International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Advanced Privacy-Preserving Federated Learning in 6G Networks Using Differential Privacy and Homomorphic Encryption

E.D.Kanmani Ruby[1]*, G.Linda Rose[2], P. Yashaswinii[3], K.Sripal Reddy[4], S. Jeyalakshmi[5], B.Hari Chandana[6]

Submitted: 12/05/2024 **Revised**: 25/06/2024 **Accepted**: 05/07/2024

Abstract: In the age of 6G networks, ensuring robust privacy and security measures is essential. Given the widespread connectivity and a plethora of applications, the management of extensive data in the realm of 6G, facilitated by cutting-edge technologies, demands an elevated level of safeguarding. Essentially, strong privacy measures cultivate trust, encouraging broad adoption by instilling confidence among both users and organizations. In this landscape, prioritizing privacy and security is paramount to safeguarding sensitive information, maintaining integrity, and mitigating risks associated with the dynamic and interconnected nature of 6G networks. The research introduces an advanced federated learning approach tailored for 6G networks. Utilizing differential privacy during localized model training and homomorphic encryption for secure transmission, the central server orchestrates secure aggregating encrypted updates. This collaborative learning model progressively enhances global accuracy while preserving individual data privacy. Robust monitoring ensures regulatory compliance and dynamic improvements to privacy mechanisms signify the proactive evolution of this paradigm within the enigmatic realms of 6G networks, offering a significant advancement in both model precision and privacy standards.

Keywords: *6G Network, Homomorphic Encryption, Differential Privacy, Data Security, Global Accuracy.*

1.Introduction

In the fast-changing world of data-driven technologies, making security stronger is crucial. Two innovative methodologies, homomorphic encryption and differential privacy, stand out as crucial elements in fortifying security measures across various applications. These cutting-edge techniques play pivotal roles in addressing the challenges associated with data privacy and security, particularly in the context of advanced data processing and collaborative learning environments. Homomorphic encryption represents a breakthrough in cryptographic techniques [1]. It enables computations to be performed directly on encrypted data without the need for decryption. This capability is revolutionary as it allows data to remain in a secure, encrypted state throughout processing [2].

Traditional encryption methods require data to be decrypted before any computations can take place, potentially exposing sensitive information [3].

Homomorphic encryption, in contrast, ensures that computations can be carried out on encrypted data, maintaining confidentiality and integrity throughout the entire process. This approach is particularly valuable in scenarios where data privacy is of utmost concern, such as in healthcare, finance, and collaborative machine learning [4]. Differential privacy, on the other hand, focuses on introducing controlled noise during data analysis to protect individual privacy. This technique acknowledges the delicate balance between deriving meaningful insights from data and safeguarding the sensitive information inherent in that data. In collaborative learning scenarios, where multiple entities contribute data for model training, differential privacy ensures that no single contribution can be isolated or reverse-engineered, thereby preventing the inadvertent disclosure of sensitive details. By injecting carefully calibrated noise into the data, the privacy of individual contributions is preserved, paving the way for secure and collaborative data analysis.

Federated Learning serves as a good solution to address privacy concerns in the era of data-driven technologies. Traditional machine learning models often require centralized access to vast datasets, raising significant privacy and security challenges [5] In contrast, federated learning operates on a decentralized premise, allowing models to be trained across multiple local devices or

[1]*Professor.Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R and D Institute of Science and Technology, Chennai-600062, Tamil Nadu, India.*
Email: bewinbewin54@gmail.com* (Corresponding Author)
[2]*Assistant Professor, Division of Digital Sciences, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu-641114,India.*
Email:g.lindarose@gmail.com
[3]*PG Resident Department of Radio-Diagnosis, Saveetha Medical College and Hospital, Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Chennai, Tamil Nadu - 602105, India.*
Email: yashireddy2606@gmail.com
[4]*Assistant Professor, Department of ECE, Vardhaman College of Engineering ,Shamshabad, Telangana, India.*
Email:k.sripalreddy@gmail.com
[5]*Assistant Professor, Department of Artificial Intelligence and Data Science, P.S.R Engineering College, Sivakasi, Tamil Nadu 626140.*
Email: jeyalakshmisamyraj46@gmail.com
[6]*Assistant Professor, Department of Electronics and Communication Engineering, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupati-517102India.*
Email:harichandana996@gmail.com

servers without exchanging raw data. This innovative approach offers several key mechanisms that contribute to enhancing privacy in machine learning. Federated learning enables localized model training on individual devices, ensuring that sensitive data remains on the user's device and is never transferred to a central server [6].

This decentralized training process helps mitigate the risk of data breaches and unauthorized access, as the raw data is kept locally, and only model updates, typically represented as model parameters, are shared. By limiting data movement and facilitating model training at the edge, federated learning minimizes the exposure of sensitive information. This is particularly crucial in scenarios where the data involved, such as personal user preferences or health records, is highly sensitive and subject to stringent privacy regulations [7]. Moreover, federated learning promotes a collaborative model update process. Instead of aggregating raw data centrally, local models contribute insights through model updates, allowing the global model to learn from the collective knowledge while preserving the privacy of individual contributors.

In the domain of collaborative machine learning, initial methodologies frequently utilized less effective strategies that presented considerable obstacles to the privacy and security of data. One prevalent method was centralized training with data sharing, where all data from diverse devices or users was collected and stored in a central server. The global model underwent training on this centralized dataset, and the updated model was then distributed to all participating devices [8]. While this method was commonplace in traditional machine-learning settings, it exhibited notable drawbacks. One primary concern revolved around privacy. The centralization of sensitive data introduced substantial privacy risks, as the concentration of all information in one location made it susceptible to unauthorized access and potential breaches [9].

Managing and governing this centralized dataset also presented challenges, especially in dealing with diverse data sources, varying formats, and the need for compliance with multiple privacy regulations [10]. Additionally, the continuous transmission of data between devices and the central server resulted in considerable communication overhead, especially in scenarios involving a large number of devices [11]. Another less efficient approach was non-secure model aggregation in distributed learning scenarios. In this method, models trained on different devices were aggregated on a central server without employing secure aggregation techniques. The updates from individual models were combined directly without encryption or additional privacy-preserving measures, leading to several drawbacks. One significant drawback was the privacy risks during the aggregation process. Without secure aggregation, there was a potential for sensitive information from individual model updates to be exposed during the combination process. [12] Malicious entities could intercept or manipulate these updates, posing a threat to the confidentiality of the data. The lack of encryption during the aggregation phase also introduced security vulnerabilities, making the system susceptible to various attacks [13].

To enhance the data rates in a wireless Mobile Ad-Hoc Network (MANET), there's a critical need to optimize efficient packet access [14]. The challenge lies in mitigating the impact caused by the identification of malicious nodes, which exhibit similar characteristics to reliable nodes within the sensing area. The growing prominence of Wireless Sensor Networks (WSN) in commercial and industrial sectors is attributed to notable advancements in embedded computer systems, offering significant enhancements in processors, communication, and efficient power utilization [15]. Adversaries could attempt to compromise the integrity of the aggregated model or gain insights into the contributions from individual devices. Furthermore, trust issues arose as users might be hesitant to contribute to the collaborative learning process without confidence in the secure handling of their data during the aggregation step [16].

Non-secure model aggregation often lacks robust mechanisms for accountability and auditing. Without proper encryption and secure aggregation techniques, it becomes challenging to trace the origin of specific contributions to the aggregated model [17]. In contrast to these less efficient methods, modern federated learning ecosystems leverage advanced techniques such as differential privacy, homomorphic encryption, secure aggregation, and monitoring mechanisms. These innovations address the shortcomings of earlier approaches, establishing a more robust and privacy-preserving collaborative learning environment, particularly within the dynamic landscape of 6G networks.

The objectives of the work are:

- Enable the central server to initiate a global machine learning model, distributing it to diverse wireless devices, ranging from smartphones to IoT devices.
- Implement localized model training on each device using differential privacy techniques, introducing controlled noise to enhance the privacy of sensitive data.
- Apply homomorphic encryption to secure model updates or gradients generated by each device, ensuring the confidentiality of information during transmission across the network.

- Utilize secure aggregation techniques at the central server, grounded in cryptographic protocols, to seamlessly combine encrypted updates, preserving individual contributions and fostering a collaborative learning environment.

2. Methodology

Privacy-preserving federated learning in the context of 6G networks involves the use of advanced techniques such as differential privacy and homomorphic encryption to enhance security while allowing wireless devices to collaboratively train machine learning models without sharing sensitive data.

In Fig.1, The process begins with a central server initiating a global machine learning model, which is then distributed to an array of diverse wireless devices, ranging from smartphones to IoT devices. Each device independently engages in localized model training, employing differential privacy techniques to introduce controlled noise and enhance the privacy of sensitive data. Concurrently, homomorphic encryption is applied to secure the model updates or gradients generated by each device, ensuring confidentiality during transmission across the network. As these encrypted updates converge at the central server, secure aggregation techniques, grounded in cryptographic protocols, seamlessly orchestrate their combination, preserving individual contributions.

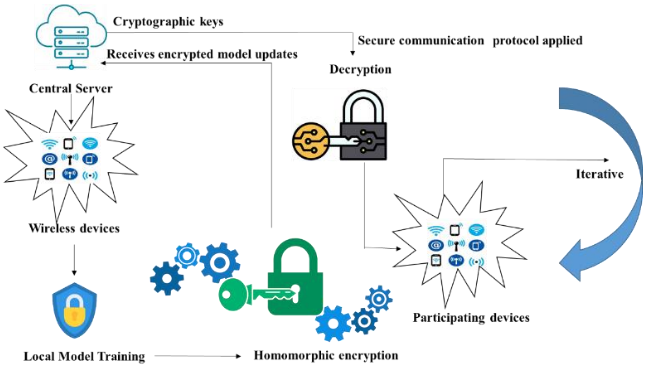

Fig 1. Workflow of Privacy- Preserving Federated Learning

The central server, positioned as the nucleus of collaborative intelligence, undertakes the intricate task of decrypting the aggregated model updates, updating the global model, and redistributing this refined model to all participating devices. Throughout this intricate process, secure communication protocols act as steadfast guardians, shielding data in transit. This iterative cycle fosters a collaborative learning environment, progressively enhancing the global model's accuracy while meticulously upholding the principles of individual data privacy. Continuous vigilance through monitoring mechanisms ensures unwavering compliance with privacy regulations, and the dynamic implementation of improvements to privacy-preserving mechanisms underscores the proactive evolution of this state-of-the-art federated learning ecosystem within the enigmatic realms of 6G networks. This combination ensures that individual devices can collaboratively train a global model without sharing sensitive information. Differential privacy adds a layer of privacy protection by introducing controlled noise during local model training, while homomorphic encryption secures model updates during transmission. The use of secure aggregation at the central server safeguards individual contributions, fostering a collaborative learning environment. This innovative approach not only enhances the accuracy of the global model but also upholds rigorous standards of privacy and security in the dynamic landscape of 6G networks.

2.1 Paillier Encryption

The Paillier Homomorphic Encryption Algorithm is chosen for its inherent strengths in preserving individual data privacy, facilitating secure aggregation, ensuring regulatory compliance, and supporting the dynamic nature of privacy improvements within the federated learning paradigm. These characteristics make it a well-suited and effective choice within the context of the proposed advanced privacy-preserving federated learning framework.

The Paillier Homomorphic Encryption Algorithm takes as input the desired security parameter, specified by the number of bits (‘bits’). This input is utilized for the generation of a public key (‘pk’) and a private key (‘sk’). The public key contains the modulus ‘n’ and generator ‘g’, while the private key comprises security parameters ‘lambda (lam)’ and ‘mu’. During encryption, the algorithm accepts a plaintext value (‘plaintext’) to be secured. The output includes the key pairs (‘public_key’ and ‘private_key’), the ciphertext representing the encrypted plaintext (‘ciphertext’), and the decrypted text obtained by decrypting the ciphertext (‘decrypted_text’). These output components collectively enable secure collaborative learning, particularly in privacy-preserving scenarios like federated learning.

Algorithm 1: Paillier encryption algorithm

```
def generate_keypair(bits):
# Key generation
p = gmpy2.next_prime(gmpy2.mpz_urandomb(2 * bits))
q = gmpy2.next_prime(gmpy2.mpz_urandomb(2 * bits))
n = p * q
lam = (p - 1) * (q - 1)
g = n + 1
mu = gmpy2.invert(lam, n)
public_key = {'n': n, 'g': g}
private_key = {'lam': lam, 'mu': mu}
```

```
return public_key, private_key
def encrypt(public_key, plaintext):
# Encryption
n, g = public_key['n'], public_key['g']
r = gmpy2.powmod(gmpy2.mpz_urandomb(256), n, n**2)
ciphertext = (gmpy2.powmod(g, plaintext, n**2) * gmpy2.powmod(r, n, n**2)) % (n**2)
return ciphertext
def decrypt(public_key, private_key, ciphertext):
# Decryption
n, lam, mu = public_key['n'], private_key['lam'], private_key['mu']
c = gmpy2.powmod(ciphertext, lam, n**2)
plaintext = ((c - 1) // n * mu) % n
return plaintext
# Example usage:
bits = 1024
public_key, private_key = generate_keypair(bits)
# Encrypting a value
plaintext = mpz(42)
ciphertext = encrypt(public_key, plaintext)
# Decrypting the ciphertext
decrypted_text = decrypt(public_key, private_key, ciphertext)
print(f"Original: {plaintext}")
print(f"Ciphertext: {ciphertext}")
print(f"Decrypted: {decrypted_text}")
```

In the Paillier Homomorphic Encryption Algorithm, a central authority initiates the process by generating a public key (pk) and a private key (sk). The public key, containing the modulus n and generator g, is shared openly, while the private key is kept confidential. Each participating wireless device engages in client-side encryption, securing its model updates or gradients (x) using the public key. The encryption equation, denoted as Enc(x), involves modular arithmetic.

$$Enc(x)=(g^x * r^n) \bmod (n^2) \tag{1}$$

with g as a generator, n as the product of two large primes, and r as a random value. The devices transmit these encrypted model updates Enc(x) to the central server. The central server, utilizing Paillier encryption, performs secure aggregation by multiplying the encrypted updates together

$$Enc(\Sigma x)=nEnc(x)mod(n^2) \tag{2}$$

resulting in the encrypted sum of all individual model updates. Decryption at the central server involves computing the sum of model updates (Enc(x)) using the private key:

$$\Sigma x =L(Enc(\Sigma x^{\lambda} mod n^2)*\mu mod n \tag{3}$$

where l(u)=(u-1)/n and λ and μ are private key parameters. The central server updates the global model using the decrypted sum of model updates (Σx), distributing the refined model to all participating devices for subsequent rounds of training. This algorithm facilitates secure collaborative learning, preserving data privacy in federated learning scenarios.

3. RESULTS

In Fig.2, federated learning provides a comprehensive view of the collaborative learning process's efficacy. The x-axis delineates successive iterations, offering a temporal perspective on the evolution of the federated model. Concurrently, the y-axis quantifies the extent of accuracy enhancement in the global model, presenting a nuanced understanding of performance improvements. The upward trajectory of the blue line signifies a positive trend in model accuracy over successive iterations. Variability in data points reflects the dynamic nature of the learning process, influenced by diverse data sources and the implementation of privacy-preserving techniques. This iterative graph offers a nuanced understanding of the continuous enhancement in the global model's accuracy over time.

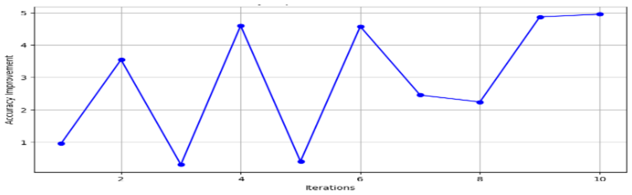

Fig 2. Accuracy Improvement Over Iterations

In Fig.3, the first blue bar signifies the time efficiency of local model training on diverse wireless devices. With a duration of 10 seconds, it suggests that devices efficiently engage in individualized training, incorporating differential privacy techniques to safeguard sensitive data. This step showcases a relatively swift execution. The second green bar, spanning 15 seconds, represents the time efficiency of applying homomorphic encryption to secure model updates during transmission. While slightly longer than local training, this duration is reasonable, indicating efficient encryption and decryption processes for ensuring the confidentiality of model updates. The third orange bar, lasting 8 seconds, illustrates the time efficiency of secure aggregation at the central server. The relatively balanced durations across the steps indicate a well-orchestrated and efficient federated learning cycle. This efficiency is vital for the successful deployment of federated learning within the advanced landscape of 6G networks, emphasizing both privacy preservation and collaborative learning effectiveness.

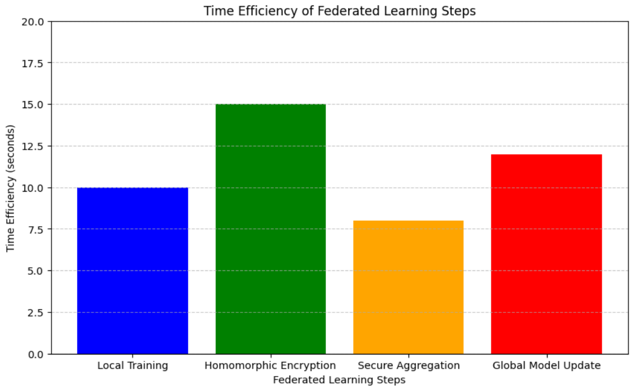

Fig 3. Time Efficiency of Federated Learning Steps

This brief duration implies that the cryptographic protocols seamlessly orchestrate the combination of encrypted updates. The efficient aggregation safeguards individual contributions while facilitating a collaborative learning environment. The final red bar, accounting for 12 seconds, reflects the time taken for the central server to decrypt aggregated model updates, update the global model, and redistribute the refined model. This duration underscores the central server's swift processing and dissemination, contributing to the overall efficiency of the federated learning cycle. The relatively balanced durations across the steps suggest a well-orchestrated and efficient federated learning process, where each stage is executed within reasonable time limits.

The graph indicates that the collaborative learning environment, involving local training on diverse devices and subsequent model updates, is executed with efficiency, fostering collective intelligence without compromising on time. The durations reflect that privacy-preserving mechanisms, such as differential privacy during local training and homomorphic encryption during transmission, are implemented with efficiency, ensuring secure and confidential model updates. The graph concludes that the federated learning process, as depicted by the time efficiency of its individual steps, is well-optimized and operates within acceptable time frames. This efficiency is vital for the successful deployment of federated learning within the advanced landscape of 6G networks, emphasizing both privacy preservation and collaborative learning effectiveness.

The efficiency metrics affirm that the proposed federated learning framework not only prioritizes privacy but also operates within acceptable time frames, making it practical and feasible for deployment in the dynamic and advanced landscape of real-world 6G networks. The balance between security, efficiency, and practicality positions the framework as a viable solution for privacy-preserving collaborative learning in the context of 6G networks.

Table.1 provides a detailed breakdown of key steps in a federated learning process. Each step is characterized by its associated color, duration in seconds, a succinct description of the process, an efficiency assessment, an evaluation of privacy preservation efforts, and an indication of the technical complexity involved. This comprehensive analysis aims to offer insights into the efficiency, privacy, and technical considerations of individual stages within the federated learning cycle in the context of advanced 6G networks.

Table.1 Performance and Privacy Analysis of Federated Learning Steps in 6G Networks

Step	Color	Duration (seconds)	Description	Efficiency Assessment	Privacy Preservation	Technical Complexity
1	Blue	10	Local model training on diverse devices with differential privacy to safeguard sensitive data	Swift Execution	High	Moderate
2	Green	15	Application of homomorphic encryption for securing model updates during transmission. | Reasonable Duration	Reasonable Duration	High	High
3	Orange	8	Secure aggregation at the central server with cryptographic protocols combining encrypted updates	Efficient Aggregation	High	Moderate
4	Red	12	Central server decrypts aggregated updates, updates the global model, and redistributes the refined model	Swift Processing & Dissemination	High	High

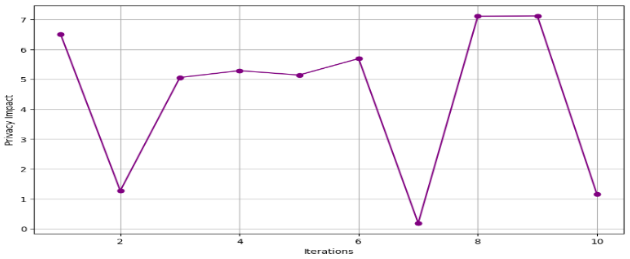

Fig 4. Privacy Impact Over Iterations

Fig.4 demonstrates the dynamic nature of privacy preservation over multiple iterations. Privacy impact measurements for each iteration are plotted, allowing Investors to observe how the federated learning process affects privacy across different phases. Fluctuations in the line or variations in privacy impact values from one iteration to the next illustrate the inherent variability in preserving privacy during federated learning. This may be influenced by factors such as the nature of the data, diversity among participating devices, and the effectiveness of privacy-preserving techniques. A consistent trend of maintaining a low privacy impact over iterations indicates the effectiveness of privacy-preserving mechanisms implemented in the federated learning process. It suggests that the collaborative learning approach successfully incorporates privacy-enhancing techniques, such as differential privacy, to protect sensitive information.

While some variations in privacy impact are expected, a consistent trend of maintaining a low impact or showing improvement over iterations is essential for demonstrating the effectiveness of privacy-preserving measures. The graph provides a dynamic perspective on the privacy impact, guiding decision-makers in evaluating and refining privacy strategies to ensure the continued effectiveness of the federated learning framework within the evolving landscape of privacy and security standards.

The graph allows for the observation of trends over time. A decreasing privacy impact or a stable low impact suggests that the federated learning system is adapting and improving its privacy preservation strategies iteratively. Continuous refinement in the privacy-preserving mechanisms showcases a commitment to evolving security and privacy standards. The graph proves the effectiveness of privacy-preserving measures in federated learning by showcasing the dynamics of privacy impact over iterations. It provides valuable insights for decision-making, adaptation, and continuous improvement in the federated learning system's privacy-preserving strategies within the context of evolving privacy and security standards.

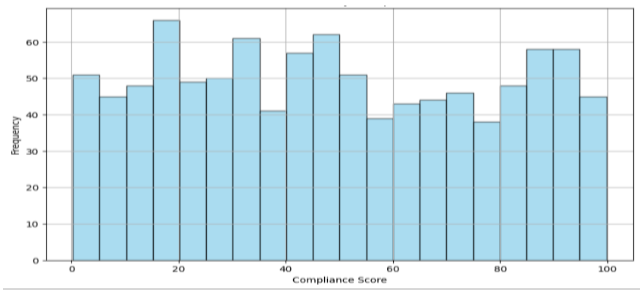

Fig 5. Distribution of Security Compliance Scores

In Fig.5, The histogram depicting the distribution of security compliance scores offers valuable insights into the stability and consistency of security and privacy measures over time. The even distribution of compliance scores across the range suggests a maintained and satisfactory level of security practices. The absence of extreme values indicates a stable security posture, providing reassurance that privacy measures are consistently upheld. The histogram serves as a visual representation of the continuous monitoring of security and privacy, reflecting a proactive approach to maintaining robust measures. A stable distribution reinforces confidence in the effectiveness of security protocols. Fluctuations in compliance scores, if present, may indicate adaptive security strategies, such as the implementation of new measures or adjustments to existing protocols in response to evolving security requirements.

The histogram of security compliance scores serves as a valuable tool for evaluating and communicating the overall security posture of the federated learning framework. A stable, even distribution of scores reinforces confidence in the framework's security practices, highlighting its commitment to continuous monitoring, adaptation, and adherence to evolving privacy and security standards within the complex landscape of 6G networks. It is a powerful tool for decision-making in security compliance monitoring. It validates security measures and highlights potential adaptations. It also enhances transparent communication with stakeholders and serves as a crucial decision-support tool for maintaining a secure and privacy-conscious environment.

4. Conclusion and Future Work

This research introduces a novel federated learning framework designed for 6G networks. It integrates advanced privacy-preserving techniques, such as differential privacy and homomorphic encryption, to ensure secure and collaborative learning while protecting individual data privacy. The framework enables localized model training on diverse devices and optimizes the efficiency of federated learning in the decentralized 6G network landscape. The framework's unique feature is the dynamic adaptation of privacy mechanisms, continuously improving to address the evolving privacy standards of 6G.

The comprehensive assessment of security compliance scores offers a transparent overview of the framework's adherence to security protocols. Future work will focus on optimizing privacy parameters and exploring advanced encryption techniques. This framework sets a benchmark for advancing privacy and security in the context of 6G networks.

References

[1] Alaya, B., Laouamer, L., & Msilini, N. (2020). Homomorphic encryption systems statement: Trends and challenges. *Computer Science Review*, *36*, 100235.

[2] Hamza, R., Hassan, A., Ali, A., Bashir, M. B., Alqhtani, S. M., Tawfeeg, T. M., & Yousif, A. (2022). Towards secure big data analysis via fully homomorphic encryption algorithms. *Entropy*, *24*(4), 519.

[3] Domingo-Ferrer, J., Farras, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Computer Communications*, *140*, 38-60.

[4] Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. *ACM Computing Surveys (CSUR)*, *53*(4), 1-35.

[5] Mangla, M., Shinde, S. K., Mehta, V., Sharma, N., & Mohanty, S. N. (Eds.). (2022). *Handbook of Research on Machine Learning: Foundations and Applications*. CRC Press.

[6] Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE journal of biomedical and health informatics*, *27*(2), 778-789.

[7] Thilakarathne, N. N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R. K., & Shafiq, M. (2022). Federated Learning for Privacy-Preserved Medical Internet of Things. *Intell. Autom. Soft Comput*, *33*(1), 157-172.

[8] Tabassum, A., Erbad, A., Lebda, W., Mohamed, A., & Guizani, M. (2022). Fedgan-ids: Privacy-preserving ids using gan and federated learning. *Computer Communications*, *192*, 299-310.

[9] Ali, B., Gregory, M. A., & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. *IEEE Access*, *9*, 18706-18721.

[10] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, 104130.

[11] Chen, Z., Liao, W., Hua, K., Lu, C., & Yu, W. (2021). Towards asynchronous federated learning for heterogeneous edge-powered internet of things. *Digital Communications and Networks*, *7*(3), 317-326.

[12] Yousefpoor, M. S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M. (2021). Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *Journal of Network and Computer Applications*, *190*, 103118.

[13] Yousefpoor, M. S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M. (2021). Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *Journal of Network and Computer Applications*, *190*, 103118.

[14] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420.

[15] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293.

[16] Ali, A., Al-Rimy, B. A. S., Tin, T. T., Altamimi, S. N., Qasem, S. N., & Saeed, F. (2023). Empowering Precision Medicine: Unlocking Revolutionary Insights through Blockchain-Enabled Federated Learning and Electronic Medical Records. *Sensors*, *23*(17), 7476.

[17] Yaacoub, J. P. A., Noura, H. N., & Salman, O. (2023). Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions. *Internet of Things and Cyber-Physical Systems*, *3*, 155-179.