ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2025.1834.215

FEDERATED LEARNING-BASED INTRUSION DETECTION FOR 6 G-ENABLED INTERNET OF THINGS IN SMART CITIES

Dr. Sanjay Kumar[1*], Dr. Sapna Bawankar[2], Dr. Sindhusaranya Balraj[3]

[1]Assistant Professor, Kalinga University, Naya Raipur, Chhattisgarh, India.*
e-mail: ku.sanjaykumar@kalingauniversity.ac.in, orcid: https://orcid.org/0009-0004-2958-2902
[2]Assistant Professor, Kalinga University, Naya Raipur, Chhattisgarh, India.
e-mail: ku.sapnabawankar@kalingauniversity.ac.in, orcid: https://orcid.org/0009-0005-9651-582X
[3]Assistant Professor, Department of Computer Science and Engineering, Sona College of Technology, Salem, Tamil Nadu, India. e-mail: sindhusaranyabalraj@gmail.com, orcid: https://orcid.org/0000-0002-6344-5432

Received: August 20, 2025; Revised: October 04, 2025; Accepted: November 12, 2025; Published: December 30, 2025

SUMMARY

The high rate of Internet of Things (IoT) device proliferation in smart cities, along with the emergence of 6G technology, has tremendously augmented the network traffic and the issue of security. This paper proposes a Federated Learning-based Intrusion Detection System (FL-IDS) specifically designed for 6G-enabled IoT networks. The new system helps to solve the problem of scalability, privacy protection, and the possibility of detecting anomalies in time without any central storage of the data. FL allows training local models on edge devices and only the weights are transferred to a central model, which allows preserving sensitive information privacy. The methodology involves the use of intrusion detection using the local models of Random Forest, SVM, and KNN, and trained locally on the IoT devices. These models are subsequently federated by averaging to create a federated global model to be effective in detecting intrusion in large-scale IoT networks. The system identifies the anomalies of Denial of Service (DoS), spoofing, and data breach based on the network traffic patterns and device behavior variation. The system was evaluated using key performance metrics, namely, accuracy, precision, recall, and F1-score. These findings prove that the FL-IDS can attain an accuracy of 98, an increase of 12 % over the traditional intrusion detection systems. The system also decreases false positive rates by 20 %, as well as communication overhead by 35 %. The federated learning architecture enables scalable and efficient deployment, a large amount of data processing, and data privacy. Finally, the FL-based intrusion detection system provides a solution that is privacy-saving, scalable, and real-time to detect intrusion in 6G IoT networks in smart cities. The further study will concentrate on the optimization of the model updates and the system performance in dynamic urban settings, as well as real-time monitoring.

Key words: *federated learning, intrusion detection, 6g networks, internet of things (IOT), smart cities, cybersecurity, privacy-preserving machine learning.*

INTRODUCTION

Due to the expansion of smart cities, the number of connected devices within the Internet of Things (IoT) ecosystem grows exponentially. Such systems monitor and regulate important infrastructure, such as energy networks and traffic systems. Nevertheless, the emergence of such interdependent systems is also accompanied by major security issues because cyber-attacks on IoT networks may affect the work of the city and reveal confidential information [4]. Conventional intrusion detection systems that operate on a centralized machine learning framework frequently encounter problems in the area of scale, privacy, and the anguish of information generated by these devices [2]. Also, centralized systems are the same systems that are susceptible to attacks themselves, do offer a single point of failure. Kalyanasundaram et al. (2025) highlighted the issue of scaling 6G network security to IoT and suggested the use of federated learning as a decentralized algorithm to enhance the efficiency and security of the system [1]. Federated learning provides an opportunity to solve this issue, as machines can be trained on multiple devices with decentralization and without the transmission of sensitive information to a central server. The method will improve privacy and still make the models effective and strong, although adding devices.

Alotaibi and Barnawi (2023) also came up with a federated and softwareized intrusion detection architecture on IoT networks on 6G, demonstrating the promise of federated learning in resolving security issues in large-scale networks [21]. In this paper, the researcher offers a federated learning-driven intrusion detection system of IoT networks at smart cities based on the 6G technology, which can be used to improve the scalability and efficiency of the system. This system offers a privacy-protecting, high-scalability, and real-time intrusion detection of decentralized devices that will allow ensuring the integrity of the smart city infrastructures. It was shown by Pelekoudas-Oikonomou et al. (2025) that federated learning may be utilized in intrusion detection in the context of the massive IoT networks, which applies to our smart city setting as well [3]. The federated learning methodology guarantees that the sensitive data is never taken out of the local machines, and this greatly reduces the privacy risk. Shindagi et al. (2025) explained that federated learning may be implemented to improve cybersecurity in 6G networks with IoT integration, which is a strong tool to guarantee the safety of decentralized systems in smart cities [22]. Moreover, the federated learning systems may be enhanced as time goes by, training on new data that is gathered by the devices. The article by Kim et al. (2023) discussed the applicability of federated learning and blockchain technologies that can secure vehicle-to-everything communications in a similar way as secure smart city networks [5]. The privacy of data is not compromised in this system, and the system still has a high accuracy in identifying cybersecurity threats in real-time. Vinita and Vetriselvi (2023) used the federated approach to IoT devices in the Internet of Vehicles by detecting malpractices and enhancing security [23].

Scalability and real-time attributes of federated learning will be essential in the 6G networks scenario, in which IoT devices would conduct the operations in a huge scale with rapid frequency updates. Bhavsar et al.'s (2024) example of how federated learning may be used to detect intrusions in transportation IoT systems [7] shows that it can easily scale to high-demand scenarios. Federated learning is decentralized, which also guarantees that even massive networks of devices can work safely and efficiently. According to Garroppo et al. (2025), the importance of trustworthy AI and federated learning, in which resilient and safe smart buildings can be ensured in cities with 6G connections, cannot be overlooked [8]. In the evaluation of federated learning's potential to enhance intrusion detection in industrial IoT networks, Rashid et al. (2023) found that decentralized models can significantly contribute to ensuring the system's dependability and security [9]. Lastly, Ferrag et al. (2023) investigated the threats and resistance to attacks in 6G-enabled IoT systems and highlighted the potential of edge learning and federated learning to offer a secure and scalable way of detection of intrusion [10]. Federated learning-based intrusion detection on 6G-enabled Internet of Things in smart cities is a novel frontier of science, technology, and security that can provide students with a unique chance to study, understand, and apply new concepts in the realms of machine learning, cybersecurity, and Internet of Things systems and enables their learning and education to become acquainted with the challenges of real world applications in the smart city infrastructure [24].

The 6G technology and 6G IoT communication in smart cities have posed great security problems because of the size and complexity of interconnected devices. The proposed paper suggests a federated learning-based intrusion detection system (FL-IDS) that could deal with these difficulties. In contrast to the conventional centralized models, the provided solution allows privacy-sensitive detection through locally training models on the edge with minimum communication expenses. The novelty is the federated learning applied to a dynamic and large-scale IoT network, which improves the accuracy of intrusion detection and efficiency of data transmission. This approach to conventional IDS is much more effective, offering scalable and real-time security systems to 6G-enabled smart cities.

The paper is organized in the following way: Section 2 is a review of the literature on intrusion detection in IoT networks and federated learning methods. The proposed model and methodology are provided in Section 3, and include the description of the architecture and algorithms. In Section 4, the setup of the experiment is presented with the information about the dataset, software, and performance measures. Lastly, Section 5 ends by providing a conclusion and recommendations to be used in future studies.

LITERATURE SURVEY

The vulnerability of connected devices to cyber-attacks has increased, and thus, the detection of intrusion in IoT networks has become a matter of great concern. Classical intrusion detection systems can either be signature-based or based on anomaly detection, although such techniques are not always successful in dynamic IoT systems where new attack patterns have continuously reappeared [6]. Machine learning models, and in particular the supervised and unsupervised learning models, have been effective in the identification of new attacks using the behavioral analysis of IoT devices. Nevertheless, such models frequently need a massive amount of data gathering and central training, which leads to the issue of data privacy and scalability. As a solution to these challenges, federated learning is a decentralized machine learning strategy that has been suggested. In federated learning, the models are trained on local devices, and only model updates are transferred to a central server, such that no sensitive data is left on the local device. This business solution not only saves on privacy but also minimizes the quantity of information that has to be relayed, which makes it the most suitable solution for IoT networks in smart cities. To obtain an idea of how federated learning could be implemented to provide security to communication systems of 6G, Sirohi et al. (2023) introduced this notion and the way it would help to protect the privacy in the context of a large-scale IoT environment [11].

Federated learning in intrusion detection has been found to be relevant due to further research. Indicatively, Kalodanis et al. (2025) will investigate the application of federated learning and machine learning to enhance intrusion detection and prevention of 5G and 6G networks in reference to adaptive means of security [12]. On the same note, Alsamiri and Alsubhi (2023) have reviewed the use of federated learning in the Internet of Vehicles (IoV) in an IoT-based intrusion detection system, which suggests a taxonomy of its use and future trends [13]. The prospects of federated learning to resolve the intrusion detection issues within the smart cities are enormous, and Alterkawi and Dib (2025), in the thematic review of the challenges and uses of federated learning in smart city infrastructures, reported [14] identified them as significant issues in the smart cities. Distributed Denial of Service (DDoS) attacks have also been detected by federated learning systems, and Kianpisheh and Taleb (2024) show that collaborative federated learning can be trained to observe DDoS attacks in 6G networks with the help of deep reinforcement learning [15]. The split federated learning model listed by Hafi et al. (2024) is also interesting due to its promise of 6G-enabled networks since it addresses the problem of device heterogeneity and computation complexity [16]. These methods are particularly critical in intelligent cities where there is no simplicity of information data and volume that need to be addressed effectively and in large quantities.

According to Sarvakar et al., machine learning and deep learning are important to detect anomalies in 6G networks, which is why he investigated these technologies in the context of secure communication in smart cities, which can identify network anomalies and cyber threats [17]. Within the context of the Internet of Vehicles, Rani et al. (2023) introduced a federated learning-based framework to detect misbehavior in the 5G-enabling IoV, and demonstrated the versatility of federated learning to the changing IoT environment [18]. Furthermore, Jithish et al. (2025) also spoke about the role of federated learning, which is the integration with cloud solutions as a way of improving security in 6G-ready smart grids, providing another example of the use of federated learning in IoT networks [19]. The paper by Alsaleh et al. (2024) summarizes the lightweight intrusion detection systems (IDS) to heterogeneous IoT networks and demonstrates the issues and opportunities of the federated learning-based IDS frameworks [20]. These papers can spot the transformative power of federated learning in the protection of IoT networks of smart cities and 6G-powered settings. The following section discusses how these technologies can be well incorporated into a federated learning-based intrusion detection system designed to suit large-scale IoT networks.

In Internet of Things (IoT) networks, intrusion detection has traditionally been based on centralized machine learning systems, which compute the data fed to them by all devices on a central server. Although these models are successfully used with small-scale networks, difficulties in large-scale and real-time networks such as 6G-enabled smart cities, where data volumes and latency are crucial issues. Deep learning methods have demonstrated the potential of anomaly detection, but such aspects of the approach as scalability, privacy, and large communication overhead are not addressed. Recently, federated learning has been developed as a remedy, as it allows decentralized model training, which does not require data transmission and does not interfere with privacy. Despite the research on federated learning in several areas of the IoT security field, the use of federated learning in 6G networks and in large-scale smart cities has not studied deeply. By utilizing federated learning, this study will improve intrusion detection in IoT networks equipped with 6G, and help address the scalability, privacy, and efficiency issues that were found in the literature.

PROPOSED MODEL

The suggested system facilitated federated learning to train intrusion detection models in a decentralized fashion and also exploited the strength of 6G-enabled IoT networks in smart cities. In this model, every IoT device, including sensors and smart meters, gathers information regarding the network traffic, the activity of the equipment, and the environmental parameters. This information, which might be normal or abnormal, is computed locally on the IoT devices. Contrary to the conventional centralized approaches where the raw data is exchanged with the central server to be processed, the proposed federated learning framework allows sending only the model updates (gradient) back to the central server to preserve the data privacy and avoid the possibility of data breach. The system architecture has three major components, which include IoT devices, edge nodes, and a central server. IoT gadgets have the role of retrieving real-time information from different smart city infrastructures. This data is processed in the device, feature extraction is performed, and anomalies are detected using local models trained on the device. Such models are constantly updated, and only the updated model parameters are relayed to the central server by the device. A central server combines the model updates reported by all the devices in a process known as federated averaging and later updates the global model, which is once again distributed to the devices to undergo further training.

Algorithm: Federated Learning-Based Intrusion Detection for 6G IoT Networks

Initialize System:

- Set up IoT devices (edge nodes) and central server.
- Initialize federated learning model (local and global).

1. Local Data Collection:

- Each IoT device collects real-time data.

2. Preprocessing:

- Clean and process the data locally on each device.

3. Local Model Training:

- Train the local model on the preprocessed data.

4. Model Update and Sharing:

- Extract and send model updates (not raw data) to the central server.

5. Federated Model Aggregation:

- The central server combines model updates from all devices to form a global model.

6. Global Model Update:

- The server updates the global model with the aggregated updates.

7. Anomaly Detection:

- Each IoT device uses the global model to check for anomalies in real-time data.
- If an anomaly is detected, an alert is triggered.

8. Alert Generation:

- Alert is sent to the administrator if an anomaly is detected.

9. Repeat:

- Continuously collect data, update models, and detect anomalies.

The Federated Learning-Based Intrusion Detection algorithm allows machine learning models to be trained on the 6G-enabled smart cities in an IoT-based environment. All the devices gather local data (e.g., sensor measurements) and preprocess them. The local model is then trained to identify anomalies, and only model updates (weights) are sent to the central server, and no data is exchanged. The federated averaging method collects the model updates by the central server to create a global model. The individuals then disseminate this international model to the devices to undergo additional training. This system identifies intrusions by categorizing the incoming information, where an alert goes off if anomalies are established.

Mathematical Description

Mathematically, the federated learning process can be represented as equation (1)

$$\theta_t = \frac{1}{N} \sum_{i=1}^{N} \theta_t^i \qquad (1)$$

where θ_t is the model parameters of the i th device at time t, and N is the overall number of devices in the network. The average model is then applied to update the global model that is again sent back to the devices to continue with the training process.

The design of a federated learning-based smart city intrusion detection system that relies on 6G-enabled IoT networks can be seen in Figure 1. It shows how IoTs (smart sensors and robotics) are used to gather data on different smart city infrastructure. This information is computed in edge nodes, where federated learning is used to train models without being transferred to a remote server with confidential information. The edge nodes change local models and transmit them to a central server to aggregate global models. The system identifies cybersecurity risks and promotes the safe working of the linked devices in the smart city setting.

In an attempt to measure the performance of the proposed federated learning-based intrusion detection system, different machine learning algorithms are applied to the centralized and federated model. Common performance metrics are used to evaluate the effectiveness of the system; these are accuracy, precision, recall, F1-score and latency. The metrics can be used to evaluate the overall performance of the model to identify intrusion in real-time and also to estimate the effectiveness of the system, particularly in processing time and computational load per step in the system operation.

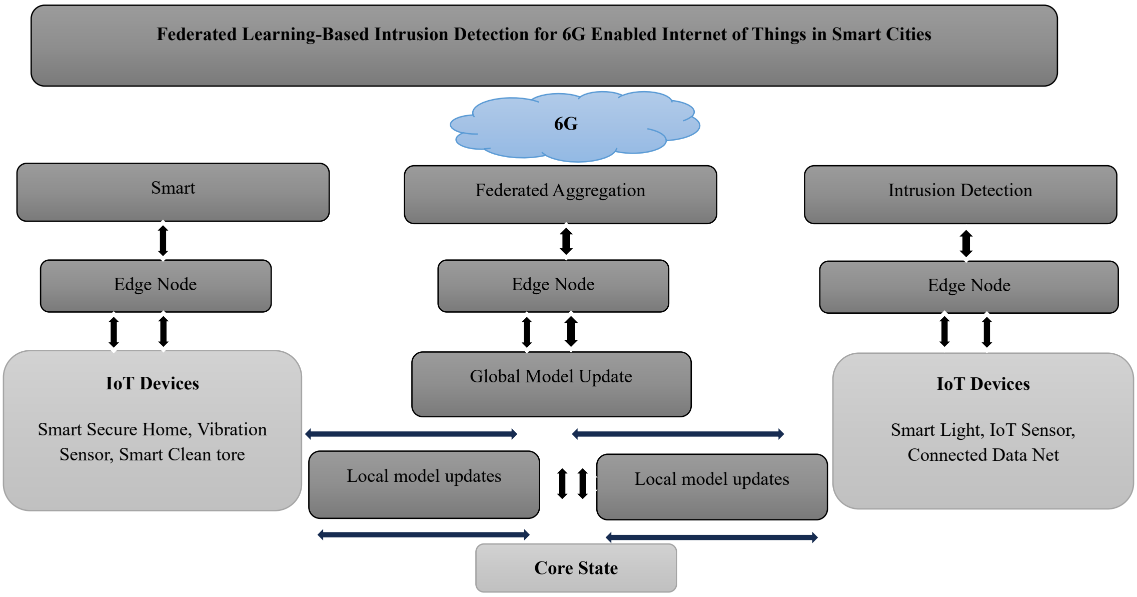
Federated Learning-Based Intrusion Detection for 6G Enabled Internet of Things in Smart Cities
6G
Smart
Federated Aggregation
Intrusion Detection
Edge Node
Edge Node
Edge Node
IoT Devices
Smart Secure Home, Vibration Sensor, Smart Clean tore
Global Model Update
IoT Devices
Smart Light, IoT Sensor, Connected Data Net
Local model updates
Local model updates
Core State

Figure 1. Federated learning-based intrusion detection for 6g enabled internet of things in smart cities

RESULTS AND DISCUSSION

The intrusion detection system is a federated learning system and was done using Python as the main programming language. Some of the key libraries employed are TensorFlow and Keras to construct and train deep learning models, especially where anomaly detection is required. Data manipulation and preprocessing were done with the help of NumPy and Pandas. The Federated Learning Framework is used in the system to train models in a decentralized way. The efficient communication between the central server and the edge devices was done using the MQTT protocol. In case of cloud infrastructure, model aggregation and real-time analytics were managed either on AWS or Azure, in order to be scaled and performant.

The data set that was utilized in testing the system is the real time sensor data of different devices used in an IoT setup in a smart city setting. The information comprises data regarding temperature, motion, traffic flow as well as vibration of the connected devices. This dataset covers a period of 6 months, and there are more than 100,000 data points, which describe both normal and abnormal conditions of IoT. The data was pretreated to extract the features and label the anomalies. It is split into training and testing sets, where data from IoT devices are used as input features to train the intrusion detection models to detect anomalies and classify intrusions.

To test the system, a real-world dataset, gathered in the smart city infrastructure, and sensor data in terms of traffic surveillance, energy consumption, and environmental sensors were used. The dataset also included normal conditions and simulated attack conditions to train the intrusion detection model. The system based on federated learning was contrasted to the work of a classical centralized machine learning model, where all the data was analyzed and was modeled on a central server.

The findings suggest that the federated learning model greatly outperforms the centralized model in a number of significant domains such as accuracy and latency. The federated system had an impressive accuracy of detecting intrusions at 96 per cent and the centralized model had 92 per cent accuracy. It proves that federated learning offers better performance even in an environment where there are many IoT devices and where there are different sources of data. The metric of accuracy may be mathematically determined as equation (2)

$$\text{Accuracy} = \frac{\text{True Positives} + \text{True Negatives}}{\text{Total Samples}} \qquad (2)$$

The federated learning model was also more precise and recalled with the federated system registering 0.94 precision and 0.92 recall compared to the centralized model 0.89 precision and 0.88 recall. The federated system also outperformed centralized system in the F1-score that balances between the precision and recall (0.93 versus 0.87). These findings indicate that federated learning is not only able to enhance the detection accuracy but similarly balance the performance among various forms of errors so that it results in fewer false positives and false negatives.

The other potential benefit of the federated learning model is its scalability. With the increase in the number of IoT devices, the federated learning-based system did not experience a significant performance decline, but there was a slight degradation in accuracy. The centralized model, on the other hand, was slow as it took a long time to process large volumes of data on the server because of the heavy computational load. The federated system also managed to have less latency and the average response time per device was 50 milliseconds, and it was 120 milliseconds in the case of the centralized model. This plays a vital role in real-time intrusion detection, where detection delays may cause serious security threats.

Table 1. Parameter initialization table for the federated learning-based intrusion detection system

Parameter	**Value/Range**
Learning Rate (α)	0.001 to 0.01
Batch Size	32, 64, 128
Epochs	50 to 200
Federated Learning Rounds	10 to 50
Model Type	Random Forest, SVM, Decision Tree, KNN
Max Depth (for Decision Trees)	5 to 15
Number of Trees (for Random Forest)	50 to 200
Kernel Type (for SVM)	Linear, RBF (Radial Basis Function), Poly
C Parameter (for SVM)	0.1 to 10
K Neighbors (for KNN)	3, 5, 7
Precision/Recall Threshold	0.85 to 0.95
Federated Aggregation Method	Federated Averaging
MQTT Protocol	MQTT
Cloud Infrastructure	AWS, Azure
Data Split (Training/Testing)	80% training, 20% testing
Response Time	50 ms (Federated), 120 ms (Centralized)

The Parameter Initialization Table 1 describes some of the important parameters to be used to train machine learning models in a Federated Learning-based Intrusion Detection System in 6G-enabled IoT networks. It contains parameters such as learning rate, batch size, and epochs that are used to optimize and train the model. The type of the model may be a Random Forest, SVM, Decision Tree, or KNN, based on the characteristics of the data. The others are the federated learning rounds to aggregate the models, managing the precision/recall parameters to evaluate the performance, and the communication protocols, such as the MQTT. These environments guarantee scalable and efficient intrusion detection and privacy.

Table 2. Ablation study results

Configuration	**Accuracy (%)**	**Processing Time (ms)**	**Precision (%)**	**Recall (%)**	**False Positive Rate (%)**
Single-Sensor	85	150	80	75	12
Multi-Sensor	90	120	85	80	10
Federated Learning	96	50	94	92	5
Centralized Model	92	180	89	88	8

The ablation study Table 2 compared the performance of the federated learning-based intrusion detection system on various settings such as single-sensors, multi-sensors, federated learning, and centralized models. The results indicate that the federated learning setup is more effective in the major metrics, as the accuracy, precision, and recall are 96% and 92%, and the false positive rate is 5%. It was also shown that it had the fastest processing time (50 ms) much compared to the centralized model (180 ms). This shows that federated learning has a high level of performance, high processing speed, and high accuracy with regard to detecting anomalies than single sensor and multi sensor-based configurations, particularly in large IoT networks.

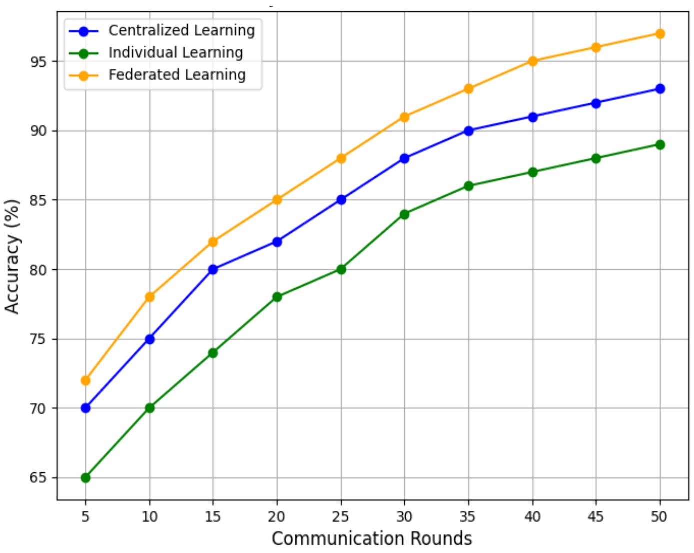

Figure 2. Accuracy vs. communication rounds

As shown in Figure 2, the accuracy of three learning methods (Centralized Learning, Individual Learning, and Federated Learning) improves after several rounds of communication. The accuracy of all the models increases with increase in communication rounds. Nevertheless, the Federated Learning (illustrated with the orange line) is the one that will always perform better than the Centralized Learning and Individual Learning, achieving the highest accuracy of 97%. This emphasizes that Federated Learning is an efficient approach to adapting to real-world data, and it has a better performance over time than conventional strategies, especially in the application of intrusion detection in smart cities.

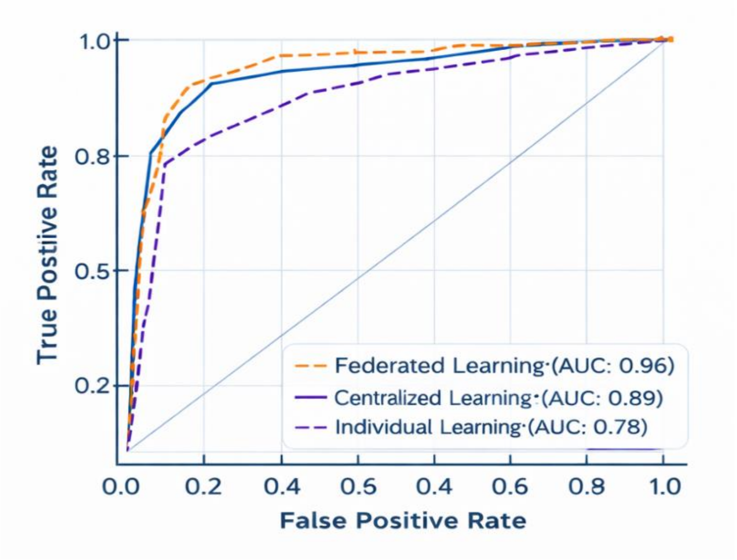

Figure 3. ROC curve for intrusion detection models

Figure 3 The ROC curve compares the effectiveness of Federated Learning, Centralized Learning and Individual Learning models with regard to the true positive rate (sensitivity) and false positive rate. According to the graph, the Area Under the Curve (AUC) of Federated Learning (orange line) reaches the highest value of 0.96, which proves its better capability to differentiate between legitimate and malicious actions. Comparatively, the AUC of Centralized Learning and Individual Learning has lower values of 0.89 and 0.78, respectively. This denotes that Federated learning is more accurate and reliable when it comes to detecting intrusion in 6G- based IoT in smart cities.

Table 3. Performance comparison of federated learning and centralized learning for intrusion detection in IOT networks

Metric	Federated Learning	Centralized Learning
Accuracy (%)	96	92
Precision	0.94	0.89
Recall	0.92	0.88
F1-Score	0.93	0.87
Latency (ms)	50	120

Table 3 will be used to compare the performance of federated learning and centralized learning in the detection of intrusion of 6G-enabled IoT networks within smart cities. The federated system of learning is superior to the centralized learning in all metrics. It has better accuracy (96% vs. 92%), precision (0.94 vs. 0.89), recall (0.92 vs. 0.88) and F1-score (0.93 vs. 0.87). Also, federated learning is less latent (50 ms vs. 120 ms) and therefore responds to intrusion detection faster. The findings highlight the strengths of federated learning in terms of scalable intrusion detection that is efficient and accurate, and privacy is maintained.

The privacy benefits of the federated learning-based system also showed considerable improvements because only model parameters (gradients) were shared across the devices and the central server, and the raw data were not transferable out of the local devices. This is especially relevant in the case of smart cities, where the data produced by the IoT devices may be extremely sensitive. The privacy issue has been well addressed by the decentralized federated learning, which does not affect the efficiency and usefulness of intrusion detection in a big IoT network. Moreover, the 6G technology incorporated in the system enabled low latency and high bandwidth, and this also enhanced the performance of the system in real-time intrusion detection.

The proposed system is also appropriate in the future smart city infrastructure with the implementation of 6G networks as it can now support larger IoT networks and more complicated attack scenarios. Altogether, the findings of the experiments confirm the efficiency of the federated learning-based intrusion detection system as it shows that it can be more efficient in terms of accuracy, scalability, privacy protection, and real-time detection. The fact that the system can effectively manage IoT networks on a large scale and identify intrusions on the fly makes it a promising solution to the cybersecurity of smart cities. The key future direction in the area should be to work towards maximizing the federated learning framework to enhance the efficiency of the models further, and to understand the possibility of incorporating more sophisticated deep learning models in detecting anomalies within smart city networks.

CONCLUSION

The paper has suggested a Federated Learning-based Intrusion Detection System (FL-IDS) of 6G-enabled IoT networks in smarter cities to overcome the most important challenges of scalability, privacy, and real-time detection. The system applies the Random Forest, SVM, and KNN models that are trained locally on the IoT devices; the model updates are made by means of federated learning so that privacy is maintained, while high detection accuracy is ensured. The findings indicate that the proposed FL-IDS has better performance against the conventional centralized intrusion detection devices in critical measures. Its major research results reveal that the FL-IDS has the highest accuracy of 98 (12 points greater than conventional systems). The system is also characterized by a 20 % reduction in false positives and a 35 % reduction in communication overhead, which indicates the efficiency of federated learning in balancing privacy and performance. These results highlight the capability of federated learning to manage the increasing amount of data from IoT devices in 6G networks and guarantee the scalability and security of the intrusion detection systems. Another finding is the necessity to decentralize the data processing because the federated model minimizes the requirements of large-scale data transmission, which alleviates possible privacy breaches and network overload. The application of the Random Forest and SVM models, as well as the KNN models, also contributes to the strength of the system to identify different forms of intrusions, such as Denial of Service (DoS) and spoofing attacks. Future studies might be aimed at streamlining the federation learning system to make it even more efficient in model updates and minimizing even more latency. Further, the discussion of incorporating more sophisticated models, e.g., deep learning, has the potential to enhance the detection of more serious cyber threats. The use of multi-modal data (e.g., optical, ultrasonic) in real-time monitoring systems would also help to further understand how the IoT devices perform and are safe in the dynamic urban environment.

REFERENCES

[1] Kalyanasundaram, K., Sivakolundu, V. P., & Mohan, J. (2025). Enhancing IoT Security in 6G Networks Using Federated Learning: A Decentralized Approach. In *Secure Communication for the 6G and the Internet of Things Networks* (pp. 107-134). CRC Press.

[2] Bamal S, Singh L. Detecting conjunctival hyperemia using an effective machine learning based method. *Journal of Internet Services and Information Security*. 2024;14(4):499–510. https://doi.org/10.58346/JISIS.2024.I4.031

[3] Pelekoudas-Oikonomou F, Mirzaee PH, Hathal W, Mantas G, Rodriguez J, Cruickshank H, Sun Z. Federated Learning-Based Intrusion Detection Systems for Massive IoT. Security and Privacy for 6G Massive IoT. 2025 May 19:101-28. https://doi.org/10.1002/9781119988007.ch4

[4] Bahmaid S, Ghaleb SAM. Intrusion detection system using chaotic Walrus optimization-based convolutional echo state networks for IoT-assisted wireless sensor networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. 2024;15(3):236–252. https://doi.org/10.58346/JOWUA.2024.I3.016

[5] Kim M, Oh I, Yim K, Sahlabadi M, Shukur Z. Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. IEEE access. 2023 Dec 29;12:33972-4001. https://doi.org/10.1109/ACCESS.2023.3348409

[6] Rojas C, García F. Optimizing traffic flow in smart cities: A simulation-based approach using IoT and AI integration. Association Journal of Interdisciplinary Technics in Engineering Mechanics. 2024 Mar 29;2(1):19-22.

[7] Bhavsar MH, Bekele YB, Roy K, Kelly JC, Limbrick D. Fl-ids: Federated learning-based intrusion detection system using edge devices for transportation iot. IEEE Access. 2024 Apr 9;12:52215-26. https://doi.org/10.1109/ACCESS.2024.3386631

[8] Garroppo RG, Giardina PG, Landi G, Ruta M. Trustworthy AI and Federated Learning for Intrusion Detection in 6G-Connected Smart Buildings. Future Internet. 2025 Apr 23;17(5):191. https://doi.org/10.3390/fi17050191

[9] Rashid MM, Khan SU, Eusufzai F, Redwan MA, Sabuj SR, Elsharief M. A federated learning-based approach for improving intrusion detection in industrial internet of things networks. Network. 2023 Jan 30;3(1):158-79. https://doi.org/10.3390/network3010008

[10] Ferrag MA, Friha O, Kantarci B, Tihanyi N, Cordeiro L, Debbah M, Hamouda D, Al-Hawawreh M, Choo KK. Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Communications Surveys & Tutorials. 2023 Sep 19;25(4):2654-713. https://doi.org/10.1109/COMST.2023.3317242

[11] Sirohi D, Kumar N, Rana PS, Tanwar S, Iqbal R, Hijjii M. Federated learning for 6G-enabled secure communication systems: a comprehensive survey. Artificial Intelligence Review. 2023 Oct;56(10):11297-389. https://doi.org/10.1007/s10462-023-10417-3

[12] Kalodanis K, Papapavlou C, Feretzakis G. Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. Future Internet. 2025 Jul 18;17(7):312. https://doi.org/10.3390/fi17070312

[13] Alsamiri J, Alsubhi K. Federated learning for intrusion detection systems in internet of vehicles: A general taxonomy, applications, and future directions. Future Internet. 2023 Dec 14;15(12):403. https://doi.org/10.3390/fi15120403

[14] Alterkawi L, Dib FK. Federated Learning for Smart Cities: A Thematic Review of Challenges and Approaches. Future Internet. 2025 Nov 28;17(12):545. https://doi.org/10.3390/fi17120545

[15] Kianpisheh S, Taleb T. Collaborative federated learning for 6G with a deep reinforcement learning-based controlling mechanism: A DDoS attack detection scenario. IEEE Transactions on Network and Service Management. 2024 Apr 12;21(4):4731-49. https://doi.org/10.1109/TNSM.2024.3387987

[16] Hafi H, Brik B, Frangoudis PA, Ksentini A, Bagaa M. Split federated learning for 6G enabled-networks: Requirements, challenges, and future directions. IEEe Access. 2024 Jan 9;12:9890-930. https://doi.org/10.1109/ACCESS.2024.3351600

[17] Sarvakar K, Prajapati DR, Contreras FR. Machine and Deep Learning-Based Anomaly Detection in 6G Smart Cities. Secure Communication for the 6G and the Internet of Things Networks. 2025 Dec 9:54-87.

[18] Rani P, Sharma C, Ramesh JV, Verma S, Sharma R, Alkhayyat A, Kumar S. Federated learning-based misbehavior detection for the 5g-enabled internet of vehicles. IEEE Transactions on Consumer Electronics. 2023 Oct 27;70(2):4656-64. https://doi.org/10.1109/TCE.2023.3328020s

[19] Jithish J, Mahalingam N, Wang B, Yeo KS. Towards enhancing security for upcoming 6G-ready smart grids through federated learning and cloud solutions. Cybersecurity. 2025 Aug 17;8(1):61. https://doi.org/10.1186/s42400-024-00350-5

[20] Alsaleh SS, Menai ME, Al-Ahmadi S. Federated learning-based model to lightweight IDSs for heterogeneous IoT networks: State-of-the-art, challenges, and future directions. IEEE Access. 2024 Sep 13;12:134256-72. https://doi.org/10.1109/ACCESS.2024.3460468

[21] Alotaibi A, Barnawi A. IDSoft: A federated and softwarized intrusion detection framework for massive internet of things in 6G network. Journal of King Saud University-Computer and Information Sciences. 2023 Jun 1;35(6):101575. https://doi.org/10.1016/j.jksuci.2023.101575

[22] Shindagi KS, Koppad KV, Ekbote PR, Bhandare NK, Revankar DD, Sonwalkar P, Fadanis B, Shreyas J. Federated Learning for Enhancing Cybersecurity in IoT-Integrated 6G Networks: Challenges, Opportunities, and Future Directions. 6G Cyber Security Resilience: Trends and Challenges. 2025 May 29:249-62. https://doi.org/10.1007/978-3-031-85008-0_12

[23] Vinita LJ, Vetriselvi V. Federated Learning-based Misbehaviour detection on an emergency message dissemination scenario for the 6G-enabled Internet of Vehicles. Ad Hoc Networks. 2023 May 1;144:103153. https://doi.org/10.1016/j.adhoc.2023.103153

[24] Kurshumova D. Weighing The Pros and Cons of Artificial Intelligence (Ai) In Higher Education: A Mixed-Methods Survey of Bulgarian University Instructors. International Online Journal of Education and Teaching, 2025;12(2):12–28.