ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

JOURNAL OF CURRENT SCIENCE

Efficient Cross-Silo Federated Learning Against False Data Injection Attacks

Dr.Kundunuri Ramakrishna[1] ,Hymavathi[2], Vineetha[3], K.Anvitha[4]

[1]Associate Professor, Department of CSE, MallaReddy Engineering College for Women, Hyderabad, drkrk.mrecw@gmail.com

[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, 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 [1] is an emerging machine learning paradigm which addresses critical data privacy issues by enabling clients to store their raw data locally and transfer

only their updated local model parameters to an aggregator server for jointly training a global model. Due to this characteristic, federated learning offers significant privacy improvements over centralizing all the training data. However, federated learning is vulnerable to inference attacks from dishonest aggregators who can infer information about clients' training data from their model parameters (weights, gradients) [2], [3], [4], [5], [6], [7]. For example, [4] employed generative adversarial networks to infer the private data of a target client from its shared model parameters. This means that even if the model is trained in federated learning, data privacy still cannot be rigorously guaranteed. Information can be extracted from global model parameters, but this information cannot be linked to a specific single client because the data samples are anonymized among multiple clients. However, this is not the case if the information is inferred from local model parameters by a corrupted aggregator. Thus, clients' model parameters should be protected from the access of a corrupted aggregator to prohibit these potential inference attacks.

To address this problem, existing approaches focus on two main techniques, which are differential privacy-based and secure aggregation-based. The former adds noise directly to the client's models over a numerous number of iterations; thus, it has the drawbacks of sacrificing the global model accuracy to make a trade-off of privacy-utility. The latter utilizes techniques in cryptography such as secure multiparty computation and homomorphic encryption to securely aggregate the clients' models without knowing their specific values. However, most of these existing approaches rely on a trusted third party to generate the master key for aggregation or a setting with multiple noncolluding servers. Besides, many proposed schemes are still inefficient and impractical due to the expensive overhead of computation and communication among multiple clients over multiple rounds of training.

False data injection attack (FDIA) detection [8], [9] 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 [10], [11]. To build a high-accuracy model for false data injection detection, measurement data from all involved sub-grids should be shared. However, transmitting such huge measurement

data over the network for a centralized detection machine learning algorithm is expensive and also leads to security and privacy issues including competitive privacy [12]. The question is how to coordinate these TGCs to detect FDI attacks while preserving their competitive privacy. This remains a challenging problem which has been attracting recent studies with federated learning-based solutions. In federated learning, a cross-silo setting is often established where a number of companies or organizations have a common incentive to train a model based on all of their data, but do not share their data directly due to confidentiality/privacy or legal constraints [13]. To enhance the privacy of power companies when they contribute their local training models, an efficient privacy preserving cross-silo federated learning for FDIA detection over multi-area transmission grids should be designed.

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.

This paper consists of eight sections. Following this Introduction section are the Related Works and Preliminaries sections. The proposed privacy-enhancing cross-silo federated learning without any trusted third parties is given in Section 4, followed by the analysis of the scheme in Section 5. A concrete scenario of enhancing privacy in cross-silo federated learning for FDIA detection in smart grids with empirical evaluation is given in Section 6 and Section 7. Finally, Section 8 is for the discussion and conclusions.

II. LITERATURE REVIEW

An Efficient Privacy-Enhancing Cross-Silo Federated Learning and Applications for False Data Injection Attack Detection in Smart Grids, Hong-Yen Tran; Jiankun Hu; Xuefei Yin; Hemanshu R. Pota, 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.

III.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. Doublemasking 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 SAFELearn, 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 realworld federated learning applications. Functional encryption and differential privacy is utilized in [27] to design the HybridAlpha scheme. However, HybridAlpha 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. Thescheme 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 found privacy-enhancing cross-silo federated learning fdia detection in smart grids.
- The system doesn't implement Rule-based Methodology for supporting ML Algorithms.

IV. 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

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

- 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.

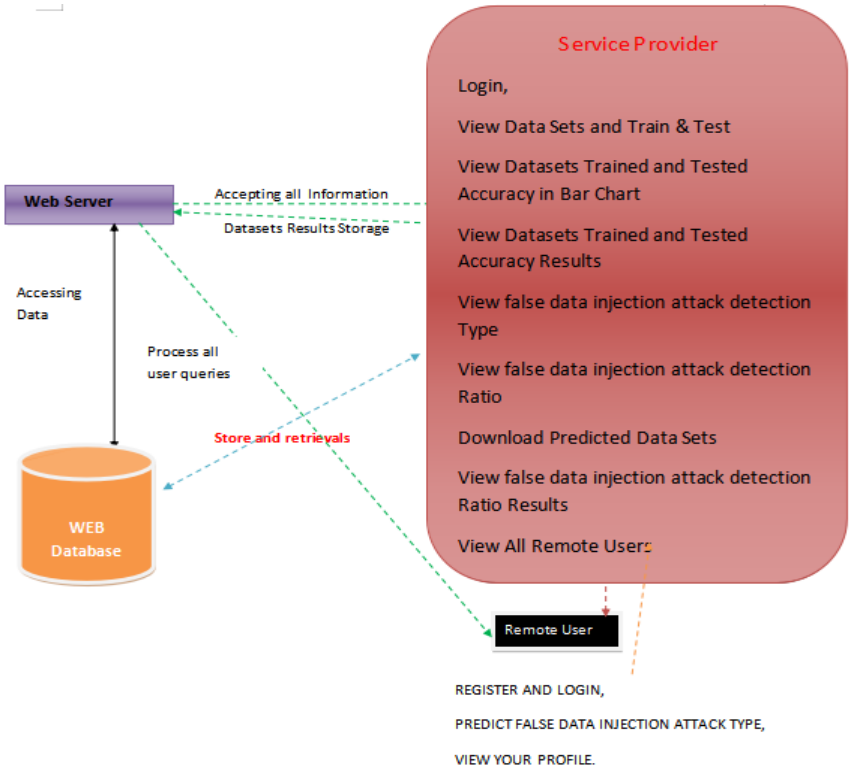

Fig1: architecture diagram

V. 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 operations 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 authorizes 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.

VI. ALGORITHMS

Decision tree classifiers

Decision tree classifiers are used successfully in many diverse areas. Their most important feature is the capability of capturing descriptive decision making knowledge from the supplied data. Decision tree can be generated from training sets. The procedure for such generation based on the set of objects (S), each belonging to one of the classes C1, C2, …, Ck is as follows:

Step 1. If all the objects in S belong to the same class, for example Ci, the decision tree for S consists of a leaf labeled with this class

Step 2. Otherwise, let T be some test with possible outcomes O1, O2,…, On. Each object in S has one outcome for T so the test partitions S into subsets S1, S2,… Sn where each object in Si has outcome Oi for T. T becomes the root of the decision tree and for each outcome Oi we build a subsidiary decision tree by invoking the same procedure recursively on the set Si.

Gradient boosting

Gradient boosting is a machine learning technique used in regression and classification tasks, among others. It gives a prediction model in the form of an ensemble of weak prediction models, which are typically decision

trees.[1][2] When a decision tree is the weak learner, the resulting algorithm is called gradient-boosted trees; it usually outperforms random forest.A gradient-boosted trees model is built in a stage-wise fashion as in other boosting methods, but it generalizes the other methods by allowing optimization of an arbitrary differentiable loss function.

K-Nearest Neighbors (KNN)

- Simple, but a very powerful classification algorithm

- Classifies based on a similarity measure
- Non-parametric
- Lazy learning
- Does not "learn" until the test example is given

- Whenever we have a new data to classify, we find its K-nearest neighbors from the training data

Example

- Training dataset consists of k-closest examples in feature space
- Feature space means, space with categorization variables (non-metric variables)
- Learning based on instances, and thus also works lazily because instance close to the input vector for test or prediction may take time to occur in the training dataset

Logistic regression Classifiers

Logistic regression analysis studies the association between a categorical dependent variable and a set of independent (explanatory) variables. The name *logistic regression* is used when the dependent variable has only two values, such as 0 and 1 or Yes and No. The name *multinomial logistic regression* is usually reserved for the case when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Although the type of data used for the dependent variable is different from that of multiple regression, the practical use of the procedure is similar.

Logistic regression competes with discriminant analysis as a method for analyzing categorical-response variables. Many statisticians feel that logistic regression is more versatile and better suited for modeling most situations than is discriminant analysis.

This is because logistic regression does not assume that the independent variables are normally distributed, as discriminant analysis does.

This program computes binary logistic regression and multinomial logistic regression on both numeric and categorical independent variables. It reports on the regression equation as well as the goodness of fit, odds ratios, confidence limits, likelihood, and deviance. It performs a comprehensive residual analysis including diagnostic residual reports and plots. It can perform an independent variable subset selection search, looking for the best regression model with the fewest independent variables. It provides confidence intervals on predicted values and provides ROC curves to help determine the best cutoff point for classification. It allows you to validate your results by automatically classifying rows that are not used during the analysis.

Naïve Bayes

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .
Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).

While the Naive Bayes classifier is widely used in the research world, it is not widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they does not understand the interest of such a technique.

Thus, we introduce in a new presentation of the results of the learning process. The classifier is easier to understand, and its deployment is also made easier. In the first part of this tutorial, we present some theoretical aspects of the naive bayes classifier. Then, we implement the approach on a dataset with Tanagra. We compare the obtained results (the parameters of the model) to those obtained with other linear approaches such as the logistic regression, the linear discriminant analysis and the linear SVM. We note that the results are highly consistent. This largely explains the good performance of the method in comparison to others. In the second part, we use various tools on the same dataset (Weka 3.6.0, R 2.9.2, Knime 2.1.1, Orange 2.0b and RapidMiner 4.6.0). We try above all to understand the obtained results.

Random Forest

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performance.

The first algorithm for random decision forests was created in 1995 by Tin Kam Ho[1] using the random subspace method, which, in Ho's formulation, is a way to implement the "stochastic discrimination" approach to classification proposed by Eugene Kleinberg.

An extension of the algorithm was developed by Leo Breiman and Adele Cutler, who registered "Random Forests" as a trademark in 2006 (as of 2019, owned by Minitab, Inc.).The extension combines Breiman's "bagging" idea and random selection of features, introduced first by Ho[1] and later independently by Amit and Geman[13] in order to construct a collection of decision trees with controlled variance.

Random forests are frequently used as "blackbox" models in businesses, as they generate reasonable predictions across a wide range of data while requiring little configuration.

SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an *independent and identically distributed* (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point *x* and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. From a geometric perspective, learning a classifier is equivalent to finding the equation for a multidimensional surface that best separates the different classes in the feature space.

SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to *genetic algorithms* (*GAs*) or *perceptrons*, both of which are widely used for classification in machine learning. For perceptrons, solutions are highly dependent on the initialization and termination criteria. For a specific kernel that transforms the data from the input space to the feature space, training returns uniquely defined SVM model parameters for a given training set, whereas the perceptron and GA classifier models are different each time training is initialized. The aim of GAs and perceptrons is only to minimize error during training, which will translate into several hyperplanes' meeting this requirement.

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. Ristenpart, "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. Ristenpart, "Stealing machine learning models via prediction fAPIsg," in 25th USENIX 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 2019 IEEE 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 Security 19), 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 of the 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, GlobalSIP 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 preprint arXiv: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, "Privacypreserving aggregation 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 Symposium on Networked Systems Design and Implementation (fNSDIg 17), 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., “Safelearn: 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.