Enhancing Privacy in 6G Network through Decentralized Communication using CRYSTALS-Kyber 512 with Zenoh

[1]Naama Methab Athab and [2]Abdullahi Abdu Ibrahim
[1]Department of Computer Engineering
Altinbas University, Turkey
213720618@ogr.altinbas.edu.tr
[2]Department of Software Engineering
Altinbas University, Turkey
abdullahi.ibrahim@altinbas.edu.tr

Abstract: Presently, the evolution of 6G networks in dynamic and heterogeneous scenarios has gained more advancements among service providers, network operators and end users. Moreover, the 6G network built mutual trust among the users in a dynamic environment. Yet, the open nature of these networks faces multiple shortcomings in terms of trust and security because the centralized procedures are insufficient or inadequate in these scenarios. These technologies enable intelligent decision-making at the network edge, reducing latency and improving overall system responsiveness. Furthermore, several advancements in the 6G network aid in using various Artificial Intelligence (AI) techniques, edge intelligence and privacy preservation in the distributed learning models for communication enhancement. In order to offer collaborative training in the communication network without exposing the raw data, Federated Learning (FL) procedures are used. Deploying the 6G networks with FL faces more complications like inference attacks, complications in the dynamic and heterogeneous network and also an inherent trade-off between model performance and privacy protection. In order to improve the privacy preservation and decentralized communication in the 6G network, a new FL technique, CRYSTALS-Kyber 512 with Zenoh (CK512-Zenoh), is designed. The developed CK512-Zenoh is efficient in eliminating the communication overhead, privacy risks and generalization issues in the FL applications. Decentralized nature of CK512-Zenoh supports eliminating the overhead issues in low communication and makes it suitable to use in resource-constrained devices. This makes the approach particularly beneficial for edge devices with limited computational and storage capabilities. Later, different experiments are executed to verify the overall network efficiency in different classes under different experimental conditions.

Keywords: Decentralized Communication; Federated Learning; Privacy Preservation; 6G Network; CRYSTALS-Kyber 512 with Zenoh

Received: September 15, 2025 Revised: September 27, 2025 Accepted: October 16, 2025

Nomenclature

Abbreviation	Description
AI	Artificial Intelligence
IoT	Internet of Things
FL	Federated Learning
PoC	Proof-of-Concept
ECDH-P256	Elliptic Curve Diffie–Hellman (256-bit)
BIKE	Bit Flipping Key Encapsulation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
QUIC	Quick UDP Internet Connections Protocol
TLS	Transport Layer Security
CoAP	Constrained Application Protocol
MQTT	Message Queuing Telemetry Transport
gRPC	Remote Procedure Call Framework
MPI	Message Passing Interface
REST	Representational State Transfer
CPU	Central Processing Unit

1. Introduction

Some advancements in the 6G network help to redefine the intelligent connectivity by considering the2 AI-driven edge intelligence, massive machine-type communication and reliable low latency communication. These advancements are expected to support next-generation applications such as holographic communication, extended reality (XR), and intelligent automation. Among all the emerging technologies, FL is used widely, and it is considered an essential technique for improving privacy preservation in the 6G environment [1].

Performing training in the decentralized learning model supports for data localization in the edge devices, and the FL helps to eliminate the privacy-related risks in the centralized data samples. The FL models are widely used in the 6G applications like industrial automation, smart healthcare, and autonomous driving [2]. These applications demand real-time analytics and secure data processing to ensure reliability and user trust. Furthermore, the 6G technology offers more advancement in data transmission and maintaining the connectivity along with privacy-related concerns arising. Moreover, 6G effectively amplifies the challenges of data exposure in the smart devices through seamless integration, pervasive connectivity and higher data rates.

Major issues that take place in the 6G network are cyber attacks, which aid in using advanced privacy preservation techniques and scalable detection procedures [3]. These cyber threats include inference attacks, model poisoning, and data leakage, which can severely impact system performance and trustworthiness. Conventional centralized learning procedures are prone to various issues like communication overhead, privacy risks and generalization issues. Such limitations hinder their applicability in large-scale, distributed 6G ecosystems. The AI, Internet of Things (IoT), and edge computing in the 6G network help in enhancing the transmission speed and real-time decision-making. In a 6G network, exchanging the generated data samples needs huge surveillance in dynamic scenarios to protect the sensitive data from unauthorized access by attackers [4]. In addition, maintaining the geospatial precision in the 6G networks helps to improve the efficiency in the communication models and autonomous systems, yet these models need to eliminate the series threats in terms of location privacy along with unauthorized tracking. Deep interconnectivity in the 6G network helps to eliminate vulnerabilities to cyber threats and supports the implementation of advanced procedures by tackling the data breaching issues [5]. Conventional machine learning with an AI model for the 6G network supports for personalized services. But, these techniques are needed to eliminate the data misuse issues, privacy issues, and require maintaining huge trust among the users. By considering all these issues that take place in the classical techniques, a new FL-based technique is suggested to improve the privacy preservation at the 6G network with decentralized communication.

1.1 Contributions

- To implement a new privacy enhancement technique in 6G networks through decentralization and FL that helps to maintain higher security and reduce the latency. The developed technique is efficient in preserving the sensitive data from the attackers and also maintains higher preservation efficiency at data exchange and transmission. Additionally, it ensures robustness against emerging threats in dynamic network environments. Furthermore, this technique is capable of maintaining higher scalability over various decentralized system and eliminating the latency issues by reducing the transmission time.
- To propose CK512-Zenoh for improving the privacy preservation efficiency in 6G networks, which helps to maintain higher privacy while transmitting data samples. Moreover, the developed CK512-Zenoh is capable of eliminating the low computational overhead issues and also reducing the bandwidth utilization in the decentralized network. The integration of post-quantum cryptographic mechanisms further strengthens resistance against future quantum-based attacks. In addition, the confidentiality of the decentralized network is improved to restrict data access among unauthorized parties. Furthermore, this technique aids in maintaining better communication by eliminating the latency issues.

Overall organization of the research work is detailed as follows. Existing research work with critical analysis details is given in Section II. A detailed background of the privacy enhancement techniques is provided in Section III. Newly designed solutions for improving privacy in 6G networks are discussed in Section IV. Different experiments in the designed technique are given in Section V. The conclusion part with upcoming opportunities is given in Section VI.

2. Literature Survey of 6G Privacy Enhancement Framework with Critical Analysis

2.1 Related Works

Different research works designed for improving privacy in the 6G network with decentralized communication are detailed as follows. These studies focus on integrating advanced learning models and cryptographic techniques to address emerging security challenges in next-generation networks.

In 2026, Rahmati and Rahmati [6] have suggested a new resource management technique in the 6G network using the FL with a digital twin. This technique was efficient in minimizing the communication overhead and preserving the overall privacy in dynamic scenarios. The integration of digital twins enabled real-time monitoring and predictive optimization in complex network environments. The digital twin procedure was supported for dynamic optimization over different domains and for task offloading with energy balancing.

In 2026, Premkumar and Nachimuthu [7] have designed a privacy preservation technique named Federated Cross-Modal Graph Transformer (FCMGT). This technique was efficient in offering dynamic adversarial training and eliminating poisoning attacks. The use of graph-based representations improved the contextual understanding of multimodal data. Moreover, it maintained higher scalability and reliability over different attacks.

In 2025, Punitha and Preetha [8] have implemented a distributed technique using FL. The developed technique was designed by fusing the encryption procedure with Optimized Gated Transformer Networks (OGTN) for mitigating unknown cyber-attacks. The hybridization of encryption with transformer models enhanced robustness against unknown threats. The developed technique was efficient in maintaining higher integrity and data privacy.

In 2026, Dang *et al.* [9] have proposed an advanced privacy preservation technique with FL to improve the security in the cross-domain. Here, the TrustChain protocol was employed to eliminate the adaptive manipulation. TrustChain ensured decentralized validation and tamper-resistant data exchange. In addition, differential privacy procedures were employed to secure the data operator. This mechanism effectively reduced the linear complexity issues and confirmed the scalability.

In 2025, Hossain and Islam [10] have developed an FL-based privacy preservation mechanism for maintaining higher security in the decentralized network. The FL was good at maintaining higher robustness in preserving the privacy of the users. The model also incorporated adaptive learning strategies to handle dynamic data distributions. This technique was efficient in reducing the validation overhead and preserving the explainability.

2.2 Critical Analysis

Recently, various deep learning and FL techniques have been designed to improve privacy enhancement in 6G networks using decentralized communication. Despite significant progress, achieving an optimal balance between privacy, efficiency, and scalability remains a major research challenge. In this section, critical analysis is performed by considering the previously designed techniques and their details are provided as follows.

The usage of FL with a digital twin is considered in [6] for improving privacy. Nevertheless, this work fails to manage the higher communication overheads. The synchronization requirements between digital twins and physical systems increase latency in real-time applications. In addition, maintaining the generalization is challenging and also leads to more inaccuracies in the outcomes.

Next, FCMGT is employed in [7] to maintain higher privacy in the communication model. However, this technique is prone to more privacy-related risks, which may affect the global accuracy and also slow down the convergence. The complexity of graph transformer architectures also increases training time significantly. In addition, these techniques face higher complexity issues due to the FL setup and increase the communication expense. Furthermore, they lack in pre-training the network and lack in generalization.

Advancements in OGTN are considered in [8], which helps to maintain higher privacy while transmitting the data samples. Yet, the computational complexity of this technique is higher, which slows down the inference time under resource-constrained environments. This makes it less suitable for edge devices with limited processing power. Additionally, maintaining stability is challenging during the training phase and also affects decision-making.

Multiple strengths in TrustChain are considered in [9], which support maintaining higher privacy preservation and trust among the decentralized network. Yet, this technique fails to

maintain higher scalability while transmitting the enormous data samples. The blockchain-based structure may introduce latency due to consensus mechanisms. Moreover, maintaining trust among the users is challenging, and it leads to more losses.

FL is used in [10] for maintaining higher privacy under dynamic conditions. However, this technique has failed to maintain higher heterogeneity under the dynamic network conditions due to variation in the computational power and biasing issues. Data imbalance across clients further degrades the model performance. Several issues that take place in these techniques affect the overall privacy preservation efficiency in the network. Hence, tackling these issues is essential to maintain a better trade-off between network performance and privacy.

3. Background Details of the 6G Privacy Enhancement Framework through Decentralized Communication

3.1 Model Training

Different techniques employed to execute the model training are distributed learning, FL and traditional learning. These training paradigms play a crucial role in determining the efficiency, scalability, and privacy of modern 6G-enabled intelligent systems.

3.1.1 Traditional Learning

Among the entire model training procedure, it includes the basic training process. It executes the training procedure with a single computing unit and the data samples [11]. This centralized approach simplifies implementation but limits scalability in large-scale environments. Yet, they have failed to perform the vertical scaling procedure, which makes the learning process expensive. The machine learning and deep learning techniques are used widely to execute the training in minimal time.

3.1.2 Distributed Learning

In the distributed learning model, various computing units are used with the same distribution over multiple machines incorporated through high-speed links. This approach enables parallel computation and improves training efficiency for large datasets. This learning process is efficient in performing the horizontal scaling procedure on the input sample. Moreover, it uses a parameter server that is responsible for executing the training process.

3.1.3 Model Parallelism

This technique is employed to execute the partition procedures in horizontal or vertical form. It is particularly useful when the model size exceeds the memory capacity of a single device. Here, the horizontal partitioning is used to perform the separation process within the layers, and vertical partitioning is employed to separate the layers. This is efficient to use for a single computing unit, and they are not capable of handling the entire training process independently [12]. Moreover, this process faces more shortcomings at the partition phase, and also its inference time is higher.

3.1.4 Data parallelism

It is employed to distribute the training data over the different validation units. Each computing node processes a subset of data and periodically synchronizes model parameters. Its objective is to use various computing units for processing various samples at the same time. This process helps to speed up the processing speed and also minimize the time spent for each epoch.

3.1.5 Federated Learning

Presently, model training procedures face more issues due to data ownership. In order to rectify these issues, FL procedures are considered for training the entire model. FL has emerged as a key paradigm for privacy-preserving collaborative learning in distributed environments. The FL models are efficient in enhancing data centralization and data privacy through proper training at the data generation phase. The FL procedure forwards the gradients and weights instead of transferring the original data to the central server.

A structural illustration of training in a distributed learning model is offered in Fig. 1.

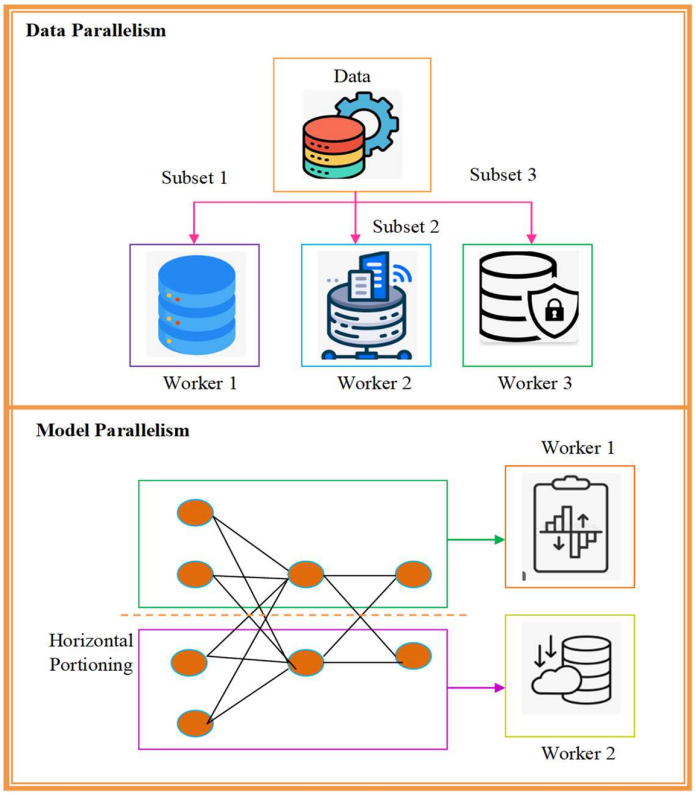


Fig. 1. Representation of Training in the Distributed Learning Model

3.2 Communication Protocols

Various communication protocols employed for the federated learning models are detailed as follows. These protocols determine the efficiency, latency, and reliability of data exchange in decentralized 6G environments.

3.2.1 Constrained Application Protocol (CoAP)

It's a kind of lightweight web transfer protocol widely used in resource-constrained networks and devices. It is specifically designed for low-power IoT environments with minimal bandwidth usage. It includes the user datagram protocol and follows the client-server architecture. It has a higher response rate and effectively reduces the overhead.

3.2.2 Message and Data Centric

They are widely used in the information and communication management process [13]. These paradigms focus on efficient data dissemination rather than endpoint-based communication. Message-centric techniques are employed to exchange messages among the particular endpoints. Moreover, the communications are coupled with the entities of identity and location. This creates more complications to maintain better performance in a distributed environment.

3.2.3 Hypertext Transfer Protocol with Representational State Transfer (HTTP REST)

This protocol is commonly designed for networking applications used in web services. It provides a standardized interface for communication across heterogeneous systems. Here, the REST is widely dependent on the HTTP procedures and supports for better communication. However, it may introduce latency due to its stateless nature and overhead.

3.2.4 Message Queuing Telemetry Transport (MQTT)

It works as a messaging protocol that supports better communication among the brokers and clients. It is optimized for low-bandwidth and high-latency networks. It has higher efficiency to use in IoT environments. It is a kind of publish-subscribe technique. Here, the clients subscribe to the specific topic and then receive the broadcast messages from another client.

3.2.5 Remote Procedure Calls (gRPC)

It is an open-source communication mechanism with higher performance. It leverages HTTP/2 for efficient binary communication and low latency. It works as a client-server communication model and permits direct calls among the distributed system for the underlying language or architecture.

3.2.6 Kafka

It is a kind of distributed streaming platform used for processing real-time data samples. It supports high-throughput data pipelines and real-time analytics. This protocol maintains higher scalability and fault-tolerance [14]. It is capable of generating the published data according to the topic, and also consumers subscribe to these topics for their personalize use.

3.2.7 Istio

It is an open-source service protocol for managing the infrastructure layer and also to observe the communication among the micro services in a distributed system. It provides features such as traffic control, security, and observability. They are operated by including the sidecar proxies for all service instances, load balancing and traffic management.

3.2.8 Message Passing Interface (MPI)

It is a standardized communication protocol used in parallel computing scenarios. It is widely adopted in high-performance computing environments. This protocol supports for efficient communication and is also capable of processing the distributed memory system for applications of higher performance computing.

3.2.9 Zenoh

It is efficient to use in the heterogeneous edge environment, which supports to ensure the robustness, efficiency and diverse interaction. Zenoh integrates data-centric communication with storage and computation, making it suitable for decentralized systems. This protocol supports providing more focus on the data processing phase.

4. Concerns and Proposed Solution for Privacy Enhancement in 6G Network through Decentralized Communication

4.1 Concerns in Traditional Communication Protocols

Various concerns associated with the classical communication protocols are given as follows. Generally, the communication protocols are employed to perform centralized control in the 6G networks. This centralized nature limits adaptability in highly dynamic and distributed 6G environments.

4.1.1 Managing Trust and Security

Classical communication protocols have failed to secure the network due to the functionalities of dispersed nodes [15]. The absence of end-to-end encryption and adaptive trust mechanisms increases vulnerability to attacks. Furthermore, these protocols lead to high latency issues in the 6G networks.

4.1.2 Higher Mobility and Incompatibility

Managing the networks from handover failures is challenging due to signalling overhead, continuous disconnection and higher latency. Frequent mobility of devices in 6G further intensifies these challenges. In some cases, the classical techniques fail to achieve higher efficiency under the multi-connectivity scenarios.

4.1.3 Resource Constraints and Performance

Overload issues in the network lead to congestion, which affects the authentication efficiency. This results in delays in identity verification and secure access control. Poor processing efficiency in the network was unable to fulfill the user needs in the 6G network.

4.1.4 Energy Consumption

Higher energy consumption in the training phase leads to quick energy draining. This is particularly critical for battery-operated edge devices. Moreover, a complicated packet structure requires enormous bandwidth, which makes it unsuitable for constrained networks.

4.1.5 Interoperability and Scalability Problems

Conventional communication protocols are limited to scalability when employed in large-scale networks [20]. They struggle to accommodate the exponential growth of connected devices in 6G ecosystems. In addition, their interoperability is limited, which creates more issues while connected to multiple devices.

4.1.6 Interference Issues

Classical networks are limited to short communication ranges. These communication protocols lead to high error rates in the dynamic environment. Environmental factors and dense deployments further increase interference levels.

4.2 Proposed Solution

Maintaining higher privacy and security in sensitive data during the transmission phase is challenging. This challenge becomes more significant in decentralized and heterogeneous 6G environments. Conventional privacy preservation techniques are prone to latency issues, which affect processing speed. These latency issues hinder real-time decision-making and system responsiveness. Moreover, these techniques face more issues while transferring the data samples to other users without any data loss. In some cases, attackers may aim to take over the sensitive information and forecast it, which affects the trust of the user. Such inference and reconstruction attacks pose serious threats to federated learning systems. These kinds of issues in the classical privacy preservation model affect the overall trust and create more challenges for the user. In order to tackle several issues in the prior techniques and also to maintain higher privacy in the 6G communication network CK512-Zenoh is employed. The proposed framework integrates post-quantum cryptography with efficient data-centric communication.

The CK512-Zenoh has higher efficiency in the edge-to-cloud, edge-to-edge and machine learning pipelines, and also its performance is contrasted over other communication protocols. This versatility makes it suitable for diverse 6G deployment scenarios. CK512-Zenoh is a kind of viable communication protocol that maintains higher efficiency in the FL environment.

In the developed CK512-Zenoh, collected attributes such as node resources, traffic parameters, performance measures, distributed system parameters, node degree and network parameters are given as the inputs. These parameters enable adaptive decision-making and optimized resource allocation. Here, the Proof-of-Concept (PoC) is included with the CK512-Zenoh, which works as an integral component and improves the performance in the applications of federated learning. The PoC validates the feasibility and effectiveness of the proposed approach in real-world scenarios.

The CK512-Zenoh is used with the distributed computing networks. Next, at the bottom-up layer, various transport protocols provide more support to CK512-Zenoh by including TLS, UDP, QUIC, and TCP. The use of multiple transport protocols enhances flexibility and reliability in communication. Moreover, supporting various transport protocols supports the entire participant takes place in the distributed system for selecting the most suitable one. Here, the nodes are efficient in providing better communication without considering any security in the CK512-Zenoh. However, the integration of cryptographic techniques ensures that security is not compromised. Moreover, the protocol CK512-Zenoh supports for maintaining higher flexibility and also maintains higher security in multiple cases.

Then, the runtime of CK512-Zenoh is analyzed with the actual component running. The CK512-Zenoh is capable of minimizing the overhead issues in multi-threading and improving the overall efficiency by improving the asynchronous system. Asynchronous execution further reduces latency and enhances throughput. Finally, the privacy-enhanced outcomes are obtained from the CK512-Zenoh.

Pictorial view of CK512-Zenoh for the privacy enhancement in the decentralized communication model is given in Fig. 2.

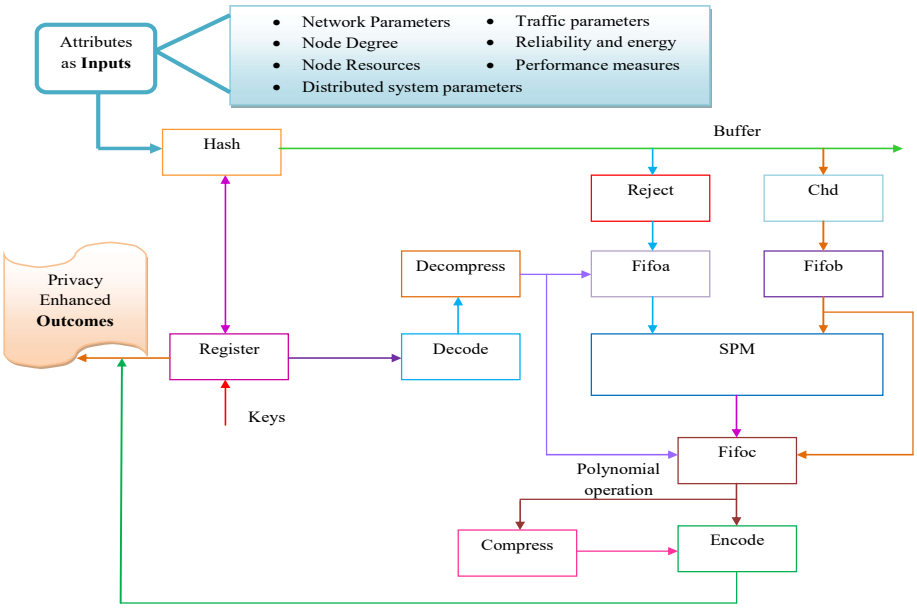


Fig. 2. Architectural Illustration of CK512-Zenoh for Privacy Enhancement in Decentralized Communication

5. Evaluation of Proposed Solution

5.1 Experiment Environment

In the developed privacy enhancement model for 6G network through decentralized communication was implemented and executed in Python. The implementation utilized standard machine learning libraries and network simulation frameworks to ensure reproducibility and accuracy. Here, different experimental procedures were considered to verify the overall network efficiency in different classes. Various privacy preservation techniques employed for the validation with CK512-Zenoh were Elliptic Curve Diffie–Hellman (ECDH-P256) [16], SABER lattice-based key encapsulation mechanism [17], Bit Flipping Key Encapsulation (BIKE) [18], and Kyber-1024 [19]. These techniques were selected due to their relevance in both classical and post-quantum cryptographic domains.

5.2 Initialization Attributes

In this research work, various attributes are initialized to enhance privacy in the 6G network for the decentralized communications as given in Table 1. These parameters are carefully selected to simulate realistic 6G network environments and heterogeneous device conditions.

Table 1. Initialization Attributes with Ranges

Parameters	Ranges with Units
Network Parameters	
Propagation Delay	1-10 (ms)
Bandwidth	50-200 (Mbps)
Transmission Rate	100-1000 (Mbps)
Packet Size	512-4096 (Bytes)
Node Resources	
Memory Size	4,8,16,32 (GB)
CPU Capacity	1.5-3.5 (GHz)
Storage Capacity	128,256,512,1024 (GB)
Node Degree	
Network Topology	Hybrid, Tree, Ring, Mesh and Star
Node Degree	2-10
Performance Measures	
Throughput	10-150 (Mbps)
Latency	5-50 (ms)
Reliability and Energy	
Recovery Time	1-10 (Seconds)
Failure Rate	0.01-0.1
Energy Consumption	10-100 (Watts)
Traffic Parameters	
Queue Size	20-100 (Packets)
Traffic Load	10-90 (%)
Packet Arrival Rate	(100-1000) (Packets/sec)
Distributed System Parameters	
Consensus Time	0.1-2.0 (Seconds)
Encryption Key Size	128,192,256, 512 (Bits)
Replication Factor	2-5

5.3 Results

In this phase, different experiments are performed to verify the overall efficiency of the developed technique over multiple performance measures and its details are given as follows. The evaluation focuses on key metrics such as latency, throughput, reliability, and bandwidth utilization.

5.3.1 Analysis on Nodes

Here, multiple validations are carried out in the developed mechanism over the nodes are represented in Fig. 3. This analysis helps to understand how the system scales with increasing node density. Performing the analysis by varying the nodes helps to verify the robustness and stability of the network in different scenarios. In the consensus delay analysis, the developed CK512-Zenoh accomplished minimal delay while transmitting the data samples. This reduction in delay indicates efficient synchronization among distributed nodes. Moreover, this validation helps to accomplish higher throughput efficiency and also improves the user efficiency in different conditions. Next, in the latency analysis, the developed CK512-Zenoh effectively reduced the latency compared to the classical models. At the 5th node, the latency is lower than other nodes. This suggests optimal resource utilization at moderate network sizes. In the bandwidth utilization validation, the designed CK512-Zenoh accomplished better efficiency as 17% for ECDH-P256, 15.6% for SABER, 6.6% for BIKE and 4.34% for Kyber-1024 at the 5th node. This demonstrates that the proposed model achieves significant bandwidth savings compared to existing techniques. Hence, the validation outcomes displayed that the suggested technique is efficient in maintaining higher privacy than the classical communication protocol in dynamic conditions.

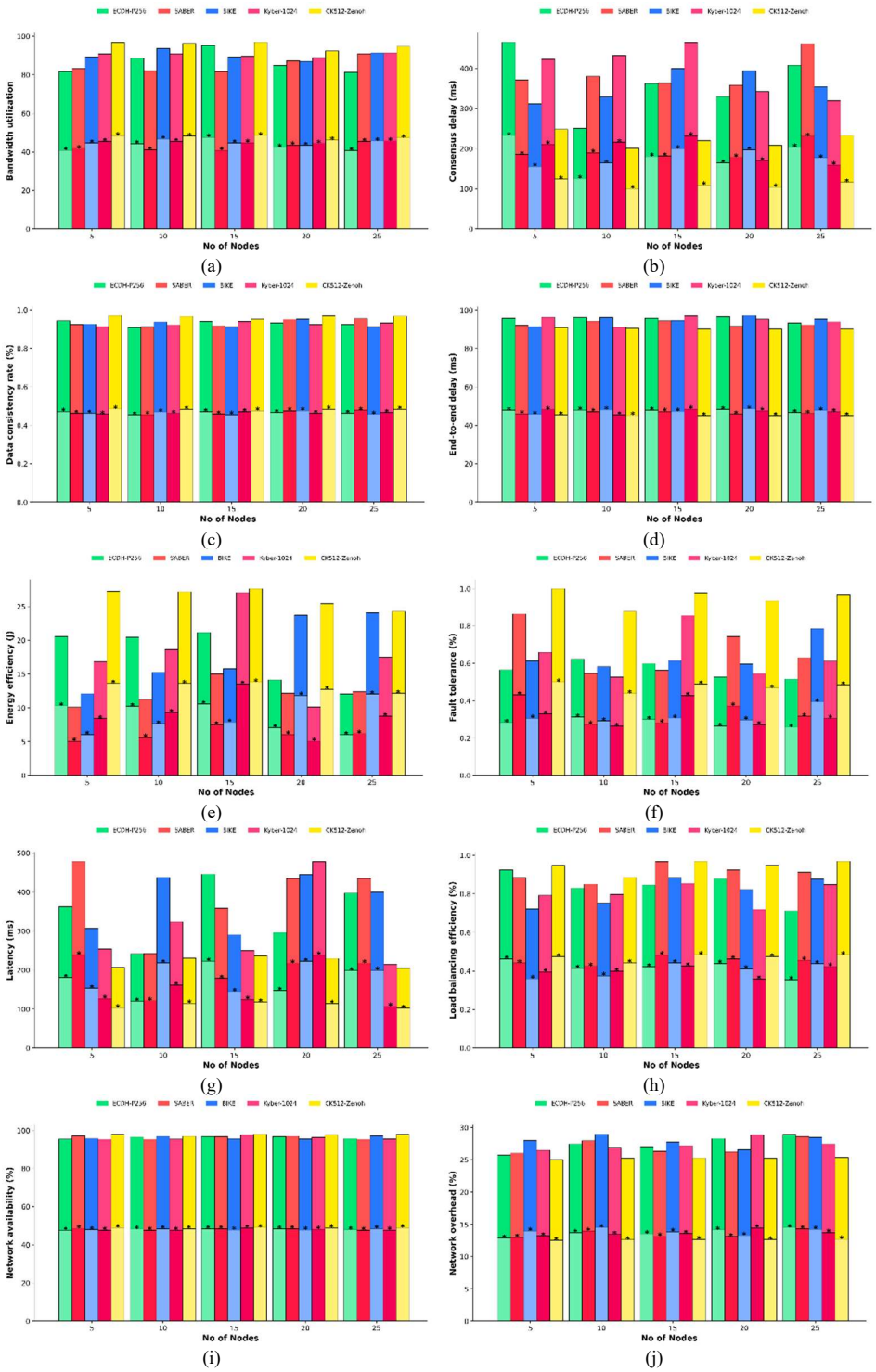


Fig. 3. Validation on Nodes in Designed Privacy Enhancement Technique for 6G Networks through Centralized Communication over (a) Bandwidth Utilization, (b) Consensus Delay, (c) Data Consistency Rate, (d) End-to-end Delay, (e) Energy Efficiency, (f) Fault Tolerance, (g) Latency, (h) Load Balncing Efficiency, (i) Network Availablity and (j) Network Overhead

5.3.2 Validation on Traffic Load

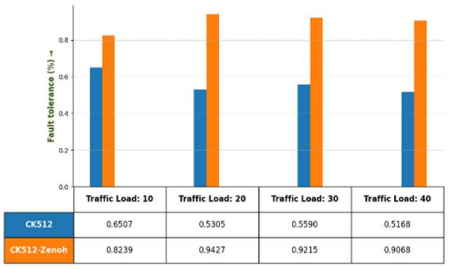
Different validations executed by analyzing the traffic load in the designed CK512-Zenoh-based privacy enhancement model in the 6G networks are displayed in Fig. 4. Traffic load analysis is essential to evaluate system performance under varying network congestion levels. Performing

the analysis by varying the traffic load supports to verify the message counts transmitted in the network in a particular time. In the end-to-end delay analysis, the developed CK512-Zenoh accomplishes a reduced delay compared to the classical models. This indicates efficient routing and communication handling under heavy traffic conditions. Here, the developed CK512-Zenoh accomplished a reduced delay rate as 90.14% at a traffic load of 30. Next, in the reliability analysis, the developed CK512-Zenoh accomplished a higher reliability as 0.97% for the traffic load 20. Moreover, the analysis outcomes displayed that the packet loss ratio of the developed model is lower than the classical techniques. Reduced packet loss improves overall communication quality and user experience. Thus, the overall analysis outcomes displayed that the suggested communication protocol CK512-Zenoh is good in maintaining higher privacy than the classical schemes in different classes.



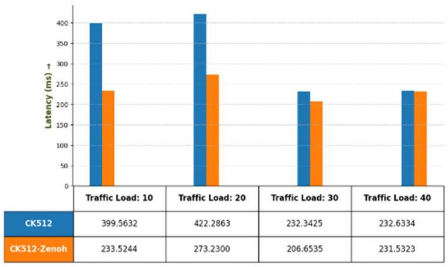
	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	96.9007	92.2206	91.5819	95.9889
CK512-Zenoh	91.2186	90.3782	90.1427	90.1850

(a)



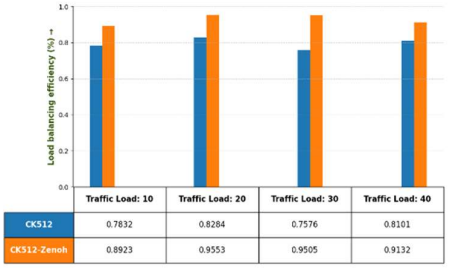
	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	0.6507	0.5305	0.5590	0.5168
CK512-Zenoh	0.8239	0.9427	0.9215	0.9068

(b)



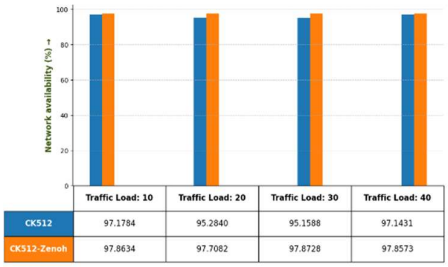
	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	399.5632	422.2863	232.3425	232.6334
CK512-Zenoh	233.5244	273.2300	206.6535	231.5323

(c)



	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	0.7832	0.8284	0.7576	0.8101
CK512-Zenoh	0.8923	0.9553	0.9505	0.9132

(d)



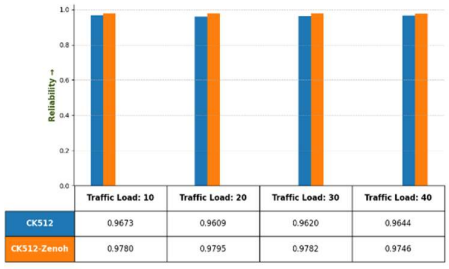
	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	97.1784	95.2840	95.1588	97.1431
CK512-Zenoh	97.8634	97.7082	97.8728	97.8573

(e)



	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	88.9072	71.5497	77.1788	65.8660
CK512-Zenoh	51.7475	50.9267	53.6379	51.5059

(f)



	Traffic Load: 10	Traffic Load: 20	Traffic Load: 30	Traffic Load: 40
CK512	0.9673	0.9609	0.9620	0.9644
CK512-Zenoh	0.9780	0.9795	0.9782	0.9746

(g)

Fig. 4. Analysis over Traffic Loads on the Designed Privacy Enhancement Technique over (a) End-to-end Delay, (b) Fault Tolerance, (c) Latency, (d) Load Balancing Efficiency, (e) Network Availability, (f) Packet Loss Rate, and (g) Reliability

6. Conclusion

An efficient privacy enhancement technique for 6G networks through a decentralized network was designed with FL, which helped to improve the privacy preservation in different classes.

The proposed approach leverages decentralized intelligence to address the growing concerns of data security in next-generation networks. Here, an advanced communication protocol CK512-Zenoh was used to enhance privacy by tackling the privacy risks and communication overheads. The integration of post-quantum cryptographic mechanisms further strengthens the resilience of the system against emerging threats. The developed CK512-Zenoh was capable of tackling the generalization and overhead problems at the resource-constrained devices. Further, the efficiency of the designed techniques was verified over different communication protocols to ensure privacy in several classes. Extensive experimental evaluations confirmed its superiority in multiple performance metrics. In the bandwidth utilization validation, the designed CK512-Zenoh accomplished better efficiency as 17% for ECDH-P256, 15.6% for SABER, 6.6% for BIKE and 4.34% for Kyber-1024 at the 5th node. These improvements highlight the effectiveness of the proposed protocol in optimizing communication resources. Thus, the validation outcomes displayed that the suggested technique was efficient in improving the overall privacy of the network in different classes.

6.1 Limitations and Future Directions

Though the developed technique effectively improved the privacy in 6G communication, it faces several limitations, and they are detailed as follows. Despite its advantages, certain challenges remain in achieving complete security in highly dynamic environments. Maintaining the security of sensitive information is challenging, which leads to data breaches. This kind of issue in the developed technique will be rectified in future work by considering the Blockchain technology to store the sensitive information, which helps to protect the data from unauthorized data access. Blockchain integration can provide immutability, transparency, and enhanced trust in decentralized systems. Further improvements may include optimizing computational efficiency and reducing energy consumption in large-scale deployments.

References

[1] Kumar, A., Chaudhary, A. and Singh, B.K., "Differential Privacy Enabled Federated LSTM Model for Decentralized Active User Detection in 6G Cell-Free mMIMO Networks," IEEE Access, vol. 13, pp. 197345-197360, 2025.

[2] Du, M., Yang, P., Liu, Y., He, X. and Chen, M., "DP-Fed6G: An adaptive differential privacy-empowered federated learning framework for 6G networks," Digital Communications and Networks, Vol. 11, no. 6, pp. 1994-2002, December 2025.

[3] Nez-Gómez, C.N., Garcia-Font, V., Rifá-Pous, H. and Asad, M., "NxGenT: A decentralized trust system for B5G and 6G networks based on blockchain and smart contracts," Blockchain: Research and Applications, pp. 100447, 20 January 2026.

[4] Yang, T. and Wang, J., "BHMFL: Autonomous Federated Learning for Privacy-Aware Health Monitoring via Self-Balancing Data Synthesis in Smart 6G-HIoT Systems," IEEE Internet of Things Journal, vol. 13, no. 5, pp. 8108-8119, 1 March 1, 2026.

[5] Yan, K., Ma, W. and Sun, S., "BECS: A Privacy-Preserving Computing Resource Sharing Mechanism for 6G Computing Power Network," IEEE Transactions on Network Science and Engineering, vol. 13, pp. 4725-4742, 2026.

[6] Rahmati, M. and Rahmati, N., "Federated learning-driven digital twin framework for adaptive resource management in 6G edge networks," Journal of Electrical Systems and Information Technology, Vol. 13, no. 5, 2026.

[7] Premkumar, D.P. and Nachimuthu, S.K., "Privacy-preserving cyberthreat detection in decentralized social media with federated cross-modal graph transformers," Scientific Reports, Vol. 16, no. 3608, 2026.

[8] Punitha, S. and Preetha, K.S., "Enhancing reliability and security in cloud-based telesurgery systems leveraging swarm-evoked distributed federated learning framework to mitigate multiple attacks," Scientific Reports, Vol. 15, no. 27226, 2025.

[9] Dang, Q.V., Vo, T.B.D. and Nguyen, N.S.A. "FORTRESS-FL: Byzantine-robust and privacy-preserving federated orchestration for next-generation networks," Array, Vol. 29, pp. 100680, March 2026.

[10] Hossain, M.A. and Islam, M.S., "Towards Decentralized Cybersecurity: A Novel Privacy-Preserving Federated Learning Approach for Botnet Attack Detection," Blockchain: Research and Applications, pp.100355, 16 August 2025.

[11] Batool, I., Fouda, M.M., Ismail, M., Rabie, K., Verma, S. and Fadlullah, Z.M., "AMADRL: Privacy-Aware Attention-Based Multiagent Deep Reinforcement Learning for Optimizing Spectral Allocation in 6G Vehicular Networks," IEEE Internet of Things Journal, vol. 13, no. 3, pp. 4792-4808, 1 Feb.1, 2026.

[12] Singh, N.K., Chandel, S.T., Lim, S. and Lee, J., "Federated Learning-Based Energy-Efficient Consumer-Centric Access Strategy for Cell-Free MIMO in 6G Wireless Networks," IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 4292-4303, May 2025.
[13] Prajapat, S., Kumar, D., Kumar, P., Das, A.K. and Hossain, M.S., "A Lattice-Based Ring Signcryption Scheme for Secure Communication in 6G-Enabled Vehicular Ad Hoc Networks Using Blockchain," IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 12, pp. 23007-23020, Dec. 2025.
[14] Ning, B., Zhang, X., Liu, C., Wang, N. and Li, G., "Enhancing Group Privacy for Effective CIoT Data Mining in 6G Networks Using Differential Privacy," IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 5969-5983, May 2025.
[15] Zheng, W., Anwlnkom, T. and Liu, Y., "TRUST-Med6G: A Secure and Trustworthy Medical Data Privacy Protection Mechanism in 6G-IoT," IEEE Internet of Things Journal, vol. 13, no. 5, pp. 8248-8260, 1 March 1, 2026.
[16] Tanksale, V., "Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices," Electronics, vol. 13, no. 18, pp. 3631, 2024.
[17] Samiullah, F., Gan, M.L., Akleylek, S. and Aun, Y., "Quantum Resistance Saber-Based Group Key Exchange Protocol for IoT," IEEE Open Journal of the Communications Society, vol. 6, pp. 378-398, 2025.
[18] Nosouhi, M.R., Shah, S.W.A., Pan, L. and Doss, R., "Bit Flipping Key Encapsulation for the Post-Quantum Era," IEEE Access, vol. 11, pp. 56181-56195, 2023.
[19] de la Torre, M.Á.G., Morales Sandoval, I.A., de Abreu, G. T. F. and Hernández Encinas, L., "Post-Quantum Wireless-based Key Encapsulation Mechanism via CRYSTALS-Kyber for Resource-Constrained Devices," 2025.
[20] Teixeira, R., Baldoni, G., Antunes, M., Gomes, D. and Aguiar, R.L., "Leveraging decentralized communication for privacy-preserving federated learning in 6G Networks," Computer Communications, Vol. 233, pp. 108072, 1 March 2025.