Developing Dilated Echo State Network with GELU Activation Function for Privacy-Preserving Federated Learning in 6G Networks

Mohammed Jameel Patel
College of Pharmacy, Nursing and Medical Sciences.
Riyadh Elm University
Riyadh, Kingdom of Saudi Arabia
Jameelpatel@riyadh.edu.sa

Abstract: Future 6G networks require intelligent, adaptable and privacy-friendly machine learning methods. Federated Learning helps keep customer data safe from threats, but it still faces challenges like high communication costs and limited model performance. In this study, we developed a new decentralized communication method for privacy-preserving federated learning, merged with a Dilated Echo state Network with GELU activation function (DESN-GAF) for performing intrusion detection in the network. Further, to enhance the security of the communication data, encryption is performed using Elliptic Curve Cryptography (ECC). Test results showed that our method increases accuracy and reliability, while maintaining data security and reducing the communication needs.

Keywords: 6G Communication Network; Federated Learning; Privacy-Preserving; Dilated Echo State Network with GELU Activation Function; Elliptic Curve Cryptography

Received: May 15, 2025 Revised: May 21, 2025 Accepted: May 25, 2025

Nomenclature

Abbreviation	Definition
6G	Sixth Generation Wireless Communication Network
AI	Artificial Intelligence
FL	Federated Learning
DESN-GAF	Dilated Echo State Network with GELU Activation Function
ESN	Echo State Network
GELU	Gaussian Error Linear Unit
ECC	Elliptic Curve Cryptography
IoE	Internet of Everything
IoT	Internet of Things
XR	Extended Reality
DDPG	Deep Deterministic Policy Gradient
DNN	Deep Neural Network
MUECD-SAP	Multi-UAV Energy Efficient Coverage Deployment algorithm using Spatial Adaptive Play
LSTM	Long Short-Term Memory
PSO	Particle Swarm Optimisation
GRU	Gated Recurrent Unit
MAE	Mean Absolute Error
RMSE	Root Mean Square Error
QoS	Quality of Service
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman Cryptosystem
DSA	Digital Signature Algorithm
DHA	Diffie–Hellman Algorithm
UAV	Unmanned Aerial Vehicle
SINR	Signal-to-Interference-plus-Noise Ratio
CSI	Channel State Information
RORA	Reinforcement learning based Optimal Resource Allocation
MARL	Multi-Agent Reinforcement Learning
ADPA	Attention-based Decentralized Policy Algorithm
IFDSDA	Information-Fusion based Decentralized Swarm Decision Algorithm

1. Introduction

With the rapid advancement of wireless communication, 6G networks promise ultra-fast speeds, extremely low latency, and massive connectivity [1]. These capabilities are expected to support a wide range of future smart applications. However, the immense volume of sensitive data

transmitted across 6G networks raises serious privacy and security concerns [2]. Traditional privacy-preserving methods may not be sufficient to handle the scale and complexity of these new systems [3]. Therefore, there is a critical need to develop advanced privacy-preservation frameworks tailored for 6G. Such frameworks must protect user data while maintaining the high efficiency and reliability that 6G demands [4]. Key features include proactive threat detection and adaptive encryption to secure data without adding delays. These solutions work together to safeguard sensitive information against emerging cyber threats [5]. Ensuring strong privacy protection in 6G networks is essential for building user trust and supporting secure communication services.

Traditional approaches to protecting privacy in wireless networks do not work well for 6G because they use fixed rules. These fixed rules are not flexible enough to handle the rapidly changing environment and new types of services that 6G offers [6]. This can cause user data to be unsafe, leading to privacy leaks and hackers getting in. Many current systems fail to monitor privacy all the time, so attacks can happen without anyone noticing [7]. This makes people trust the network less and makes 6G less reliable. Also, 6G has many different devices, which makes it harder to keep privacy strong everywhere. Because of this, we need smart and flexible systems to protect data and keep the network fast. Such systems should be able to adapt to new threats without slowing down communication [8].

To fix these problems, new smart methods using AI have been made that use deep learning to protect data better and keep the network working well [9]. For example, smart programs can change how data is encrypted and shared based on what users do and network conditions. This helps the system run faster and saves energy. At the same time, deep learning can find privacy problems and unauthorized access quickly [10]. Using these smart tools, 6G can stop privacy risks before they cause trouble. This way, privacy stays safe without slowing down the network.

Contribution: This section describes the contributions of the developed model:

- To develop a privacy-preserving learning model integrated with FL that boosts 6G networks using secure and smart data processing. The model uses a deep learning technique for preserving privacy-related data and training beyond distributed devices. This improves accurate predictions while also maintaining security and minimizing the communication overhead. It supports scalable, real-time applications while maintaining users' privacy in next-generation networks.
- To develop DESN-GAF, a recurrent architecture improved with dilated connections for effective intrusion detection in 6G networks. The dilations extend the input coverage, making a better capture of temporal dependencies with minimum variables. Merging with GELU activation boosts learning dynamics and stability. This supports precise, low-delay FL while also keeping the user data safe in the network.
- To ensure more security for the data, ECC is used for safeguarding communication in privacy-preserving FL. It gives strong encryption with smaller key sizes, minimising resource load on edge devices. It guarantees data security and integrity among distributed 6G networks. This makes ECC important for ensuring safe, low-delay learning in next-generation wireless communication systems.

Organization of the Manuscript: Section 2 presents the background study on privacy-preserving FL techniques; Section 3 provides the proposed framework and working of privacy-preserving FL in 6G networks; Section 4 discusses the results and analysis; and Section 5 summarizes the study, offering final insights and future directions.

2. Related Works

2.1 FL in wireless and 6G networks

FL in wireless and 6G networks allows for decentralized model training beyond edge devices, keeping private data safe without sharing the raw data. It incorporates low-delay 6G communications to manage learning effectively among distributed nodes and high speed. FL minimizes the use of bandwidth and improves data security by sharing only the model updates, not the complete datasets. This method helps intelligent, real-time applications in modern cities, automated systems and IoT networks.

Previously, a MUECD-SAP [11] was proposed, which used a modified PSO to optimise the accurate location of deployed UAVs based on a SINR to increase the data collection rate. Also, to make the FL run for multiple iterations [12], SAP dynamically allocates resources using DDPG to optimise the energy consumed and the link latency between the user and the UAV

system. The simulation outcomes demonstrated that MLCFL significantly enhanced the accuracy of mobility forecasting while lowering both energy usage and latency by enabling adaptable deployment strategies.

In conclusion, FL over 6G networks supports secure, efficient, and collaborative AI development at the edge. It paves the route for scalable, privacy-preserving solutions in next-generation wireless ecosystems.

2.2 Decentralized Communication Strategies

Decentralized communication strategies include sharing information directly between nodes without depending on a central server. These strategies improve network reliability, minimize single points of failure and increase scalability. They are specifically useful in peer-to-peer systems, ad hoc networks and in blockchain-based applications.

In existing works, a 2D-Ring network structure-based parameter synchronisation strategy and a 2D-attention-based device placement algorithm [13] were proposed and aimed to reduce communication overhead. ADPA [14] was designed to address the challenges in large-scale multi-agent environments. ADPA leveraged an attention mechanism to adaptively identify relevant data for evaluating critics during the training of decentralized policies. This enabled effective and scalable learning, supporting both cooperative and competitive settings, and scenarios with non-global states.

IFDSDA [15] was developed to manage UAV swarm coordination under disrupted or failed communication conditions. This approach empowers UAVs to fully utilise diverse sources of information in cases of communication failure. A decentralised MARL [16] framework was developed to address the problem of allocating constrained resources across heterogeneous traffic in RSU-deployed V2X communications.

To boost scalability and efficiency, a fully decentralized MARL framework [17] was introduced. In addition, a communication-efficient method was implemented to minimize data exchange without notably affecting control performance.. This was accomplished by applying randomised rounding numbers to encode transmitted data and transmitting only the non-zero elements after quantization.

Based on these observations, a decentralized communication strategy provides scalable, reliable and error-tolerant networking solutions. They are playing an important role in allowing secure and effective communication in smart distributed systems like IoT, blockchain and mesh networks.

2.3 Computational constraints at edge devices

Edge devices like smartphones, sensors and IoT nodes often face computational constraints like limited processing power, storage and energy. These disadvantages make the AI model's execution more complex, and real-time data processing is challenging. As edge computing becomes very common and solving these issues is critical for the system's effectiveness.

In 2024, a novel deep-learning-based algorithm [18] was introduced that leveraged the advantages of deep reinforcement learning. During training, it estimated the state components without relying on exact CSI, which was computationally expensive. This estimation reduced the communication overhead caused by collecting CSI data. Following this, in 2025, a RORA [19] method was introduced to address the short-sighted decision-making issue by an autonomous vehicle acting as an RL agent. This approach enables the agent to strategically choose power levels and the most suitable sub-band.

Solving computational problems requires lightweight models, hardware optimization and effective resource management. Addressing these issues helps edge devices to support intelligent, low-delay applications effectively.

3. Proposed Methodology

3.1 Overview of 6G Network

6G is the emerging future evolution of mobile network technology, providing high-speed connectivity, minimal transmission delay, and support for a large number of devices beyond 5G. It will allow modern applications like intelligent communication systems, live holographic displays and fully independent systems. The uses of 6G include improved customer experiences, smart cities and also helps for growing technologies like XR and the IoE. 6G connects devices in a mesh or cloud-based network. It will manage a larger number of devices at a time and

process larger amounts of data. It also enables the devices to work together intelligently to share data effectively. In 6G networks, the data will be shared among many devices and locations for fast processing and to minimize delays. This means the data will not always go to a central server but will also be shared with nearby edge devices. Because a lot of sensitive information and personal data is involved, the privacy policies will be very strict. Here, the data is safeguarded using strong security methods like encryption and access controls to protect it from hackers and unauthorised users. Additionally, edge devices like mobile phones, sensors, or small IoT gadgets have limited computing power, storage and battery charge. To manage this, the 6G system will balance the workload by sending some of the tasks to edge devices for processing, and the heavy tasks will be sent to cloud servers for processing. This will make the devices work effectively without wasting the battery or slowing down, and will ensure smooth and secure communication across the network.

3.2 Proposed Decentralised FL Architecture

Privacy preservation in 6G networks faces several problems, like increased data leakage because of high device connectivity and real-time data transmission. Enabling secure data exchange among dynamic environments is difficult. In addition, maintaining minimum delay performance with strong encryption and users' sensitive data remains a difficult challenge. Conventional data protection methods in 6G, such as end-to-end encryption, VPNs, and access control, offer fundamental security by safeguarding data during transmission and limiting access. However, they don't address risks associated with centralized data storage and processing, and they face difficulties with large datasets, ultra-low delay and large-scale device connectivity in 6G networks. Maintaining privacy without losing speed and effectiveness remains a challenging task. The visual representation of decentralized FL architecture is given in Fig. 1.

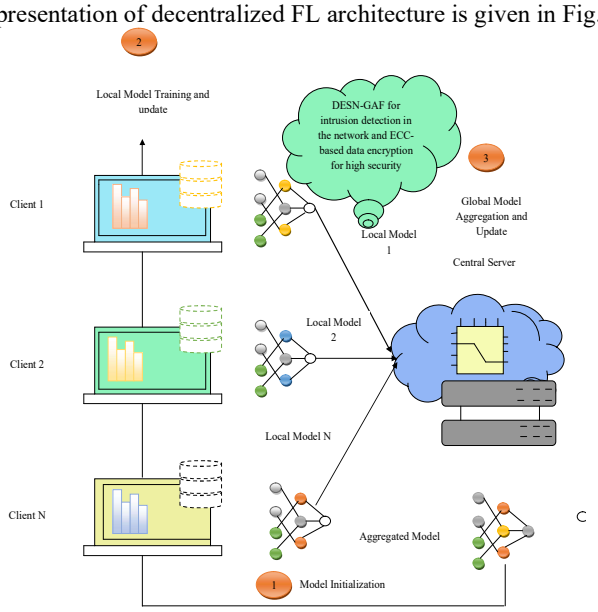


Fig. 1 Visual representation of the proposed Decentralized FL Architecture

To overcome the challenges faced in earlier approaches, FL is introduced in the 6G network for privacy preserving. FL introduces a deep learning model named DESN-GAF for detecting intrusion in the communication network. This DESN-GAF is developed by training directly on edge devices, which reduces the need for sharing the raw data; instead, it will only share the model updates. This method provides data privacy, minimizes bandwidth usage, and achieves low-delay goals of 6G. In order to achieve more security, ECC is used to safeguard data using mathematical curves to build a strong encryption with smaller key sizes. It ensures safe key interchange and data security, especially in resource-limited environments like 6G networks. ECC encrypts data before transmission and avoids third-party access. The encrypted data is taken as an output from the ECC. By managing the data locally, FL provides a secure and scalable solution for efficient network operation. The visual representation of the proposed privacy-preserving architecture in a 6G network based on intrusion detection and data encryption process is shown in Fig. 2.

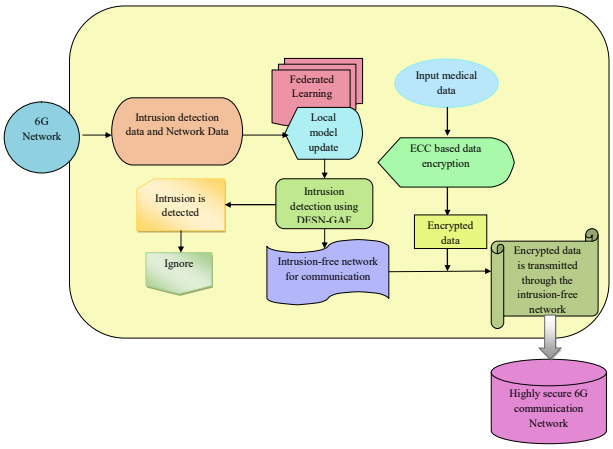


Fig. 2 Visual representation of the Proposed Privacy-Preserving Architecture in 6G Networks based on Intrusion Detection and Data Encryption Process

3.3 Dilated ESN

An ESN [21] is composed of three components, namely an input layer, a recurrent hidden layer referred to as the reservoir, and an output layer. During training, the weights of both the input and reservoir parameters are initialized randomly and remain unchanged. Moreover, the reservoir is set with very few connections to support various oscillation patterns. Only the output weights are adaptable and are typically optimized using linear regression. Given an N-dimensional starting point y (0), a D-dimensional input sequence $V=(v(1),...,v(t))^T$, and an L-dimensional output sequence $Z=(z(1),...,z(t),...,z(T))^T$, the updated expressions of an ESN with dilated connections are as follows:

$$y(t)=\begin{cases} f\left(P_{res}\,y(t-d)+P_{in}\,v(t)\right) & if\ t \bmod d=0 \\ y(t-1) & otherwise \end{cases} \tag{1}$$

$$V(t)=f_{out}\left(P_{out}\,y(t)\right) \tag{2}$$

Here, the term $v(t)\in S^D, z(t)\in S^L$ denotes the vectors of input and output at an instant t. The terms P_{in} P_{res} P_{out} specify the connection weights that link the input layer to the reservoir, govern interactions within the reservoir, and connect the reservoir to the output layer, respectively. The terms P_{in} P_{res} are randomly assigned and fixed during learning, while only P_{out} is learnable.

The terms f f_{out} represent the activation function in the reservoir and the output layer, respectively. The term d denotes the dilation factor, indicating how many time steps are skipped between reservoir state updates. When d=1, this corresponds to the conventional ESN update. The dilated update mechanism enables the reservoir to integrate data from long time intervals, enabling the network to capture distant temporal dependencies more efficiently with minimal computational cost.

3.4 GELU Activation Function

The GELU activation function [22] is a smooth, differentiable approximation of the rectifier function. It has become popular in deep learning because of its properties like non-linearity, ability to be differentiated and smoothness. The GELU activation function can be calculated from the Gaussian CDF, which is given as in Eq. (1).

$$\phi(y)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} e^{-\frac{t^2}{2}}dt \tag{3}$$

Here, the term $\phi(y)$ denotes the likelihood that a standard normal random variable assumes a value less than or equal to y. We can denote the GELU function as a multiplication of the input y and the Gaussian CDF.

$$GELU(y)=y\cdot\phi(\alpha y) \tag{4}$$

Here, the term $\alpha > 0$ is a scaling factor that handles the smoothness characteristic of the GELU function. Generally, α to summarise the GELU function and make it easier to use and faster to compute, we approximate the Gaussian CDF with this function.

$$\phi(\alpha y) \approx \frac{1}{2}\left(1 + \tanh\left(\beta\left(\alpha y + \gamma(\alpha y)^3\right)\right)\right) \tag{5}$$

$$GELU(y) = 0.5y\left(1 + y\tanh\left(\sqrt{\frac{2}{\pi}}\left(y + 0.044715y^3\right)\right)\right) \tag{6}$$

Here, $\beta > 0$ and γ constants are chosen to make the approximation as accurate as possible. Applying this approximation to the GELU function yields its final expression. Applying this approximation to the GELU function yields its final expression.

3.5 FL Integrated DESN-GAF for Intrusion Detection

DESN-GAF is used in 6G to detect intrusion in the network for privacy preserving the data due to its ability to perform effective local data processing. Because of its lightweight design, it is more suitable for edge devices and does not require central server processing. The GELU activation improves model accuracy while balancing low computational cost. This helps to keep customers' data safe while making fast, smart decisions directly at the edge. DESN-GAF is developed by improving the ESN with dilated connections and the GELU activation function. Dilated connections enable the network to study long-term dependencies in sequential data more effectively. The GELU activation improves learning performance by providing smoother and more effective nonlinear transformations. This architecture is lightweight and fast, making it suitable for edge computing in 6G networks. It provides instant data processing without high computational needs. DESN-GAF is important for performing privacy-preserving tasks smartly on edge devices directly in 6G networks. Integrating FL with DESN-GAF enables edge devices to jointly train accurate models without the need to share raw data and improves privacy. DESN-GAF's lightweight and efficient design is more suitable for the limited resources of edge nodes in 6G networks. This DESN-GAF analyses the network data and determines the intrusion in the network. If the intrusion is detected, then the network will not be considered for communication purposes. Only the intrusion-free network will be used for communicating the data in the 6G network. This integration helps to scale, privacy-preserving AI for applications like smart cities and automated systems. This ensures fast, secure and more efficient communication in 6G networks. The diagrammatic representation of FL with DESN-GAF architecture for efficient and privacy-preserving intrusion detection is shown in Fig. 3.

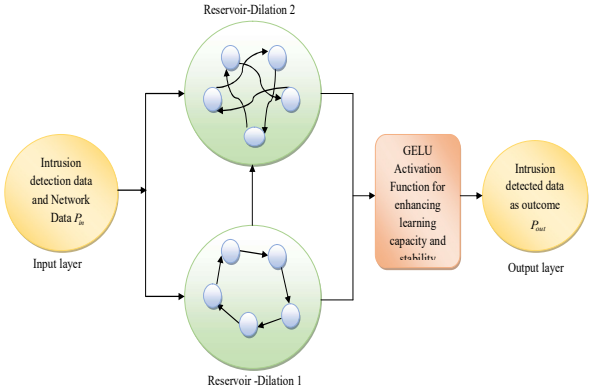


Fig. 3 Diagrammatic representation of DESN-GAF FL Architecture for Efficient Intrusion Detection

3.6 Security with ECC-based Data Encryption

ECC is used in this model for securing the data before transferring it into the network by performing data encryption at the transmitter side, and for retrieving the data, data decryption will be performed at the receiver end. In this model, for performing data encryption, input medical data from the diabetic dataset is used.

Let the term F denote an elliptic curve over a finite field G_q, a point on $F(G_q)$ it is represented by P, and it has first order o. The cyclic subgroup of $F(G_q)$ is generated by a point

$Q \quad < Q >= \{\infty, Q, 2Q, 3Q.....(O-1)Q\}$. The public domain parameters are prime, the equation of the elliptic curve, the point and its order are represented by q, F, Q and o. An integer f is a private key that is chosen randomly inside the interval $[1, o-1]$, and the public key is $R = e * Q$. The plain text message n is encoded first, and it is to be sent as an x-y point Q_n. The point Q_n is encrypted as a ciphertext, and at the same time, it will also be decrypted. To send an encrypted message Q_n to C, the term B selects a random positive integer l and generates the ciphertext $D_n = \{lQ, Q_n + lR\}$, where the term R is the public key of C. The points $D_1 = lQ \quad D2 = Q_n + lR$ are transmitted by the sender to the recipient. For decrypting the ciphertext, the term C products, the initial point in the pair by $C's$ the secret key and the results are subtracted from the secondary point $Q_n + lR - e(lQ) = Q_n + l(eQ) - e(lQ) = Q_n$. Finally, the intrusion-free encrypted data is obtained for highly secure 6G communication.

4. Experimental Setup

4.1 Datasets used

In the designed model, the intrusion detection data was collected from the following dataset for analysing the performance of DESN-GAF for intrusion detection. The intrusion detection data was accessed at https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html with the access date being 03-07-25.

In the designed model, the diabetes data was collected from the following dataset for analysing the performance of encryption and decryption with ECC. The Diabetes Dataset is accessed at https://www.kaggle.com/datasets/akshaydattatraykhare/diabetes-dataset, with the access date being 03-07-25. This dataset is 23.88kB in size and saved in a .csv format.

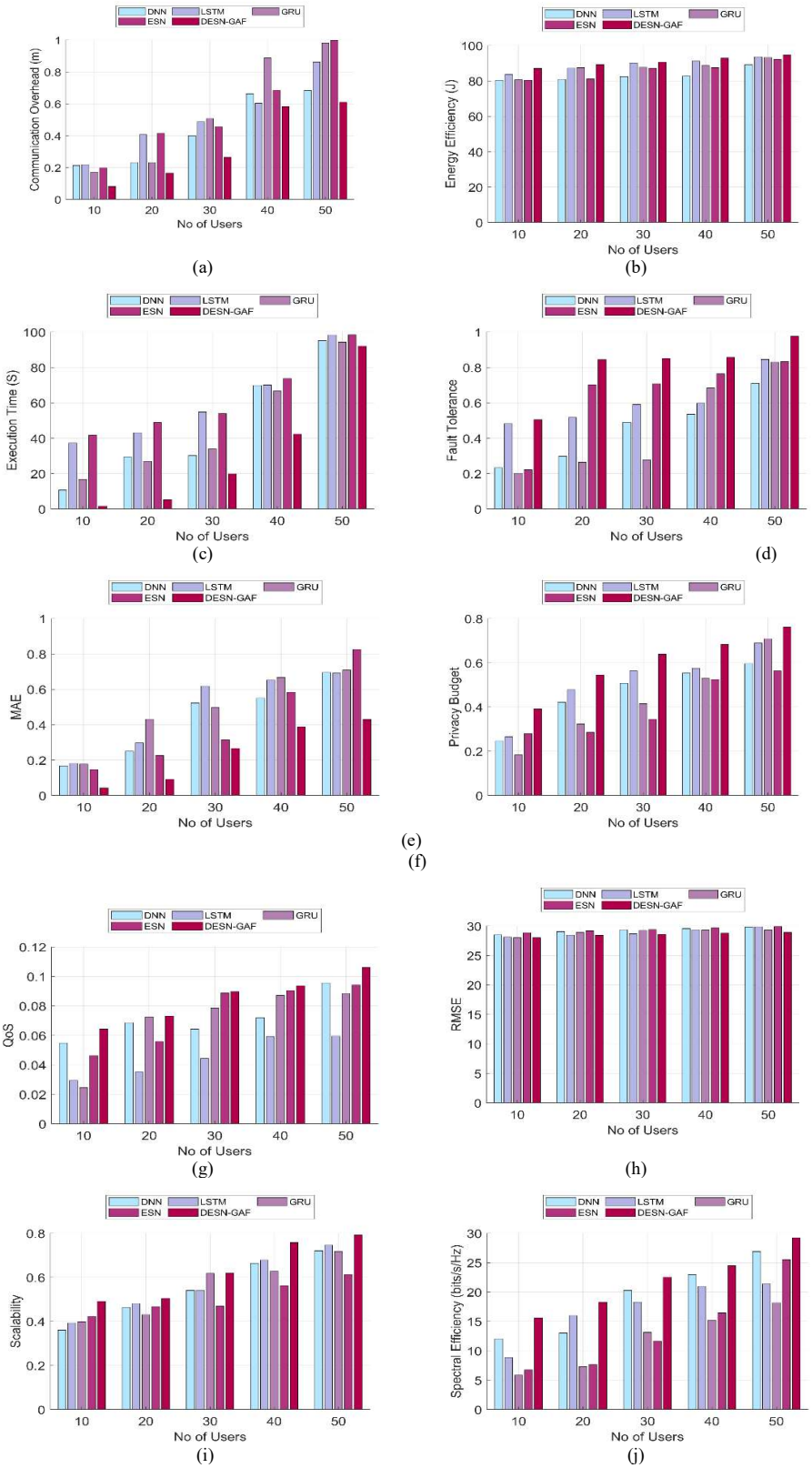
4.2 Simulation Platform and Parameters

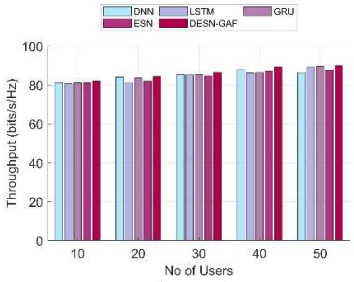
The execution environment for the developed privacy-preserving FL model in the 6G Network was built in Python. Here, the effectiveness of privacy preservation of the introduced model is compared over standard methods like DNN [24], LSTM [25], GRU [26] and ESN [21]. The time-based analysis of encryption and decryption is compared over standard methods like AES [27], RSA [28], DSA[29] and DHA[30].

4.3 Results and Discussion

Fig. 4 shows the performance of the proposed DESN-GAF method in privacy-preserving learning in a 6G network compared with several existing methods like DNN, LSTM, GRU and ESN under several metrics like communication overhead, energy efficiency, execution time, fault tolerance, MAE, privacy budget, QoS, RMSE, scalability, spectral efficiency and throughput. This investigation takes significant measures to determine the efficacy of the model in privacy-preserving FL in 6G networks. The effectiveness of the proposed DESN-GAF method is 3.9 %, 2.06 %, 4.1 % and 29 % higher when compared to standard approaches like DNN, LSTM, GRU and ESN, while taking the scalability value with 50 users. Hence, the estimated result showed that the introduced DESN-GAF achieved higher efficiency than other existing standard models for privacy-preserving FL in 6G networks.

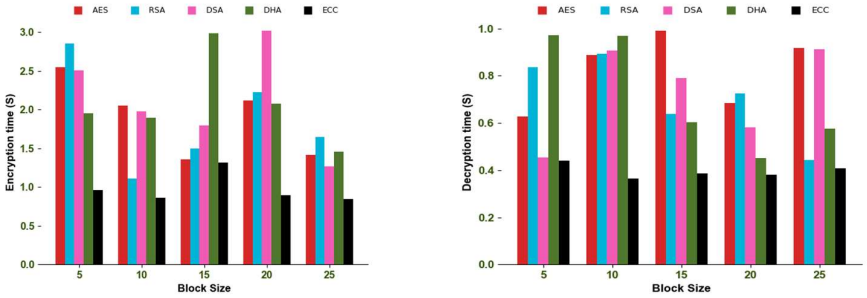
Fig. 5 shows the encryption and decryption time analysis of the proposed ECC-based method, compared with several existing methods like AES, RSA, DSA and DHA. The time taken for encrypting and decrypting the data by the proposed ECC model is 64%, 66%, 64% and 52% lower than the standard algorithms like AES, RSA, DSA and DHA, while taking the block size of 50. Hence, the estimated result showed that the introduced ECC-based method achieved lower encryption and decryption time than other existing standard algorithms. The developed ECC-based method demonstrated high performance with respect to reduced encryption and decryption times, which makes the network fast and more secure for data transmission. This is essential for making the data safe and private in 6G networks.


DNN
LSTM
GRU
ESN
DESN-GAF
Communication Overhead (m)
Energy Efficiency (J)
Execution Time (S)
Fault Tolerance
MAE
Privacy Budget
QoS
RMSE
Scalability
Spectral Efficiency (bits/s/Hz)
No of Users
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)



(ksssssss)

Fig.4 Privacy-Preserving FL Evaluation on the Developed Model over Traditional Models in terms of (a) Communication Overhead, (b) Energy Efficiency, (c) Execution Time, (d) Fault Tolerance, (e) MAE, (f) Privacy Budget, (g) QoS, (h) RMSE, (i) Scalability, (j) Spectral Efficiency and (k) Throughput



(a) (b)

Fig. 5 Analyzis on Encryption and Decryption Time on the Developed ECC-based Data Privacy Preserving Model over Traditional Methods

5. Connclusion

A novel FL approach was proposed to facilitate secure and effective data handling across distributed nodes in 6G network environments. The core of this system was the development the DESN-GAF model for performing intrusion detection to enhance local computation. Once local training is completed, the updates are securely aggregated to construct a global model, ensuring that raw data remains confidential throughout the process. Also, the data transferred through an intrusion-free network was encrypted using ECC to ensure more security. To evaluate the model's effectiveness, DESN-GAF was benchmarked against conventional architectures such as DNN, LSTM, GRU, and the standard ESN. The results highlighted performance improvements of 3.9%. 2.06%, 4.1% and 29% respectively, confirming DESN-GAF's superior accuracy and privacy efficiency. Overall, the findings indicate that DESN-GAF is a reliable and scalable solution for secure FL in advanced 6G network applications.

References

[1] V. S, R. Manoharan, S. Ramachandran and V. Rajasekar, "Blockchain-Based Privacy Preserving Framework for Emerging 6G Wireless Communications," IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4868-4874, 2022.

[2] S. A. Soleymani, S. Goudarzi, M. H. Anisi, Z. Movahedi, A. Jindal and N. Kama, "PACMAN: Privacy-Preserving Authentication Scheme for Managing Cybertwin-Based 6G Networking," IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4902-4911, July 2022.

[3] X. Wang, J. Lyu, J. D. Peter and B. -G. Kim, "Privacy-Preserving AI Framework for 6G-Enabled Consumer Electronics," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3940-3950, 2024.

[4] H. Fang, X. Wang, Z. Xiao and L. Hanzo, "Autonomous Collaborative Authentication with Privacy Preservation in 6G: From Homogeneity to Heterogeneity," IEEE Network, vol. 36, no. 6, pp. 28-36, 2022.

[5] S. Guo, A. Zhang, Y. Wang, C. Feng and T. Q. S. Quek, "Semantic-Enabled 6G Communication: A Task-oriented and Privacy-preserving Perspective," IEEE Network, 2025.

[6] Hongping Li, Shancang Li and Geyong Min, "Lightweight privacy-preserving predictive maintenance in 6G enabled IIoT, Journal of Industrial Information Integration, vol. 39, 2024.

[7] Rafael Teixeira, Gabriele Baldoni, Mário Antunes, Diogo Gomes and Rui L. Aguiar, "Leveraging decentralized communication for privacy-preserving federated learning in 6G Networks," Computer Communications, vol. 233, 2025.
[8] D. Han, Y. Liu, R. Cao, H. Gao and Y. Lu, "A Lightweight Blockchain Architecture with Smart Collaborative and Progressive Evolution for Privacy-Preserving 6G IoT," IEEE Wireless Communications, vol. 31, no. 5, pp. 148-154, 2024.
[9] Chuan Zhang, Xuhao Ren, Weiting Zhang, Yanli Yuan, Zehui Xiong and Chunhai Li, "Energy-efficient and Privacy-preserving Edge Intelligence for 6G-Empowered Intelligent Transportation Systems," IEEE Network, vol. 39, no. 2, pp. 134-141, 2025.
[10] Maira Khalid, Jehad Ali, Ahmed Raza Mohsin, Byeong-hee Roh and Mohammed J. F. Alenazi, "Deep learning techniques for enhanced security and privacy in 6G terrestrial–nonterrestrial network architecture," The Journal of Supercomputing, vol. 81, 2025.
[11] K. Raja, Kottilingam Kottursamy, Vishal Ravichandran, Sivaganesh Balaganesh, Kapal Dev and Lewis Nkenyereye, "An Efficient 6G Federated Learning-Enabled Energy-Efficient Scheme for UAV Deployment," IEEE Transactions on Vehicular Technology, vol. 74, pp. 2057-2066, 2025.
[12] Zhao, Borui, Qimei Cui, Wei Ni, Xueqi Li, and Shengyuan Liang, "Multi-Layer Collaborative Federated Learning architecture for 6G Open RAN," Wireless Networks, vol. 31, pp. 1377-1390, 2025.
[13] Zong, Ruixing, Yunchuan Qin, Fan Wu, Zhuo Tang, and Kenli Li, "Fedcs: Efficient communication scheduling in decentralized federated learning," Information Fusion, vol. 102, 2024.
[14] Y. Boutyour and A. Idrissi, "Adaptive Decentralized Policies With Attention for Large-Scale Multiagent Environments," IEEE Transactions on Artificial Intelligence, vol. 5, no. 10, pp. 4905-4914, 2024.
[15] Wang, Ziquan, Juan Li, Jie Li, and Chang Liu, "A decentralized decision-making algorithm of UAV swarm with information fusion strategy," Expert Systems with Applications, vol. 237, 2024.
[16] I. Lee and D. K. Kim, "Decentralized Multi-Agent DQN-Based Resource Allocation for Heterogeneous Traffic in V2X Communications," IEEE Access, vol. 12, pp. 3070-3084, 2024.
[17] D. Chen, K. Zhang, Y. Wang, X. Yin, Z. Li and D. Filev, "Communication-Efficient Decentralized Multi-Agent Reinforcement Learning for Cooperative Adaptive Cruise Control," IEEE Transactions on Intelligent Vehicles, vol. 9, pp. 6436-6449, 2024.
[18] Zhang, Lingling, and Yuan Zhang, "Deep Reinforcement Learning Based Subcarrier Allocation With End-To-End Implicit CSI Acquisition in Multiuser OFDM Systems," Transactions on Emerging Telecommunications Technologies, vol. 36, 2025.
[19] Mani Shekhar Gupta, Akanksha Srivastava and Krishan Kumar,"RORA: Reinforcement learning based optimal distributed resource allocation strategies in vehicular cognitive radio networks for 6G",Vehicular Communications, vol. 52, 2025.
[20] Teixeira, Rafael, Gabriele Baldoni, Mario Antunes, Diogo Gomes, and Rui L. Aguiar, "Leveraging decentralized communication for privacy-preserving federated learning in 6G Networks," Computer Communications, vol. 233, 2025.
[21] Ma, Qianli, Enhuan Chen, Zhenxi Lin, Jiangyue Yan, Zhiwen Yu, and Wing WY Ng, "Convolutional multitimescale echo state network," IEEE Transactions on Cybernetics, vol. 51, pp. 1613-1625, 2019.
[22] Lee Minhyeok, "Gelu activation function in deep learning: a comprehensive mathematical analysis and performance," 2023.
[23] Abdeltif Boujamza and Saâd Lissane Elhaq," Optimising Remaining Useful Life Predictions for Aircraft Engines: A Dilated Recurrent Neural Network Approach," IFAC-PapersOnLine, vol. 58, pp. 811-816, 2024.
[24] Liu, Guozhi, Fei Dai, Xiaolong Xu, Xiaodong Fu, Wanchun Dou, Neeraj Kumar and Muhammad Bilal, "An adaptive DNN inference acceleration framework with end–edge–cloud collaborative computing," Future Generation Computer Systems, vol. 140, pp. 422-435, 2023.
[25] X. Wen and W. Li, "Time Series Prediction Based on LSTM-Attention-LSTM Model," IEEE Access, vol. 11, pp. 48322-48331, 2023.
[26] Mim, Taima Rahman, Maliha Amatullah, Sadia Afreen, Mohammad Abu Yousuf, Shahadat Uddin, Salem A. Alyami, Khondokar Fida Hasan, and Mohammad Ali Moni, "GRU-INC: An inception-attention based approach using GRU for human activity recognition," Expert Systems with Applications, vol. 216, 2023.
[27] Ajagbe, Sunday Adeola, Oluwashola David Adeniji, Adedayo Amos Olayiwola, and Seun Femi Abiona, "Advanced encryption standard (AES)-based text encryption for near field communication (NFC) using Huffman compression," SN Computer Science, vol. 5, 2024.
[28] Mpitsi Maria, "A COMPARATIVE ANALYSIS OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM: MATHEMATICAL, ALGORITHMIC, AND PERFORMANCE COMPARISON," Knowledge-International Journal, vol. 65, pp.299-303, pp.299-303, 2024.
[29] Alfani, Mhd Reza, Mhd Furqan, and Yusuf Ramadhan Nasution, "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (DSA) Dan Advanced Encryption Standard (AES)," Journal of Science and Social Research, vol. 7, pp. 301-306, 2024.

[30] Chaudhary, Himanshi, Himanshu Chaudhary, and Awadhesh Kumar Sharma, "Optimised genetic algorithm and extended Diffie-Hellman as an effective approach for DOS-attack detection in cloud," International Journal of Software Engineering and Computer Systems, vol. 8, pp.69-78, 2022.