomaly based network intrusion detection system,” in *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, 2017, pp. 141–147, doi: 10.1109/ICEECCOT.2017.8284655.
  - [31] P. V. Theerthagiri and M. Thangavelu, “Elephant intrusion warning system using IoT and 6LoWPAN,” *International Journal of Sensors, Wireless Communications and Control*, vol. 10, no. 4, pp. 605–616, 2019, doi: 10.2174/2210327909666191129092006.




**BIOGRAPHIES OF AUTHORS**

**Sathishkumar Mani**    has obtained his B.E. degree in Computer Science and Engineering from Bharathiar University, Coimbatore, India and M.Tech. degree in Information Technology from Punjabi University, Patiala, India. He earned his Ph.D. in Computer Science and Engineering from Saveetha University, Chennai, India. He has over 25 years of experience in multiple domains like teaching, research and software development. His research area is network security, machine learning, and IoT. He can be contacted at email: sathishkumarmani17@gmail.com.






**Parasuram Chandrasekaran Kishoreraja**    is a Professor at the School of Information Technology in Vellore Institute of Technology (VIT), Vellore, India. He has a total experience of 23 years in academic and research. He has published and presented various papers in the international journal and conferences. His research interests include security systems, internet of things, and medical artificial intelligence. He can be contacted at email: kishoreraja.pc@vit.ac.in






**Christeena Joseph**    is an Associate Professor working in the Department of ECE at SRM Institute of Science and Technology, Ramapuram, Chennai, India. She has teaching experience of 17 years and has published 50 research papers in national and international journals. Her research interests include wireless communication and networks. She can be contacted at email: christeena003@gmail.com.



**Reji Manoharan**    is an Associate Professor in the Department of Electronics and Communication Engineering at Rohini College of Engineering and Technology Kanyakumari India. He has a total experience of 15 years in academic and research. He has published and presented various papers in the international journal and conferences. His research interests include network security, internet of things, antenna design, and intrusion detection. He can be contacted at email: rejiceped@gmail.com.



**Prasannavenkatesan Theerthagiri**    is working as the Assistant Professor in the Department of Computer Science and Engineering, GITAM Deemed to be University, Bengaluru, India. He was awarded Ph.D. (Full-Time) degree in the year 2021 on the work of wireless communication with machine learning from Anna University, Chennai, India. He was awarded the mobility grant award by the Republic of Slovenia in the year 2017-2018. He has published his research works in 12 SCI indexed journals, 16 SCOPUS indexed journals. His research interests are data science, AI, IoT, and MANET. He can be contacted at email: prasannait91@gmail.com.