APPLICATIONS FOR FALSE DATA INJECTION ATTACK DETECTION IN SMART GRIDS

[1]Ch. Deepthi, [2]Penchikala Bhanu Latha,

[1] Assistant Professor in the Department of Master of Computer Applications,
QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India

[2] PG Scholar, Department of Master of Computer Applications,
QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India

ABSTRACT: Federated Learning is a prominent machine learning paradigm which helps tackle data privacy issues by allowing clients to store their raw data locally and transfer only their local model parameters to an aggregator server to collaboratively train a shared global model. However, federated learning is vulnerable to inference attacks from dishonest aggregators who can infer information about clients' training data from their model parameters. To deal with this issue, most of the proposed schemes in literature either require a non-colluded server setting, a trusted third-party to compute master secret keys or a secure multiparty computation protocol which is still inefficient over multiple iterations of computing an aggregation model. In this work, we propose an efficient cross-silo federated learning scheme with strong privacy preservation. By designing a double-layer encryption scheme which has no requirement to compute discrete logarithm, utilizing secret sharing only at the establishment phase and in the iterations when parties rejoin, and accelerating the computation performance via parallel computing, we achieve an efficient privacy-preserving federated learning protocol, which also allows clients to dropout and rejoin during the training process. The proposed scheme is demonstrated theoretically and empirically to provide provable privacy against an honest-but-curious aggregator server and simultaneously achieve desirable model utilities. The scheme is applied to false data injection attack detection (FDIA) in smart grids. This is a more secure cross-silo FDIA federated learning resilient to the local private data inference attacks than the existing works.

I. INTRODUCTION

Federated learning is an innovative approach to machine learning that prioritizes data privacy by allowing clients to keep their data local and share only updated model parameters with a central server for global model training. Despite these privacy benefits, federated learning faces risks from dishonest aggregators who can infer client data from model parameters. Existing solutions, such as differential privacy and secure aggregation, aim to

mitigate these risks but often rely on trusted third parties or multiple servers, posing

efficiency challenges. In the context of smart grids, where distributed data must be protected while detecting false data injection attacks (FDIAs), there is a growing interest in applying federated learning. This paper proposes an efficient cross-silo federated learning approach with robust privacy preservation using double-layer encryption and Shamir secret sharing. Key contributions include a secure weighted aggregation scheme and provisions for dynamic client participation, addressing both privacy concerns and model utility in a practical manner.

II. EXISTING SYSTEM

The other technique is secure multiparty computation and homomorphic encryption for secure aggregation. The scheme in [18] was based on Elgamal homomorphic encryption. This scheme requires a trusted dealer to provide each participant with a secret key ski and the aggregator sk0 such that Pk i=0 ski = 0. Their private secure aggregation is aggregator oblivious in the encrypt-once random oracle model where each participant only encrypts once in each time period. To decrypt the sum, it ends up computing the discrete logarithm which can be implemented through a brute-force search or Pollard's lambda method which requires O (P k_), where k is the number of parties and _ is the maximum value of any party's input. To overcome the limitations of solving discrete logarithm problems, [19] presented a scheme

in the encrypt-once random oracle model with fast encryption and decryption based on Decisional Composite Residuosity Assumption which removes the discrete logarithm computation. However, this scheme also requires a trusted dealer to generate and distribute the secret keys to participants and an aggregator. Besides, both of the approaches in [18] and [19] only deal with secure aggregation of scalars over periods of time (not the secure weighted aggregation of model vectors over multiple iterations of federated learning) and does not deal with dropouts/rejoining problems.

Addressing the drawbacks of [18] and [19], the work in [20] proposed a secure aggregation scheme where the input is a vector and can deal with dropouts. The scheme is based on pairwise additive stream ciphers and Shamir secret sharing to tackle client failures. Diffie-Hellman key exchange is adopted to share common pair-wise seeds of a pseudorandom generator. Double masking is introduced to prevent leakage if there is any delay in transmission. Nevertheless, this approach requires at least four communication rounds between each client and the aggregator in each iteration and a repetition of Shamir secret sharing for each iteration. Thus, it suffers from communication and computation inefficiency considering the huge number of iterations of federated learning. Utilizing the technique of secure data aggregation in [20], the work in [21] proposed a general privacy-enhanced federated learning scheme with secure weighted aggregation, which can deal with both the data significance evaluation and secure data aggregation. This scheme still inherits the same drawbacks as [20]. Besides, this scheme only resolved a weak

security model where no collusion between the server and the clients participating in the federated learning. The paper [22] presented Prio, a privacy-preserving system for the collection of aggregate statistics. With a similar approach, [23] introduced SAFE Learn, a generic design for efficient private federated learning systems that protect against inference attacks using secure aggregation. However, these designs rely on multiple non-colluded server settings. Dong et. al. in [24] designed two secure ternary federated learning protocols against semi-honest adversaries based on threshold secret sharing and homomorphic encryption respectively. In the first protocol, threshold secret sharing is used to share all local gradient vectors in all iterations, which causes expensive computation and communication overhead. Besides, the limitation of their second protocol is that all clients use the same secret key and if the server colludes with a client, then it can obtain all client's models.

In [25], Fang et. al. modified the traditional ElGamal protocol into a double-key encryption version to design a new scheme for federated learning with privacy preservation in cloud computing. Nevertheless, the scheme has to solve the discrete logarithm problem as [18]. The study in [26] combined additively homomorphic encryption with differential privacy but cannot tolerate client dropouts. Their system creates significant run-time overheads which makes it impractical for real world federated learning applications. Functional encryption and differential privacy are utilized in [27] to design the Hybrid Alpha scheme. However, Hybrid Alpha relies on a trusted party that holds the master keys. The proposed scheme in [28] replaced the complete communication graph in [20] with a k-regular graph of the logarithmic degree to reduce the communication cost while maintaining the security guarantees; however, each client shares its secret across only a subset of parties, and thus the dropout-resilience is downgraded.

Considering the integrity of the global model besides the privacy preservation of the local data and models, the proposed approach in [29] combined the Paillier additive homomorphic and verifiable computation primitives. The scheme in [29] can verify the correctness of the aggregated model given the fact that every client provides their genuine local models. From the perspective of privacy preservation, the scheme can only tolerate a weaker threat model. No collusion among the server and clients participating in the federated learning protocol was assumed as the keys (sk; pk) necessary for the homomorphic encryption and the signatures are generated by one of the clients and shared among all clients. In the work [17], to deal with the problem of collusion in [29], adding Gaussian noise to the local models before homomorphically encryption was proposed. However, the standard variation of the additive Gaussian noise must be small to not destroy the genuine local models, resulting in the fact that the adding noise protection is not able to provide a high level of differential privacy (" is not small, i.e., less than 1).

Disadvantages

- The system doesn't find PRIVACY-ENHANCING CROSS-SILO FEDERATED LEARNING FDIA DETECTION IN SMART GRIDS.
- The system doesn't implement Rule-based Methodology for supporting ML Algorithms.

III.PROPOSED SYSTEM

In view of the above issues, we propose an efficient cross-silo federated learning with strong privacy preservation which can be applicable to the smart grid domain. By designing a double-layer encryption scheme over multiple federated learning rounds and utilizing Shamir secret sharing, we achieve an efficient privacy-preserving federated learning protocol, which also allows some clients to drop out and rejoin dynamically during the training process. Specifically, we summarize the main contributions as follows:

_ A general privacy-enhancing cross-silo federated learning with a secure weighted aggregation scheme is designed based on lightweight double-layer encryption and Shamir secret sharing. The scheme removes the requirement of computing discrete logarithms which is the limitation of some related works. No multiple non-colluding server settings are required. Besides, clients' secret keys of two encryption

layers are generated in a decentralized manner which helps increase privacy.

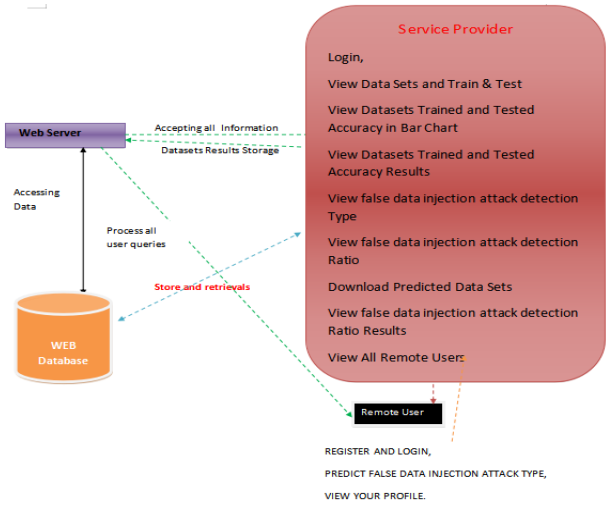
_ The proposed scheme is demonstrated theoretically and empirically to provide provable privacy against an honest-but-curious aggregator server and simultaneously achieve desirable model utility.

_ The proposed scheme is efficient in communication/ computation and robust against dropouts/rejoining during training iterations.

_ An efficient privacy-enhancing cross-silo federated learning resilient to the local training data inference attacks for FDIA detection in the smart grid domain is proposed and empirically evaluated.

Advantages

- False data injection attack (FDIA) detection is a critical security operation in a smart grid control system. and has been solved by data-driven machine learning methods.
- The data-driven machine learning methods require a huge amount of measurement data which are distributed over an interconnected grid. In such an interconnected grid, each sub-grid is possessed and managed by an independent transmission grid company (TGC) regarding power industry deregulation.



IV.MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password.

After login successful he can do some operation, such as View Data Sets and Train & Test, View Datasets Trained and Tested Accuracy in Bar Chart, View Datasets Trained and Tested Accuracy Results, view false data injection attack detection Type, view false data injection attack detection Ratio, Download Predicted Data Sets, view false data injection attack detection Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name,

email, address and admin authorize the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like register and login, predict false data injection attack type, view your profile.

V.ALGORITHMS

1.Random Forest Classifier:

Random Forest Classifier is an ensemble learning method that constructs a multitude of decision trees during training. Each tree is trained on a random subset of the dataset and a random subset of features, ensuring diversity among the trees. During prediction, the Random Forest aggregates the predictions of all individual trees to output the mode (most frequent) class label. This ensemble approach improves predictive accuracy and robustness compared to a single decision tree. Random Forests are versatile and effective for both classification and regression tasks across various types of datasets. They are particularly useful for handling high-dimensional data and capturing complex relationships in the data, making them popular in applications such as bioinformatics, finance, and image recognition.

Algorithm 1: Pseudo code for the random forest algorithm

To generate c classifiers:
for i = 1 to c **do**
  Randomly sample the training data D with replacement to produce D_i
  Create a root node, N_i containing D_i
  Call BuildTree(N_i)
end for

BuildTree(N):
if N contains instances of only one class **then**
  return
else
  Randomly select x% of the possible splitting features in N
  Select the feature F with the highest information gain to split on
  Create f child nodes of N, N_1,..., N_f, where F has f possible values (F_1, ... , F_f)
  for i = 1 to f **do**
    Set the contents of N_i to D_i, where D_i is all instances in N that match F_i
    Call BuildTree(N_i)
  end for
end if

2.Logistic Regression:

Logistic Regression is a fundamental statistical method used for binary classification tasks. Despite its name, it is used for classification rather than regression. Logistic Regression models the probability of a binary outcome based on one or more predictor variables. It estimates the probability that a given input data point belongs to a particular class using a logistic (sigmoid) function, which transforms the output into a range of [0, 1]. The decision boundary is typically set at 0.5, classifying inputs with probabilities above 0.5 into one class and below into the other. Logistic Regression is simple yet effective for linearly separable data and provides

interpretable results by estimating coefficients for each feature.

Algorithm 2: PSEUDO code for logistic regression algorithm

```
Step1: Function grad (predictor_attributes, target_attribute, weights)
            {
               Calculate gradient_descent;
               Return weights + learning_rate * gradient_descent;
            }
Step2: Normalize the dataset;
Step3: Repeat
    {
      Weights = grad (params);
      Update weights;
    } until convergence
Step4: z = dot product of predictor variables and updated weights;
Step5: prediction_limit = sigmoid function (z);
Step6: Predict the target class
```

3.Naive Bayes:

Naive Bayes is a probabilistic classifier based on Bayes' theorem with the "naive" assumption of independence between features. Despite its simplifying assumptions, Naive Bayes can be surprisingly effective in many real-world applications, especially in text classification and spam filtering. It calculates the probability of each class given a set of input features and selects the class with the highest probability as the prediction. The algorithm computes these probabilities using Bayes' theorem:

$$P(y|\mathbf{x}_1,\ldots,\mathbf{x}_n) = \frac{P(\mathbf{x}_1,\ldots,\mathbf{x}_n|y)P(y)}{P(\mathbf{x}_1,\ldots,\mathbf{x}_n)}$$

4.Support Vector Machine (SVM): Support Vector Machine (SVM) is a powerful supervised learning algorithm used for classification and regression tasks. SVM finds the optimal hyperplane that best separates classes in the feature space, maximizing the margin between classes. For linearly separable data, SVM aims to find a hyperplane that maximizes the distance between the closest data points of different classes. For non-linearly separable data, SVM uses kernel functions to map the input space into a higher-dimensional feature space where classes are separable. The decision function of SVM for classification can be represented as:

$$f(\mathbf{x}) = \text{sign}\left(\sum_{i=1}^{N_{SV}} y_i \alpha_i K(\mathbf{x}_i, \mathbf{x}) + b\right)$$

5.Decision Tree:

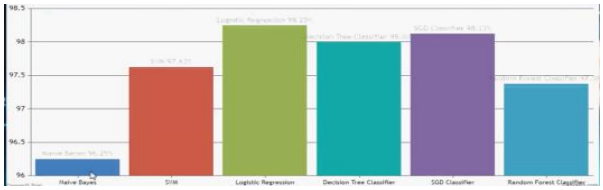
Decision Tree is a non-parametric supervised learning method used for both classification and regression tasks. It partitions the data into subsets based on features that best split the dataset, aiming to minimize impurity or maximize information gain at each node. Each node represents a decision point based on a feature, and each leaf node represents a class label (in classification) or a numerical value (in regression). Decision Trees are intuitive, easy to interpret, and capable of handling both numerical and categorical data. However, they are prone to overfitting noisy data and can create complex trees that generalize poorly to unseen data.

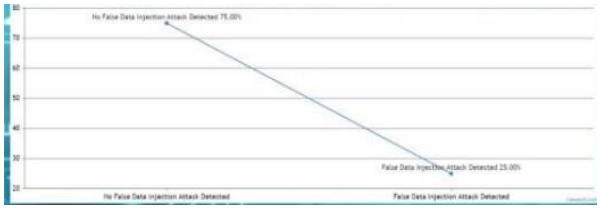
6.SGD Classifier:

Stochastic Gradient Descent (SGD) Classifier is a linear model trained using stochastic gradient descent, a variant of gradient descent optimization. SGD Classifier updates the model's parameters iteratively to minimize the loss function, using a small random subset of the training data (mini-batch) at each step. It is efficient for large-scale datasets and works well with sparse data, making it suitable for text classification and natural language processing tasks. SGD Classifier adapts quickly to new

examples and is computationally efficient, though it may require careful tuning of hyperparameters such as learning rate and regularization strength to achieve optimal performance.

VI.RESULT





S.NO	Algorithm	Accuracy
1	Random Forest Classifier	97.375
2	Logistic Regression	98.25
3	Naive Bayes	96.25
4	SVM	97.625
5	Decision Tree	98.0
6	SGD Classifier	98.125

VII.CONCLUSION

In this paper, we propose a cross-silo privacy-enhancing federated learning which is secure in the honest-but-curious adversarial model. With the main techniques of secure multiparty computation based on double-layer encryption and secret sharing, the scheme is efficient in communication and computation overhead and robust against dropouts and rejoining. The scheme removes the requirement of computing discrete logarithms or multiple non-colluding server settings which are the limitations of some related works. In addition, the client's secret keys of two encryption layers are generated by each party in a decentralized manner which helps increase the level of privacy guarantee. We also firstly design and empirically evaluate a practical and efficient privacy-enhancing cross-silo federated learning resilient to the local private data inference attacks for FDIA detection in the smart grid domain. The proposed scheme provides a framework which can be adapted to other domains. The analysis of security and the empirical evaluation proves that the proposed scheme achieves provable privacy against an honest-but-curious aggregator server colluding with some clients while providing desirable model utility in an efficient manner. In future works, we are going to investigate more different adversarial models in various federated learning settings which is applicable for security in cyber-physical systems.

VIII.REFERENCES

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial intelligence and statistics. PMLR,2017, pp. 1273–1282.

[2] M. Fredrikson, S. Jha, and T. Risten part, "Model inversion attacks that exploit
confidence information and basic countermeasures," Proceedings of the ACM Conference on Computer and Communications Security, vol. 2015-Octob, pp. 1322–1333, 2015.

[3] F. Tram`er, F. Zhang, A. Juels, M. K. Reiter, and T. Risten part, "Stealing machine learning models via prediction fAPIsg," in 25thUSENIX security symposium (USENIX Security 16), 2016, pp. 601–618.

[4] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the gan: information leakage from collaborative deep learning," in Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, 2017, pp. 603–618.

[5] Z. He, T. Zhang, and R. B. Lee, "Model inversion attacks against collaborative inference," ACM International Conference Proceeding Series, pp. 148–162, 2019.

[6] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in 2019IEEE Symposium on Security and Privacy (SP). IEEE, 2019, pp.691–706.

[7] N. Carlini, C. Liu, U´ . Erlingsson, J. Kos, and D. Song, "The secret sharer: Evaluating and testing unintended memorization in neural networks," in 28th USENIX Security Symposium (USENIX Security19), 2019, pp. 267–284.

[8] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1362–1370, 2012.

[9] G. Liang, J. Zhao, F. Luo, S. R.Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1630–1638, 2016.

[10] R. D. Christie, B. F. Wollenberg, and I. Wangensteen, "Transmission management in the deregulated environment," Proceedings ofthe IEEE, vol. 88, no. 2, pp. 170–195, 2000.

[11] F. Karmel, "Deregulation and reform of the electricity industry in australia," Australian Government-Department of Foreign Affairs and Trade, 2018.

[12] L. Sankar, "Competitive privacy: Distributed computation with privacy guarantees," 2013 IEEE Global Conference on Signal and Information Processing, Global SIP 2013 - Proceedings, pp. 325–328,2013.

[13] K. et al., "Advances and open problems in federated learning," Foundations and Trends in Machine Learning, vol. 14, no. 1-2, pp.1–210, 2021.

[14] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Foundations and Trends in Theoretical Computer Science,vol. 9, no. 3-4, pp. 211–487, 2013.

[15] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning", in Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015, pp. 1310–1321.

[16] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," arXiv preprintarXiv:1712.07557, 2017.

[17] A. G. S´ebert, R. Sirdey, O. Stan, and C. Gouy-Pailler, "Protecting data from all parties: Combining fhe and dp in federated learning," arXiv preprint arXiv:2205.04330, 2022.

[18] E. Shi, T. H. H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacypreservingaggregation of time-series data," in Proc. NDSS, vol. 2. Citeseer, 2011, pp. 1–17.

[19] M. Joye and B. Libert, “A scalable scheme for privacy-preserving aggregation of time-series data,” in International Conference on Financial Cryptography and Data Security. Springer, 2013, pp. 111–125.

[20] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan,S. Patel, D. Ramage, A. Segal, and K. Seth, “Practical secure aggregation for privacy-preserving machine learning,” Proceedings of the ACM Conference on Computer and Communications Security, pp. 1175–1191, 2017.

[21] J. Guo, Z. Liu, K.-Y. Lam, J. Zhao, and Y. Chen, “Privacy-enhanced federated learning with weighted aggregation,” in International Symposium on Security and Privacy in Social Networks and Big Data. Springer, 2021, pp. 93–109.

[22] H. Corrigan-Gibbs and D. Boneh, “Prio: Private, robust, and scalable computation of aggregate statistics,” in 14th fUSENIXg Symposiumon Networked Systems Design and Implementation (fNSDIg17), 2017, pp. 259–282.

[23] H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini,H. M¨ ollering, T. D. Nguyen, P. Rieger, A.-R. Sadeghi, T. Schneider,H. Yalame et al., “Safe learn: Secure aggregation for private federated learning,” in 2021 IEEE Security and Privacy Workshops(SPW). IEEE, 2021, pp. 56–62.

[24] Y. Dong, X. Chen, L. Shen, and D. Wang, “Eastfly: Efficient and secure ternary federated learning,” Computers& Security, vol. 94, p. 101824, 2020.

[25] C. Fang, Y. Guo, N. Wang, and A. Ju, “Highly efficient federated learning with strong privacy preservation in cloud computing,” Computers & Security, vol. 96, p. 101889, 2020.

Authors

[1] Mrs. Chepuri Deepthi, currently working as an Assistant professor in the department of Computer Science and Engineering, QIS college of Engineering and Technology, Ongole, Andhra Pradesh. She did her B. Tech from Uttar Pradesh Technical University, Lucknow and M. Tech from JNTUK, Kakinada. Her area of interests is Machine Learning, Artificial Intelligence, Cloud Computing and Programming languages.

[2] Ms. Penchikala Bhanu Latha, currently pursuing Master of Computer Applications at QIS College of Engineering and Technology(Autonomous), Ongole, Andhra Pradesh. He completed BSC in Computer er Science from Vasavi Degree College , Narasaraopet, Ongole, Andhra Pradesh. His areas of interests are Machine Learning.