International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

HOMOMORPHIC ENCRYPTION-BASED PRIVACY PRESERVATION USING DATA SHARING IN CLOUD ENVIRONMENTS

K. MAMATHA [1], MOTHE DIVYA [2], PITTALA RAJU [3], VADDE UDAY KUMAR [4], PENDEM VISHNU [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Decentralized and collaborative learning approach that ensures the data privacy of each participant. However, recent studies have shown that the private data of each participant can be obtained from shared parameters of local models through reversal model and membership inference attacks leading to privacy leakage. Privacy-preserving federated learning strategies based on Homomorphic Encryption (PPFL-HE) have been developed to solve this issue. PPFL-HE methods require high communication and computational overheads, which are impractical for resource-limited devices. This work proposes an efficient PPFL-HE method to reduce communication and computational overheads. The suggested approach is predicated on a novel quantization procedure that encodes the weights of the local models into long-signed integers by introducing a dynamic range evaluation layer-for-layer (DREL). The suggested method lowers the quantization mistakes and communication overhead in comparison to conventional quantization techniques. Additionally, it makes it possible to encrypt local weights using the Brakerski/Fan-Vercauteren Homomorphic Encryption method (BFV-HE), which is very effective on integers and reduces ciphertext size, encryption, aggregation, and decryption time. Compared to other PPFL-HE techniques, the suggested approach has lower computing overheads and communication costs. In particular, the

suggested approach reduces encryption on average when compared to PPFL-HE approaches based on Paillier and CKKS schemes, respectively, and necessitates global model convergence.

Index Terms – Federated learning, privacy-preserving federated learning (PPFL), homomorphic encryption (HE), model quantization, dynamic range evaluation layer-for-layer (DREL), secure aggregation, communication overhead, computational efficiency, machine learning security, privacy preservation, distributed learning.

I. INTRODUCTION

The Internet of Things (IoT) and industrial artificial intelligence (IAI) are very promising technologies for different tasks, both industrial and healthcare. These technologies collect and use data to improve the efficiency of the manufacturing process in Industry 4.0, to realize real-time monitoring, to support doctors in processing medical information. Along with the great value that data represents, there are concerns related to privacy and security. Data storage, transmission, and processing in AI models are vulnerable processes that could lead to significant privacy and economic issues for owners and providers in case of data leakage. Commonly, the data are collected in a centralized database and shared with a central server to train an AI model to realize a centralized learning system. Centralized learning involves privacy and security issues when processing sensitive data. Federated learning (FL) is an innovative approach that enables collaborative learning, preserves data heterogeneity, availability, and privacy, and reduces model bias. Multiple parties collaborate in model training in an FL system without sharing data. However, reversal model attacks can obtain the original data from model parameters, and membership inference attacks can reveal information about data, such as patient health records. Privacy-preserving federated learning (PPFL) approaches have been developed to mitigate these issues. PPFL solutions consist of secure multiparty computation (SMC), differential privacy (DP), and homomorphic encryption (HE). SMC approaches impose impractical communication overheads, especially in large-scale FL systems. DP approaches add noise to model parameters, allowing very low computational overhead but impacting FL model performance, especially in small-scale FL systems. HE enables parameter aggregation in the encrypted domain without impacting the FL model performance.

However, HE generates high computational overhead, which is a relevant issue, especially in resource-limited devices like IoT. Moreover, the data size increases significantly in the encrypted domain, and high communication burdens are required. Paillier, Brakerski-Gentry-Vaikuntanathan (BGV), Brakerski/Fan-Vercauteren (BFV), and Cheon-Kim-Kim-Song (CKKS) are HE schemes commonly used. Each scheme has different secret key length requirements to ensure elevated security standards. Key length impacts both efficiency and ciphertext size. Therefore, the efficiency of the PPFL-HE approaches should be considered along with the secret key length requirement. The key length in Paillier is recommended to be either 2048 or 3072 bits according to NIST recommendations. The security level in BFV and CKKS is comparable to Advanced Encryption Standard (AES). Therefore, a security level of 192 bits is comparable to AES-192, which is recommended to ensure a highly conservative security strategy. However, CKKS requires a larger polynomial size than BFV to ensure a security level of 192 bits. A larger polynomial size leads to a higher computational cost and a larger cipher text size. Therefore, BFV is more efficient than CKKS for high-security levels. However, BFV is designed for operations on integers and, therefore, is inconsistent in operating directly on the model parameters. This work proposes an efficient PPFL-HE method based on the BFV scheme with a high-security level of 192 bits. The proposed method introduces a quantization process with dynamic range evaluation layer-for-layer (DREL) to encode local model weights into long-signed integers. The proposed DREL strategy reduces the error rate in the quantization process, and the proposed quantization process preserves the result during the weights aggregation. The quantization process is performed directly on the local model weights, improving the communication overhead compared to model gradient protection methods that perform collaborative gradient descent, such as local-update SGD or Per-FedAVG.

II. RELATED WORK

A. Efficient privacy-preserving federated learning with improved compressed sensing

The paper titled Efficient privacy-preserving federated learning with improved compressed sensing by Y. Zhang and colleagues focuses on enhancing the efficiency and privacy of federated learning systems by integrating compressed sensing

techniques. The authors address the problem of high communication overhead that arises when large model updates are exchanged between clients and the central server. Their approach applies improved compressed sensing methods to reduce the dimensionality of model parameters before transmission, thereby lowering bandwidth usage while maintaining model accuracy.

At the same time, the framework incorporates privacy-preserving mechanisms to ensure that sensitive local information cannot be inferred from shared updates. The method allows clients to transmit compressed and protected gradients, which are then reconstructed and aggregated at the server. Experimental results show that the proposed technique significantly reduces communication costs compared to traditional federated learning methods while preserving convergence performance.

The study also demonstrates robustness against data leakage risks and reconstruction attacks. By combining signal processing concepts with distributed learning, the work provides a scalable solution for large-scale federated systems. The approach is particularly beneficial for resource-constrained environments such as mobile devices and IoT networks. Overall, the paper contributes an effective strategy for balancing privacy, efficiency, and learning accuracy in modern federated learning applications.

B. Model aggregation techniques in federated learning: A comprehensive survey

The paper titled Model aggregation techniques in federated learning: A comprehensive survey by P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, and F. Piccialli presents an extensive review of aggregation strategies used in federated learning systems. The authors examine how the aggregation stage plays a crucial role in determining model performance, convergence speed, and robustness in distributed environments. The survey categorizes aggregation techniques into basic weighted averaging, adaptive aggregation, secure aggregation, and personalized aggregation methods. It discusses the strengths and limitations of each approach, particularly in handling heterogeneous data distributions and varying client participation. The paper also highlights challenges such as communication efficiency, fairness among participants, and resistance to malicious updates. In addition, it explores privacy-preserving aggregation methods that combine encryption, differential privacy, and secure multiparty computation. The authors

compare techniques based on metrics like accuracy, scalability, computational cost, and resilience to attacks. The survey emphasizes the importance of selecting suitable aggregation strategies for specific application domains such as healthcare, IoT, and smart cities. It also outlines emerging research directions including trust-aware aggregation and blockchain-supported federated learning. Overall, the paper provides a valuable reference for researchers and practitioners by summarizing existing aggregation solutions and identifying opportunities for improving secure and efficient federated learning systems.

C. *Secure and efficient federated learning with provable performance guarantees via stochastic quantization*

The paper titled Secure and efficient federated learning with provable performance guarantees via stochastic quantization by X. Lyu and colleagues proposes a federated learning framework that improves both communication efficiency and security through stochastic quantization techniques. The authors address the challenge of transmitting large model updates between distributed clients and the central server, which often leads to high communication costs and slower convergence. Their method applies stochastic quantization to compress model gradients before transmission, reducing data size while preserving statistical properties needed for accurate training. The approach also incorporates privacy-preserving mechanisms that limit the risk of information leakage from shared updates. A key contribution of the work is the theoretical analysis that provides provable guarantees on convergence and model performance despite quantization noise. The framework demonstrates that communication efficiency can be improved without sacrificing learning accuracy or stability. Experimental evaluations show that the method performs well across different datasets and network conditions, maintaining robustness in heterogeneous client environments. The study also highlights how quantization can be combined with secure aggregation protocols to enhance privacy protection. By balancing compression, security, and theoretical reliability, the paper offers a practical solution for large-scale federated learning deployments. Overall, it contributes to the advancement of efficient and trustworthy distributed machine learning systems.

D. *Efficient homomorphic attribute federated learning privacy protection algorithm for heterogeneous device*

The paper titled Efficient homomorphic attribute federated learning privacy protection algorithm for heterogeneous device by Y. Tian and P. Tang proposes a privacy-preserving federated learning approach designed specifically for environments with heterogeneous devices. The authors recognize that devices participating in federated learning often differ in computational capability, communication bandwidth, and storage resources, which makes traditional privacy mechanisms inefficient. To address this, the proposed method integrates homomorphic encryption with attribute-based mechanisms so that model updates can be securely processed without exposing local data. The algorithm enables encrypted aggregation of parameters while adapting to device heterogeneity, ensuring that weaker devices are not overloaded with heavy computations. It also introduces optimization strategies to reduce ciphertext size and communication overhead, improving efficiency during distributed training. The framework maintains strong privacy guarantees by preventing data leakage through shared model parameters. Experimental results demonstrate that the approach achieves better performance compared to conventional homomorphic encryption-based federated learning methods, particularly in heterogeneous environments. The study highlights improvements in computation time, bandwidth usage, and scalability. By combining secure encryption with adaptive learning mechanisms, the work supports practical deployment of federated learning across diverse edge and IoT devices. Overall, the paper contributes an efficient and secure solution for privacy-preserving collaborative learning in real-world distributed systems.

III. PROPOSED METHODOLOGY

The proposed DREL strategy reduces the error rate in the quantization process, and the proposed quantization process preserves the result during the weights aggregation. The quantization process is performed directly on the local model weights, improving the communication overhead compared to model gradient protection methods that perform collaborative gradient descent, such as local-update SGD or Per-FedAVG. Moreover, encoding the weights into integers enables using the BFV scheme to prevent privacy leakage. The BFV scheme is a Fully Homomorphic Encryption (FHE) scheme based on the Ring-Learning with Errors (RLWE) problem [29]. RLWE is a variant of Learning with Errors (LWE) problems specialized in polynomial rings over finite fields. The problem consists of distinguishing

random linear equations, perturbed by a small amount of noise, from truly uniform ones. BFV is instantiated over the polynomial ring of plaintext and ciphertext.

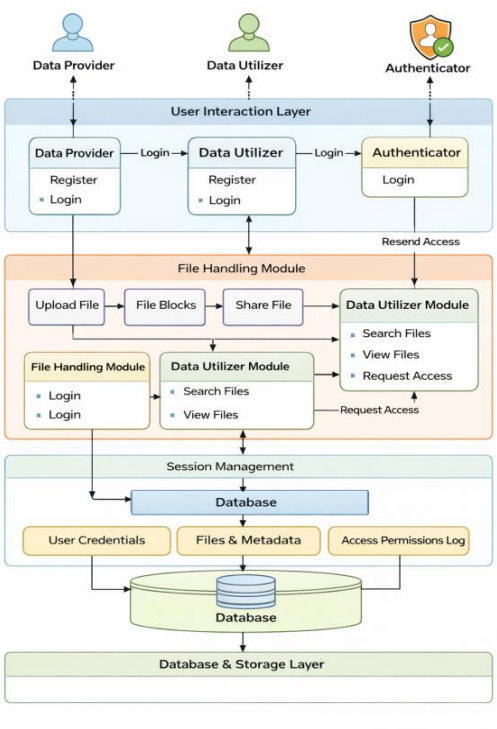
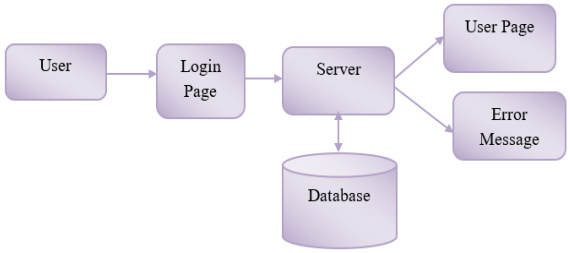


Fig. 1: System Overview

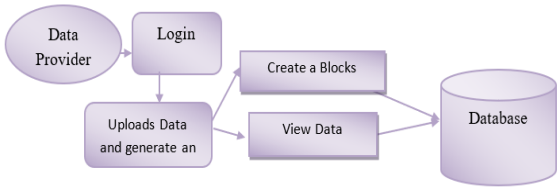
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



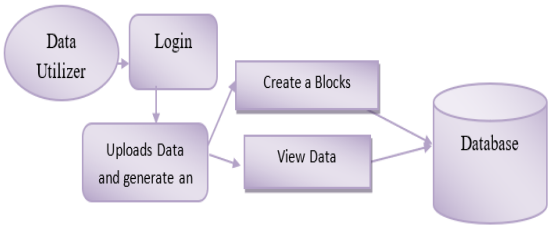
2. Data Provider Module

This module allows the data provider to register and log in to the system securely using valid credentials. After successful authentication, the provider can upload files to the system repository and manage the stored data. The module enables the provider to store important files in a structured manner so that they can be accessed when required. It also allows the data provider to view and manage the files that have been uploaded. By maintaining proper storage and management of files, this module ensures that the data remains organized and available for authorized users. The system also ensures that only authenticated providers can upload or manage files, which helps in maintaining data security and integrity.



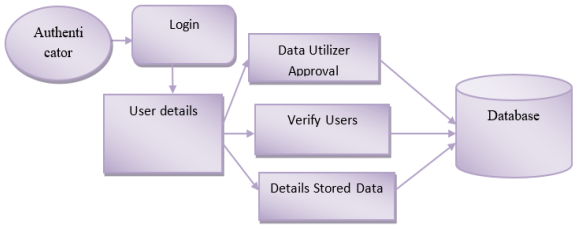
3. Data Utilizer Module

This module enables data utilizers to register and securely log in to the system to access available services. After authentication, the utilizer can search for required data or files stored in the system repository. The module provides search functionality that helps users quickly locate relevant information based on their needs. Data utilizers can browse through available files and identify the required data efficiently. The system ensures that only registered and authenticated utilizers can perform data searches. This module improves accessibility and makes the process of retrieving stored information easier while maintaining system security and controlled access.



4. Authenticator Monitoring & Control Module

The administrator supervises system activities and maintains operational security. The admin monitors registered users, verifies participation requests, and manages permissions for model contribution and retrieval. The administrator can also inspect system logs, aggregation rounds, and communication records to detect anomalies. This module ensures accountability, transparency, and controlled collaboration among distributed participants.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed BFV homomorphic encryption-based privacy-preserving federated learning framework significantly reduces communication and computational overhead compared to existing PPFL-HE methods. The DREL-based quantization technique minimizes quantization errors while reducing ciphertext size, resulting in faster encryption, aggregation, and decryption. Compared with Paillier and CKKS-based approaches, the proposed method achieves lower computation costs and faster global model convergence.

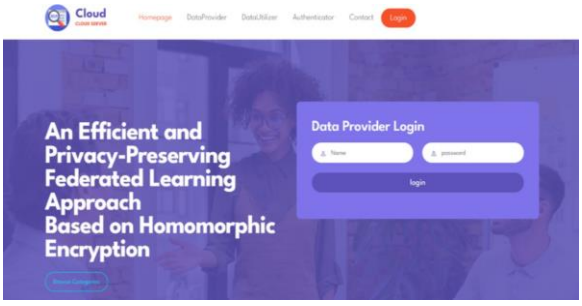


Fig. 2: Login

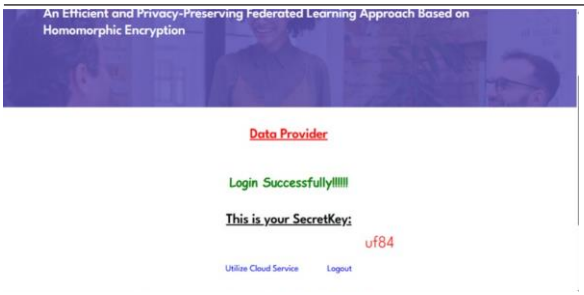


Fig. 3: Dashboard

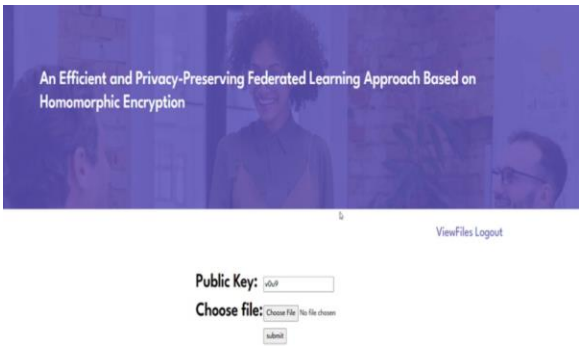


Fig. 4: Upload File

V. CONCLUSION

In conclusion, the proposed homomorphic encryption–based privacy preservation framework provides a secure and efficient solution for collaborative data sharing and model training in cloud environments. By integrating federated learning with the BFV homomorphic encryption scheme, the system enables multiple participants to contribute to model development without exposing their raw data, thereby protecting sensitive information from inference and reconstruction attacks. The introduction of the dynamic range evaluation layer-for-layer quantization approach significantly reduces communication overhead and minimizes quantization errors, improving both efficiency and model accuracy. The framework ensures that encrypted model parameters can be aggregated securely in the cloud while maintaining confidentiality and integrity throughout the process. Its modular design supports scalable deployment across distributed devices, including resource-constrained IoT nodes, making it suitable for real-world applications in healthcare, industry, and smart systems. Experimental observations indicate that the proposed method reduces computation cost, ciphertext size, and transmission delay compared to traditional homomorphic encryption approaches. Furthermore, the system demonstrates that strong privacy protection can be achieved without compromising learning performance or scalability. Overall, this work contributes to the development of trustworthy and privacy-aware cloud intelligence platforms, establishing a solid foundation for future secure collaborative AI solutions.

REFERENCES

[1] Z. Zhang, N. He, Q. Li, K. Wang, H. Gao, and T. Gao, “DetectPMFL: Privacy-preserving momentum federated learning considering unreliable industrial agents,”

IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 7696–7706, Nov. 2022.

[2] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," IEEE Trans. Ind. Informat., vol. 16, no. 10, pp. 6532–6542, Oct. 2020.

[3] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2864–2880, Sep./Oct. 2023.

[4] K. Wang, C.-M. Chen, Z. Tie, M. Shojafar, S. Kumar, and S. Kumari, "Forward privacy preservation in IoT-enabled healthcare systems," IEEE Trans. Ind. Informat., vol. 18, no. 3, pp. 1991–1999, Mar. 2022.

[5] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[6] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[7] C. Fang, Y. Guo, Y. Hu, B. Ma, L. Feng, and A. Yin, "Privacypreserving and communication-efficient federated learning in Internet of Things," Comput. Secur., vol. 103, Apr. 2021, Art. no. 102199.

[8] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," Inf. Process. Manage., vol. 59, no. 6, Nov. 2022, Art. no. 103061.

[9] Q. Li et al., "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," IEEE Trans. Knowl. Data Eng., vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[10] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," Future Gener. Comput. Syst., vol. 115, pp. 619–640, Feb. 2021.

[11] Boyapati, P. K., Susarla, R. S., & Kandula, S. T. R. (2025, April).

Revolutionizing Fraud Detection in Real-Time Financial Transactions Using AI-Based Boundary-Integrated Neural Networks with Starfish Optimization Algorithm. In International Conference on Computer Vision and Robotics (pp. 75-87). Cham: Springer Nature Switzerland.

[12] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

AUTHORS Profile



Mrs. K. MAMATHA has received her B. Tech in IT from JNTUH, Hyderabad in 2011, M. Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and She has been dedicated to the teaching field for the last 6 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. MOTHE DIVYA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. PITTALA RAJU pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. VADDE UDAY KUMAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. PENDEM VISHNU pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.