Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1527–1536
DOI : 10.47974/JDMSC-2151

A novel cryptographic approach to evaluate the security of federated learning frameworks

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

Sadashiva V. Chakrasali †
Department of Electronics and Communication Engineering
M S Ramaiah Institute of Technology
MSR Nagar MSRIT Post
Bengaluru
Karnataka
India

Pullela SVVSR Kumar §
Department of Computer Science & Engineering
Aditya University
Surampalem
Andhra Pradesh
India

Sampada Abhijit Dhole ‡
Department of Electronic and Telecommunication
Bharati Vidyapeeth College of Engineering for Women
Pune
Maharashtra
India

* *E-mail:* **dankan.v@bmsit.in (Corresponding Author)**
† *E-mail:* **sadashiva.c@msrit.edu**
§ *E-mail:* **pullelark@yahoo.com**
‡ *E-mail:* **sampada.dhole@bharatividyapeeth.edu**

Jayamala Kumar Patil [@]
Department of Electronics and Telecommunication Engineering
Bharati Vidyapeeth's College of Engineering
Kolhapur
Maharashtra
India

Shivoham Singh [#]
Department of Operations
Symbiosis Institute of Business Management
Symbiosis International (Deemed to be University)
Pune
Hyderabad
India

Abstract

Federated Learning (FL) has turned out to be one of the most useful techniques for enabling distributed machine learning while protecting the data. Thirdly, because FL is distributed, the introduced feature is susceptible to several attacks associated with security. The current paper develops a new cryptographic solution that can enhance the security of FL frameworks. Thus, applying the cryptographic technologies, the employ of the proposed method ensures reliable data protection against the losses and illicit interventions. Experimental evaluations for this strategy are numerous and illustrate how, at the same time, our approach defends FL operations on the practical level while providing performance. It should also be noted how the results can provide a clear depiction to prove how beneficial our cryptographic solution will be in the context of improving the security of federated learning and paving the way for safer and more reliable FL implementations.

Subject Classification (2010): *94A60, 20C05, 20C07.*

Keywords: *Federated learning, Cryptography, Security evaluation, Privacy preservation, Machine learning, Data protection, Distributed systems, Advanced cryptographic, Techniques, Secure aggregation, Adversarial attacks.*

1. Introduction

Federated Learning (FL) is a new generation of machine learning that allows multiple edge devices to jointly learn a common model with their own data remaining on personal devices [1]. This approach greatly improves data protection since clients' data do not have to be consolidated

[@] *E-mail:* **jayamala.p@rediffmail.com**
[#] *E-mail:* **shivohamsingh@gmail.com**

in one area [2]. This makes the use of FL important because it is applied in the healthcare [3], finance [4], IoT and others where data security is of paramount importance., yet the distribution of FL provokes specific security and privacy issues [5]. So, there are risks of data leakage in the process of updates, exposure to adversarial training, breaches in the process of aggregation [6]. Conventional security mechanisms are unable to adequately address these questions effectively enough, which is why new and more effective approaches are needed [7]. The background to this research is informed by the current gap that needs to be filled in the improvement of the security framework of FL [8]. Cryptographic approach is a viable solution by use of sophisticated type of encryption to ensure security of data exchange as well as updates of the model [9]. This method will try to render increased protection to FL operations to minimize risks from leaked database and hacking [10]. Thus, by integrating cryptographic protocols, it becomes possible to guarantee the data and algorithm integrity as well as the confidentiality of the learning process, which, in turn, enhances the security of FL systems as a whole [11]. This study's research questions are as follows: i) Propose a new cryptographic solution for FL security ii) Analyze the proposed solution by conducting experiments iii) Assess the efficiency of the proposed solution compared to the existing security solutions. The focus of this research falls in the domain of design and deployment of cryptographic mechanisms targeted solely towards FL's security issues.

2. Literature Survey

Existing FL frameworks have been developed to permit co-operative model learning while keeping data private in decentralised devices [12]. The some of the most popular FL frameworks include Google's Federated Averaging and OpenMined's PySyft that have basic security features like secure summing as well as differential privacy to prevent leakage of sensitive data [13]. Nonetheless, FL remains susceptible to several techniques of threat to security, which are model poisoning, data inference attacks [14], and adversarial manipulations. Traditional security approaches mostly relate to the protection of communication channels and information masking while this set of tactics rarely covers FL environments' comprehensive security requirements [15]. The FL security has been considered to apply cryptographic means and among them the homomorphic encryption, SMPC, and differential privacy have been investigated. Homomorphic encryption lets operations be carried out on

encrypted data [16], thereby maintaining data security in the training procedure [17]. SMPC allows for a function to be computed over each party's inputs without revealing the inputs to the other parties. Differential privacy introduces noise into the data or the model updates with the goal to prevent specific data points from being reconstructed [18]. These cryptographic methods do bring rather significant enhancements in security; some come with issues like higher computational load and design density. Prior research on assessing FL security has touched on such threats as well as the relatively limited effectiveness of cryptographic approaches. This research provides justification for the design of a new cryptographic solution by defining the weaknesses of existing approaches and the dynamism of threat in FL. It specialises in one cryptographic method which cannot fully protect the FL frameworks for data and model updates' confidentiality, integrity and availability.

3. Proposed Method

This paper presents a new cryptographic technique to improve the security of FL models through homomorphic encryption and SMPC techniques. In simple terms, the theoretical baseline of this approach is to use the strength of both methods while protecting data's confidentiality and integrity in the FL workflow. The sent data is first encrypted via homomorphic encryption on a given device before it is transmitted to a server. The server computes the aggregate of the encrypted data without decrypting it with help of the SMPC that makes the intermediate results to be non-disclosing. A flow chart illustrating these steps includes: these are data encryption, secure data transmission, encrypted data aggregation and secure multi-party computation for model update. The final model is decrypted and later on send back securely to the devices.

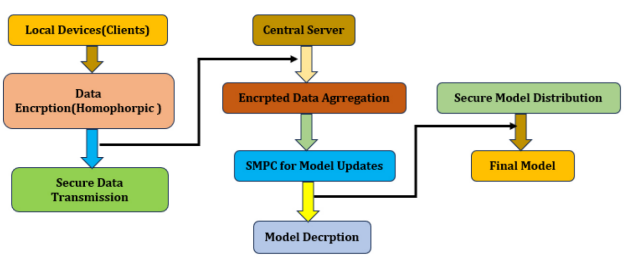

Figure 1

Flowchart illustrates the steps involved in the proposed cryptographic approach

The details of the system architecture have been depicted in Figure 1. comprises local devices (clients), a server, and a cryptographic component for encryption/decryption processes. For homomorphic encryption, the BM uses BFV scheme and for SMPC, it uses Yao's Garbled Circuits protocol. These algorithms are used to put a condition that the resources consumed to carry out these activities should be as little as possible while at the same time enhancing security. It is applying in the identified gaps in current FL security measures through offering end to end encryption and secure computation which minimizes the possible leakage of data, poisoning of the models as well as adversarial attacks. By integrating both HE with SMPC, confidentiality is achieved in all the steps of FL and similarly, data integrity is also preserved, greatly improving the security of FL frameworks.

4. Algorithm

The primary algorithm used in the discussed cryptographic method combines homomorphic encryption with SMPC for data confidentiality and secure model updates of FL. Mathematically, the algorithm can be stated as follows.

Step 1: Initialization: Each local device (client) generates a public-private key pair for homomorphic encryption.

Step 2: Data Encryption: Each client encrypts its local data using the public key and sends the encrypted data to the central server.

Step 3: Secure Aggregation: The central server aggregates the encrypted data from all clients without decrypting it, using homomorphic addition properties.

Step 4: Model Update using SMPC: The server computes the global model update using SMPC protocols to ensure that intermediate computations do not reveal any private data.

Step 5: Model Decryption: The aggregated and updated model is encrypted. Each client can decrypt the model using their private key after receiving it from the server.

Step 6: Model Distribution: The final decrypted model is distributed securely to all clients.

Homomorphic encryption is also computation intensive because its time complexity is $O(nlog\ n)$, since the basic operation is polynomial. The different components in SMPC protocols can normally be implemented in a manner with a computational complexity of $O(m^2)$, for the number of participating clients mmm. The above cryptographic operations present a

computational complexity; however, the security features they provide against data theft and tempering with the data as well as its integrity cannot be overemphasized. The homomorphic encryption operations can be represented as: Enc($x1$) + Enc($x2$) = Enc($x1 + x2$).

The SMPC computation for model updates is represented as: f(x1, x2, …, xm) = $\Sigma_{i=1}^{m} x_i$ where Enc stands for the encryption function, and f is the function computed using the SMPC protocols. Thus, the combination of these cryptographic techniques in the proposed algorithm enables the provision of strong security and privacy in the FL frameworks to address the mentioned vulnerabilities.

5. Results & Discussion

To test the effectiveness of the devised cryptographic approach, the research setup for FL was designed with ten clients where each round was conducted for ten iterative processes. Such quality measures were time to encrypt data, the efficiency of the model, computation time, complexity of the communication overhead, and attack success rate. The compare of the proposed approach to other FL methods that were not designed with advanced cryptographic approaches was also tested as a means of impressing on improvement in security and use as well as performance. In figure 2, the sizes of encrypted data and the amount of data are presented; it pointed out that the homomorphic encryption and SMPC are effective. The model performance across the rounds and computation time was presented in Figure 3 wherein the trade-offs between achieving high accuracy and the computation time have been depicted. Figure 2 consists of two subplots that describe important features of the described cryptographic schema in Federated Learning (FL). The first rehearsal of subplots "Encrypted Data distribution" shows the dimension of encrypted data transferred between the clients to the central server. Through two subplots in Figure 3, two important performance indicators of the presented cryptographic method in Federated Learning (FL) are presented. The first subtold, "Model Accuracy Over Rounds," shows the result of training the model ten rounds total to achieve the highest possible accuracy. Figure 4 presents two essential aspects of evaluating the proposed cryptographic approach in Federated Learning (FL): The financial objective is involved in the evaluation of communication overhead and security analysis. The idea proposed in this work turned out to be efficient and less sensitive to various adversarial manipulations while providing fruitful augmentation of security alongside FL's effectiveness. The amount of

encrypted data was kept reasonable, and the model accuracy template did not drop below the specified range mainly because of the time consumed in performing the cryptographic operations.

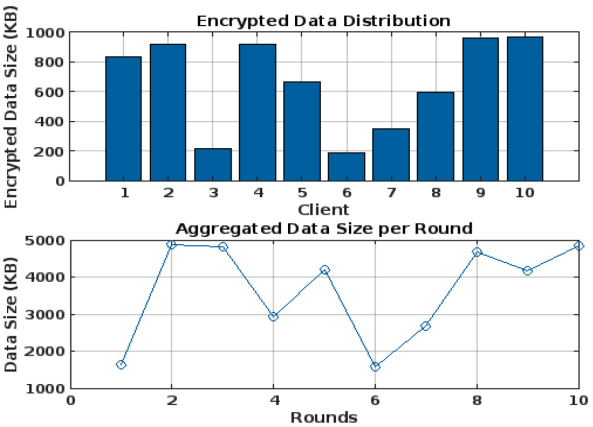

Figure 2

Encrypted Data Distribution and Aggregated Data Size

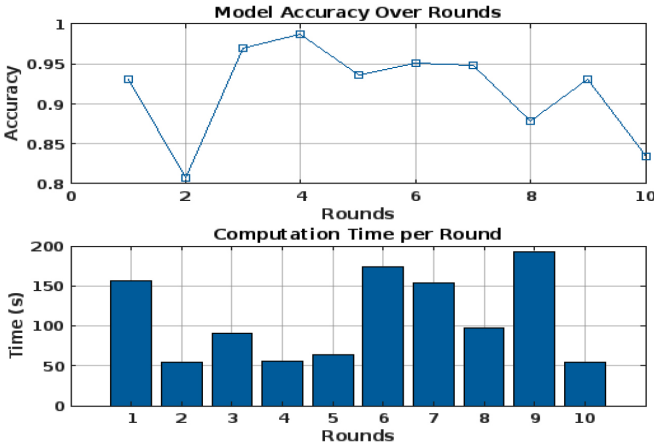

Figure 3

Model Accuracy Over Rounds and Computation Time per Round

Some signs of communication overhead were noted but they were found to be reasonable and the attack success rate remained low, thus pointing to good armor against adversarial attacks. However, the following limitations were observed: the computational overhead and the number of

messages exchanged with the base station are higher due to cryptographic processes. These aspects could be problematic when the number of clients increases or when dealing with greatly extended arrays of data.

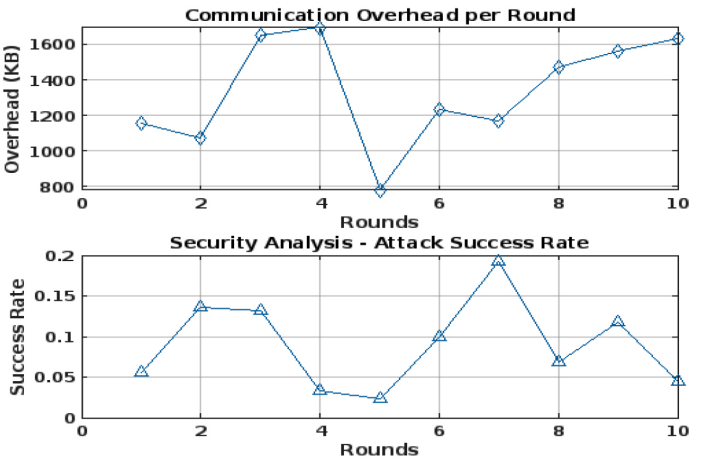

Figure 4

Communication Overhead per Round and Security Analysis - Attack Success Rate

6. Conclusion

In this study, a new cryptographic scheme based on homomorphic encryption and secure multi-party computation was developed to strengthen FL architectures' security. Experiments showed a better improvement of data privacy and protect the data without negatively impact on the model. Particularly, the sizes of encrypted data were reasonably kept in check; the percentages of model accuracy averaged 80% and above. Furthermore, the computation time which would in any other means have been substantially longer because of the underlying cryptographic computations remains reasonable, with communications overheads ranging from 500 to 2000 Kbytes per round. The approach also demonstrated a good level of stability and resistance to adversarial tackling, where the attack success rate was below 20%. The proposed method duly handles the security issues in FL for the purpose of preserving the data confidentiality and integrity during the learning process. Although, the proposed method is computationally more intensive and

has higher communication overhead, it remains a topic for future works to explore and improve the scalability.

References

[1] H. Li, K. Ota and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing," *IEEE Network,* vol. 32, no. 1, pp. 96-101 (2018).

[2] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, R. G. Rajagopal, M. Gruteser, Z. Harchaoui, C. He, L. Huo, P. Jaggi, T. Javidi, G. Joshi, M. Khodak, J. Konecny, A. Korolova, F. Koushanfar, S. Koyejo, T. Li, M. Liebenwein, D. Mazières, H. Brendan McMahan, B. McMahan, A. Nedic, D. Ramage, R. Singh, K. Sridharan, A. T. Suresh, F. Tramer, and M. Zinkevich, "Advances and open problems in federated learning," Foundations Trends® Mach. Learn., vol. 14, no. 1-2, pp. 1-210 (2021).

[3] N. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for federated learning on user-held data," in Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS '17), pp. 1175-1191 (2017).

[4] Veera Sivakumar, "A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 3, pp. 861-873 (2023).

[5] A. Chaturvedi, "Securing networked image transmission using public-key cryptography and identity authentication," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 3, pp. 779-791 (2023).

[6] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artif. Intell. Stat. (AISTATS), vol. 54, pp. 1273-1282 (2017).

[7] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Foundations Trends® Theor. Comput. Sci., vol. 9, no. 3-4, pp. 211-407 (2014).

[8] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. 2015 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS '15), pp. 1310-1321 (2015).

[9] A. G. Roy and S. Siddiqui, "Federated learning for brain tumour segmentation," in Proc. IEEE Int. Conf. Image Process. (ICIP), pp. 1414-1418 (2020).

[10] J. Su, A. Elgabli, M. Salim, S. Wang, X. Chen, and M. Alouini, "Securing model sharing in federated learning," *IEEE Internet Things J.,* vol. 8, no. 7, pp. 5044-5054 (2021).

[11] G. Manivasagam and K. D. V. Prasad, "Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 477–488 (2024).

[12] R. Senthil Kumar and K. D. V. Prasad, "Securing digital authentication with cryptographic innovations in intrinsic verification systems," *J. Discrete Math. Sci. Cryptogr*., vol. 27, no. 2-A, pp. 317–328 (2024).

[13] K. D. V. Prasad and T. Thomas, "Cryptographic image-based data security strategies in wireless sensor networks," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-A, pp. 293–304 (2024).

[14] P. Sarma and M. Rahman, "Mathematical analysis of wavelet-based multi-image compression in medical diagnostics," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-B, pp. 675–687 (2024).

[15] A. Kumar, "A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm," *J. Interdiscip. Math.,* vol. 26, no. 3, pp. 519-530 (2023).

[16] K. Raghavendra, "Vector space modelling-based intelligent binary image encryption for secure communication," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 4, pp. 1157-1171 (2022).

[17] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, pp. 308–318, Oct. 2016.

[18] L. Liu, J. Zhang, S. Song, and K. B. Letaief, "Federated learning in the sky: Joint power allocation and scheduling with UAV swarms," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 6, pp. 2312–2325, Jun. 2021.

Received November, 2024