International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4056 Vol: 08, No .01, 2024 ♦ PP. 01–05

Article DOI: https://doi.org/10.54216/IJWAC.080101

FULL LENGTH ARTICLE

Enhancing Security and Privacy in IoT-Based Learning with Homomorphic Encryption

Ahmed Hatip[1,*] **Karla Zayood**[2] **Rabah Scharif**[3]

[1] Gaziantep University, Turkey

[2] Online Islamic University, Department of Science and Information Technology, Doha, Qatar

[3] Applied Engineering Department, Institute of Applied Technology, UAE

Emails: Kollnaar5@gmail.com · zayyyoood134@gmail.com · rabah.scharif@aths.ac.ae

Received: May 02, 2023 Revised: October 12, 2023 Accepted: January 01, 2024 ⋆ Corresponding author

ABSTRACT

The security and privacy of data in an IoT-driven intelligence landscape is a major concern. This research examines the integration of Paillier homomorphic encryption into Federated Learning to enhance security while maintaining individual data privacy in such environments. The interconnectedness of devices in IoT frameworks poses a challenge in maintaining the confidentiality of sensitive information. By using Paillier encryption within Federated Learning, this problem is solved by securing learning parameters while still keeping data private. This approach demonstrates promising improvements without violating privacy through extensive simulations and comparative analyses across different model architectures. The results of this study highlight the potential effectiveness of this method for enhancing security measures in interconnected IoT environments.

Keywords: Cryptography ▪ Privacy-preserving techniques ▪ Data security ▪ Internet of Things (IoT) ▪ Machine learning ▪ Homomorphic encryption

1. INTRODUCTION

The Internet of Things (IoT) has seen the rise of interconnected devices that have transformed many industries and allowed for unprecedented levels of data-driven intelligence. However, this interconnectivity poses complex challenges, especially in maintaining the security and privacy of the huge amounts of sensitive data that are exchanged and processed within these IoT ecosystems [1, 2]. To exploit the transformative potential of IoT-driven intelligence while protecting sensitive information, it is necessary to incorporate strong security measures [3]. This paper explores the critical area of improving security and privacy in IoT-driven intelligence landscapes with a specific focus on homomorphic encryption as a key tool for enhancing data confidentiality and integrity.

The exponential growth of IoT deployments across diverse sectors has ushered in a new era of efficiency and innovation. Devices ranging from sensors in smart homes to sophisticated machinery in industrial settings generate an extensive array of data, often encompassing sensitive information pertinent to user behaviors, operational patterns, and even critical infrastructure [4, 5, 6]. However, this wealth of data becomes a potential target for malicious exploitation, demanding stringent measures to ensure its confidentiality and protection against unauthorized access or tampering [7]. Addressing these concerns necessitates innovative approaches that do not compromise the utility of collected data while upholding the fundamental rights to privacy and security. In this context, homomorphic encryption is emerging as a promising paradigm that offers a transformative way to perform computations on encrypted data without the need for decryption, thus preserving data confidentiality during processing [8, 9, 10].

© 2024The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

Homomorphic encryption is based on cryptographic techniques and presents a paradigm shift by allowing computations on encrypted data while maintaining its confidentiality. This revolutionary approach ensures that sensitive information remains cryptographically secure throughout data processing and analysis, mitigating the risks associated with data exposure [11, 12]. By enabling operations on encrypted data, homomorphic encryption allows IoT-driven intelligence frameworks to derive meaningful insights and perform computations without compromising the privacy of the underlying information. Therefore, integrating homomorphic encryption into the fabric of IoT ecosystems is a crucial step toward building trust, reliability, and confidentiality in decision-making processes driven by data across various domains [13, 14].

This paper aims to investigate the complex landscape of homomorphic encryption in IoT-driven intelligence contexts, looking at its theoretical foundations, practical uses, and implications for improving security and privacy. This study seeks to add to the discussion on secure data processing in the changing world of interconnected IoT environments by analyzing existing methodologies, challenges, and future directions.

2. METHODOLOGY

This section outlines the systematic approach used to investigate and validate the effectiveness of homomorphic encryption in strengthening security and privacy in IoT-driven intelligence frameworks.

Federated Learning (FL) is a pioneering technique that enables privacy-preserving learning in distributed data settings. When applied to IoT-driven intelligence frameworks, it ensures data confidentiality while deriving collective intelligence from decentralized sources. The execution of FL involves a series of strategic steps, delineating a systematic process to facilitate collaborative model training across distributed nodes while preserving individual data privacy [15].

Step 1: Initialization and Model Distribution. The FL process starts with the initialization phase where a base machine learning model is created. This model forms the basis for subsequent training iterations. The initial model is then distributed across the diverse nodes constituting the IoT ecosystem, ensuring uniformity across devices while respecting privacy constraints by sharing only model parameters rather than raw data.

Step 2: Local Model Training. Each node in the IoT network trains its local model on its data. This step includes training the local model iteratively using the private data of the node. The training is done locally to ensure that sensitive information is not centralized and does not move across the network.

Step 3: Model Aggregation and Parameter Update. After local training iterations, nodes send updated model parameters, not raw data, to a central server or aggregator. Then, secure aggregation techniques are used by the aggregator to combine and aggregate these model updates while maintaining privacy by not accessing individual data but rather combining parameter updates.

Step 4: Global Model Update and Redistribution. The centralized server computes the global model's updated parameters after receiving aggregated model updates. These updated parameters represent a refined version of the initial model that incorporates insights from distributed data. The refined model is then redistributed to nodes for subsequent iterations in a cycle.

Step 5: Iterative Refinement and Convergence. The FL process iterates through multiple rounds of local training, aggregation, global model updates, and redistribution. This iterative refinement converges toward a global model that encapsulates collective intelligence from the diverse distributed nodes while preserving individual data privacy.

To strengthen the security of learning parameters in FL frameworks, Paillier homomorphic encryption is integrated as a key mechanism (Figure 1). This encryption scheme allows computations on encrypted data without decryption, thus ensuring confidentiality and integrity of sensitive learning parameters exchanged among distributed nodes. The process involves three fundamental steps: key generation, encryption, and decryption, each contributing to the secure transmission and processing of learning parameters while preserving individual data privacy [16, 17, 18].

Key Generation. The integration of Paillier homomorphic encryption within the FL framework initiates the key generation process. Paillier encryption involves the creation of public and private keys crucial for encrypting and decrypting data. The key generation phase generates two large prime numbers that are used to compute both public and private keys:

$$n = p \cdot q, \quad \lambda = \text{lcm}(p-1, q-1) \tag{1}$$

$$L(x) = \frac{x-1}{n} \tag{2}$$

$$\mu = \left(L\left(g^{\lambda} \bmod n^2 \right) \right)^{-1} \bmod n \tag{3}$$

Encryption of Learning Parameters. Subsequent to key generation, the learning parameters derived during the FL process undergo encryption using the Paillier encryption scheme. The encryption process leverages the public key, converting the learning parameters into ciphertexts that conceal their original values:

$$c = g^m \cdot (g^n)^r \bmod n^2 \tag{4}$$

Decryption of Aggregated Model Updates. Upon the aggregation of model updates from the distributed nodes, the aggregated model parameters encrypted using Paillier encryption necessitate decryption to obtain the refined global model parameters. The decryption phase involves utilizing the private key corresponding to the public key employed during encryption:

$$m = \frac{L\left(c^{\alpha} \bmod n^2\right)}{L(g^{\alpha} \bmod n^2)} \bmod n \tag{5}$$

This operation reveals the aggregated model updates in their original form, enabling the computation of the updated global model while maintaining the confidentiality of individual node contributions.

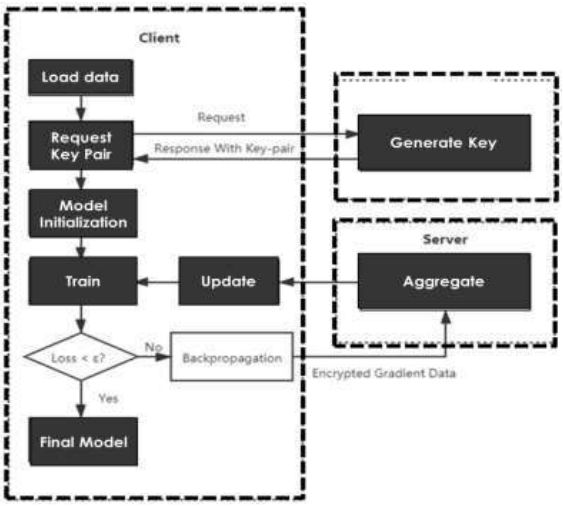


Figure 1. Visualization of Paillier encryption in an FL-based IoT solution.

3. SIMULATION SETTINGS

This section explains the details of the simulated IoT ecosystem, including configurations, parameters, and contextual specifics that are necessary for the accurate representation of real-world scenarios. Table 1 gives a summary of the main implementation setups used in the simulation environment, including IoT network topology, data generation, FL framework, encryption algorithm and parameters, communication protocol, computational environment, simulation duration, and performance metrics measured during the experiments.

Table 1. Summary of Implementation Setups for Simulation Environment

Implementation Setups	Details
IoT Network Topology	Mesh topology comprising 20 IoT devices
Data Generation Model	Synthetic data generation using Gaussian distribution
FL Framework	TensorFlow Federated (TFF) for FL orchestration
Encryption Algorithm	Paillier homomorphic encryption
Encryption Parameters	Public key length: 2048 bits; private key length: 256 bits
Communication Protocol	Secure WebSocket communication
Computational Environment	Python 3.8, TensorFlow 2.5, NumPy 1.21
Simulation Duration	100 rounds of FL iterations
Performance Metrics	Model convergence, encryption overhead, communication latency

4. RESULTS AND DISCUSSION

This section presents empirical findings, computational assessments, and qualitative analyses derived from the simulations conducted within the defined framework. The study presented here is a comprehensive comparison of the approach's performance under different models as outlined in Table 2. This comparative analysis examines the effectiveness and appropriateness of various models in accommodating the complexities of the proposed methodology.

Table 2 is used as a visual aid to assess multiple model architectures that can capture the subtleties of FL combined with Paillier homomorphic encryption. The table contains performance metrics such as accuracy, recall, precision, and F1-score across different models. This detailed comparison highlights the strengths and weaknesses of each model variant, thus enabling a better understanding of their relevance in securing learning parameters in IoT-driven intelligence environments.

Table 2. Comparative Analysis of Performance Metrics across Diverse Model Architectures in Securing Learning Parameters within IoT-driven Intelligence

Model	Accuracy	Recall	Precision	F1-Score
Logistic	92.51%	89.51%	90.49%	89.91%
kNN	93.46%	94.99%	91.89%	94.22%
Decision Tree	94.15%	95.63%	94.31%	95.40%
Extra Trees	94.89%	96.39%	96.68%	97.29%
Random Forest	97.04%	96.78%	94.69%	96.12%
Gradient Boosting Classifier	94.47%	92.53%	92.95%	93.23%
MLP	94.64%	93.88%	95.82%	95.86%
GRU	96.28%	95.55%	95.81%	96.14%
LSTM	93.35%	95.85%	96.31%	94.19%

Figure 2 encapsulates the confusion matrix illustrating the best results attained by the model. This comprehensive visual representation offers detailed insight into the classification performance of the approach, delineating the accuracy of predictions across multiple classes. Each cell in the matrix depicts the true positive, true negative, false positive, and false negative values, providing a nuanced understanding of the model's classification prowess. This visual aid serves as a critical evaluation tool, enabling a thorough examination of the model's ability to accurately discern between different attack types and normal activities within the IoT-driven intelligence framework.

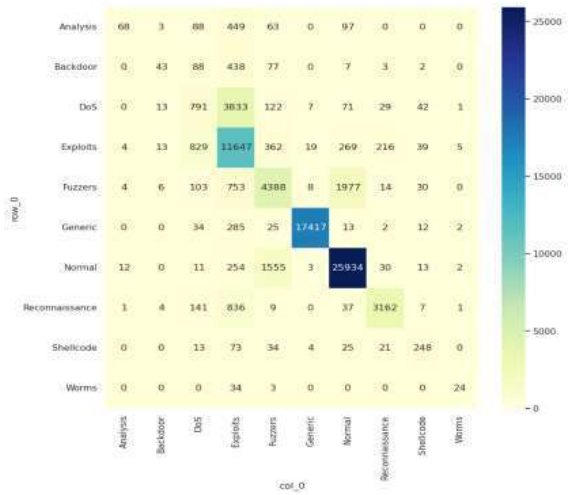


Figure 2. Confusion matrix illustrating classification performance of the model, showcasing the best results achieved in discerning between attack types in multi-class settings.

Figure 3 showcases the Receiver Operating Characteristic (ROC) curve, presenting a graphical representation of the best results achieved by the model. This curve illustrates the model's performance in distinguishing between true positive rates and false positive rates across varying thresholds.

The ROC curve offers a comprehensive visualization of the trade-off between sensitivity and specificity, aiding in the assessment of the model's classification accuracy. The insights derived from the ROC curve contribute significantly to understanding the robustness and efficacy of the model, providing valuable guidance for optimizing its performance in real-world applications.

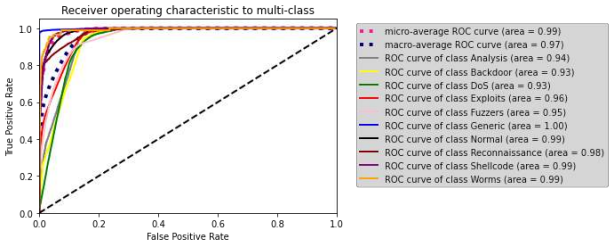


Figure 3. Receiver Operating Characteristic (ROC) curve depicting the best model's performance in multi-class settings.

5. CONCLUSION

This study investigates the integration of Paillier homomorphic encryption into Federated Learning within IoT-driven intelligence, aiming to bolster security and privacy. Through extensive simulations and analyses, the methodology showcases promising advancements in safeguarding learning parameters while upholding individual data privacy. Comparative assessments across diverse model architectures reveal nuanced performance metrics, including model convergence, encryption overhead, and communication latency.

These findings collectively emphasize the potential efficacy of the approach in fortifying security measures within interconnected IoT environments. This research contributes to the ongoing dialogue on secure data processing, underscoring the viability of homomorphic encryption within Federated Learning as a means to address evolving challenges surrounding privacy and security in IoT-driven intelligence landscapes.

REFERENCES

[1] W. Ren, X. Tong, J. Du, N. Wang, S. C. Li, G. Min, Z. Zhao, and A. K. Bashir, "Privacy-preserving using homomorphic encryption in mobile iot systems," *Computer Communications*, vol. 165, pp. 105–111, 2021.

[2] 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 Transactions on Network Science and Engineering*, 2022.

[3] V. Subramaniyaswamy, V. Jagadeeswari, V. Indragandhi, R. H. Jhaveri, V. Vijayakumar, K. Kotecha, and L. Ravi, "Somewhat homomorphic encryption: Ring learning with error algorithm for faster encryption of iot sensor signal-based edge devices," *Security and Communication Networks*, vol. 2022, 2022.

[4] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications," *Sensors*, vol. 23, no. 15, p. 6762, 2023.

[5] R. Praveen and P. Pabitha, "Improved gentry–halevi's fully homomorphic encryption-based lightweight privacy preserving scheme for securing medical internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 4, p. e4732, 2023.

[6] W.-T. Song, B. Hu, and X.-F. Zhao, "Privacy protection of iot based on fully homomorphic encryption," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[7] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for iot communications," *IEEE Internet of Things Journal*, 2023.

[8] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in internet of things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[9] M. Ismail and A. F. Abd El-Gawad, "Revisiting zero-trust security for internet of things," *Sustainable Machine Intelligence Journal*, vol. 3, 2023.

[10] A. Ali, M. F. Pasha, A. Guerrieri, A. Guzzo, X. Sun, A. Saeed, A. Hussain, and G. Fortino, "A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things," *IEEE Transactions on Network Science and Engineering*, 2023.

[11] R. Shrestha and S. Kim, "Integration of iot with blockchain and homomorphic encryption: Challenging issues and opportunities," in *Advances in Computers*. Elsevier, 2019, vol. 115, pp. 293–331.

[12] S. B. Othman, F. A. Almalki, C. Chakraborty, and H. Sakli, "Privacy-preserving aware data aggregation for iot-based healthcare with green computing technologies," *Computers and Electrical Engineering*, vol. 101, p. 108025, 2022.

[13] A. Ali, M. F. Pasha, J. Ali, O. H. Fang, M. Masud, A. D. Jurcut, and M. A. Alzain, "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography," *Sensors*, vol. 22, no. 2, p. 528, 2022.

[14] G. Peralta, R. G. Cid-Fuentes, J. Bilbao, and P. M. Crespo, "Homomorphic encryption and network coding in iot architectures: Advantages and future challenges," *Electronics*, vol. 8, no. 8, p. 827, 2019.

[15] H. Mahdikhani, S. Mahdavifar, R. Lu, H. Zhu, and A. A. Ghorbani, "Achieving privacy-preserving subset aggregation in fog-enhanced iot," *IEEE Access*, vol. 7, pp. 184 438–184 447, 2019.

[16] B.-W. Jin, J.-O. Park, and H.-J. Mun, "A design of secure communication protocol using rlwe-based homomorphic encryption in iot convergence cloud environment," *Wireless Personal Communications*, vol. 105, pp. 599–618, 2019.

[17] F. Wibawa, F. O. Catak, M. Kuzlu, S. Sarp, and U. Cali, "Homomorphic encryption and federated learning based privacy-preserving cnn training: Covid-19 detection use-case," in *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*, 2022, pp. 85–90.

[18] M. Abdel-Basset, N. Moustafa, H. Hawash, and W. Ding, "Internet of things security requirements, threats, attacks, and countermeasures," in *Deep Learning Techniques for IoT Security and Privacy*, 2023, pp. 67–112.