Journal of Information Processing Vol.30 789–795 (Dec. 2022)

[DOI: 10.2197/ipsjjip.30.789]

Invited Paper

Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks

Sachiko Kanamori[1,a)] Taeko Abe[1] Takuma Ito[1] Keita Emura[1] Lihua Wang[1]
Shuntaro Yamamoto[1] Le Trieu Phong[1] Kaien Abe[2] Sangwook Kim[2] Ryo Nojima[1]
Seiichi Ozawa[2] Shiho Moriai[1]

Received: May 9, 2022, Accepted: September 27, 2022

Abstract: To tackle financial crimes including fraudulent financial transactions (FFTs), money laundering, illegal money transfers, and bank transfer scams, several attempts have been considered to employ artificial intelligence (AI)-based FFT detection systems, particularly, deep learning-based ones. However, to the best of our knowledge, no federated learning systems using *real* transaction data among financial institutions have been implemented so far. This is because there are several issues to be addressed as follows: (1) it is difficult to prepare sufficient amount of transaction data for training by one financial institution (e.g., a local bank), and a small amount of dataset does not promise high accuracy for detection, (2) each transaction data contains personal information, and thus it is restricted by Act on the Protection of Personal Information in Japan to provide the transaction data to a third party. In this paper, we introduce out demonstration experimental results of privacy-preserving federated learning with five banks in Japan: the Chiba Bank, Ltd., MUFG Bank, Ltd., the Chugoku Bank, Ltd., Sumitomo Mitsui Trust Bank, Ltd., and the Iyo Bank, Ltd. As the underlying cryptographic tool, we proposed a privacy-preserving federated learning protocol which we call `DeepProtect`, for detecting fraudulent financial transactions. Briefly, `DeepProtect` allows parties to execute the stochastic gradient descent algorithm using a set of techniques for the privacy-preserving deep learning algorithms (IEEE TIFS 2018, 2019). In the demonstration experiments, we built machine learning models for detecting two types of financial frauds — detecting fraudulent transactions in customers/victims' accounts and detecting criminals' bank accounts. We show that our federated learning system detected FFTs that could not be detected by the model built using the dataset from a single bank and detected criminals' bank accounts before the bank actually froze them.

Keywords: privacy-preserving federated learning, deep learning, fraudulent financial transaction detection, demonstration experiment

1. Introduction

1.1 Background

Financial crimes have become more common, including fraudulent financial transactions (FFTs), money laundering, unauthorized money transfers, and bank transfer scams. According to the National Police Agency of Japan, the total loss due to special frauds in 2021 was 282 billion yen in Japan [*1]. To tackle this issue, several attempts have been considered to employ artificial intelligence-based FFT detection systems such as in Refs. [3], [5], particularly, deep learning-based ones. As a well-known fact in deep learning, large amount of training data set yields high prediction accuracy. Thus, one naive approach is to collect transaction data from multiple banks and implement a deep learning algorithm, e.g., stochastic gradient descent (SGD) [2]. However, each transaction data contains personal information: thus, this approach is difficult because it is restricted by Act on the Protection of Personal Information in Japan to provide the transaction data to a third party. Moreover, it is difficult to prepare a sufficient amount of transaction data for training by one financial institution (e.g., a local bank), and a small amount of dataset does not promise high accuracy for detection.

A promising approach for collecting data in a privacy-preserving manner is to employ cryptographic tools, e.g., multi party computation (MPC) [*2]. Mainly, two types of MPCs — secret sharing-based and homomorphic encryption-based protocols — have been widely studied. Roughly speaking, in a secret sharing-based MPC protocol, all parties (banks in our usage) are required to run a computation on shares of data, and in a homomorphic encryption-based MPC protocol, each party sends a ciphertext of data to another party, who runs homomorphic operations on ciphertexts. To avoid complex computations on each party, we prefer to employ a homomorphic encryption-based MPC protocol that allows us to prepare a central server that runs homomorphic operations and can decrease the computational cost for each party as much as possible.

Technically, any computation on encrypted data can be real-

[1] National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[2] Kobe University, Kobe, Hyogo 657–8501, Japan
[a)] kanamori@nict.go.jp

[*1] https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf (in Japanese)
[*2] Since MPC is a quite hot topic, many important papers have been published so far and it is hard to refer all of them. Thus, we refer a survey paper by Lindell [4] here.

ized via fully homomorphic encryption, and several libraries have been launched (see Ref. [1]). For example, each bank could encrypt transaction data using a (fully) homomorphic encryption scheme, and send the corresponding ciphertext to a central server. Then, the server could run any statistical method on transaction data without decrypting the ciphertexts. Besides computational costs and accuracy, this naive approach does not fit the Act on the Protection of Personal Information in Japan because encrypted personal data are still considered to be personal data.

In addition, we need to decide on a training data format, which contains attributes and features for improving accuracy. Each bank has its own data format, thereby yielding the following points: (1) all banks do not always consider the same attributes/features, and (2) the data format is considered confidential information and is not allowed to be revealed to other banks. Moreover, the purpose of introducing a FFT detection system differs. Thus, besides technical issues, we need to consider how to decide the data format for training without disclosing confidential information, and how to state what the purpose of FFT detection is.

1.2 Our Contributions

In this paper, we introduce our demonstration experimental results of privacy-preserving federated learning with five banks in Japan: the Chiba Bank, Ltd., MUFG Bank, Ltd., the Chugoku Bank, Ltd., Sumitomo Mitsui Trust Bank, Ltd., and the Iyo Bank, Ltd. In the demonstration experiments, we build models for detecting two types of financial frauds — detecting fraudulent transactions in customers/victims' accounts and detecting criminals' bank accounts. We show whether federated learning system can detect FFTs with higher accuracy than the model built using the dataset from a single bank. In some cases, more than 70% of actual illegal money transfers can be correctly identified as illegal money transfers. However, the number of illegal money transfers occurring every day at individual banks is not sufficient for learning data. We aim to improve the detection accuracy of illegal money transfers to more than 80% by integrating the results of learning based on data from more banks. We set the target accuracy based on the opinion of the banks' related staffs.

As the underlying cryptographic tool, we developed a privacy-preserving federated learning protocol [6], [7], which we call `DeepProtect`, for detecting fraudulent financial transactions. Briefly, `DeepProtect` allows a bank to execute SGD on data including other banks' data in a privacy-preserving manner that employs a homomorphic encryption scheme in a symmetric key setting. Each bank can locally compute a gradient on its own transaction data, encrypt it, and send the ciphertext to a central server. The central server updates the weights of the model by operating addition with the received encrypted gradients without decryption. Each bank downloads the encrypted model from the central server, decrypts it, and obtains an updated model. By operating this procedure repeatedly, each bank can obtain a model updated by transaction data from the other banks' data, without showing its own transaction data to others and without knowing other banks' transaction data. The crucial point is that no actual data containing personal information are sent outside of each bank, even encrypted ones. That is, all data shared among banks via the central server are statistical data. This situation complies with the Act on the Protection of Personal Information in Japan.

We had several data management issues in the demonstration experiments (see Section 3 for details). First of all, we signed a contract entrusting the processing of personal data with each bank so that we could analyze transaction data and discuss the underlying data format. Secondly, to store and analyze the data securely, we prepared in NICT a physically secure isolation room employing a biometric fingerprint access control system. We set our central server in the room. Thirdly, network access from outside the room to the server was strictly restricted. Any file downloading required approval from the administrator, and all access logs were recorded. Moreover, in transporting the transaction data from banks to the server room in NICT, we carried the media containing the data by an official vehicle in a physically secure manner. Then, we extracted common attributes/features and selected them to improve the detection accuracy via a classical trial and error. How to securely handle the transaction data containing personal information was quite essential to implement the demonstration experiments successfully.

Disclaimer. Owing to our contracts with the banks, we can't show some facts, e.g., which bank participated in either detecting fraudulent transactions in customers/victims' accounts or detecting criminals' bank accounts. Moreover, we can not disclose the number of data records, data format, attributes, and features in detail for running `DeepProtect`, because these may reveal confidential information. We also do not show which machine learning method was employed, except SGD run in `DeepProtect`. Although we recognize that such information disclosure restrictions significantly reduce the technical value of this report, we believe the readers will understand that there is currently no way to perform demonstration experiments using actual sensitive data without such restrictions. Nevertheless, we hope that our results will be useful in introducing a rare scenario in which sensitive data such as transaction data from multiple banks is effective to achieve high accuracy by leveraging privacy-preserving federated learning.

In addition, although we could run `DeepProtect` among banks and the central server via the internet technically, we locally ran `DeepProtect` on the central server because it was difficult to request the banks to join the computation even in a privacy-preserving manner. Our aim was to confirm whether the detection accuracy is improved by employing a federated learning protocol with transaction data obtained from banks, so we prioritized confirming whether the federated learning protocol is effective over running the protocol with banks. Moreover, we had to reduce the risk of data leakage in handling sensitive data. Thus, we decided to run `DeepProtect` locally without any internet connection. We hope this work will continue to the next step for the banks to deploy a privacy-preserving federated learning system, not just to provide transaction data.

Ethics. Our experiments were conducted with the approval of the Personal Data Handling Research and Development Council of the National Institute of Information and Communications Technology, Japan.

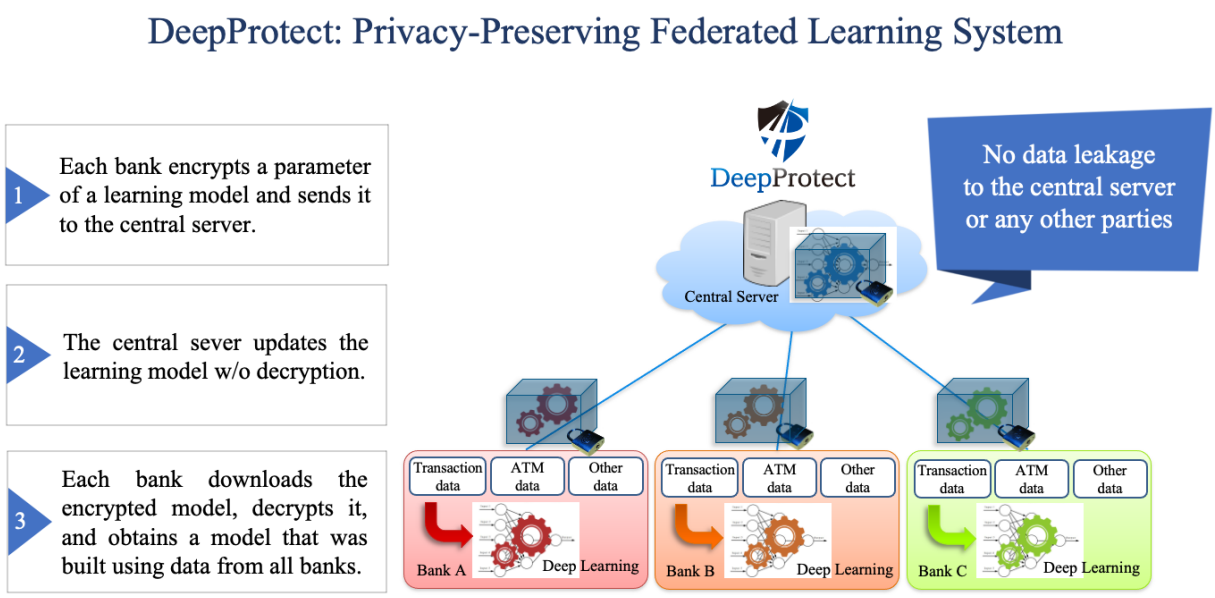


Fig. 1 `DeepProtect` overview.

2. DeepProtect: Privacy-Preserving Federated Learning

In this section, we introduce `DeepProtect`, which is a set of protocols and techniques for privacy-preserving federated learning developed in Refs. [6], [7]. The system overview is depicted in **Fig. 1**. In `DeepProtect`, there are N distributed learning participants and a parameter server (central server) whose operations are described as follows.

The participants locally possess their datasets, and do not send them to outsiders such as the server or any other participants. They also locally run copies of an artificial neural network, and interact with the server in many communication rounds. The initial, possibly random, weight W_{global} of the neural network is initialized by Participant 1. Then participant then sends the homomorphic encryption $\mathbf{E}(W_{\text{global}})$ to the server initially. The purpose of the encryption $\mathbf{E}$ is to protect the secrecy of the weight against the server, which is possibly honest-but-curious.

At any communication round, the participants obtain the latest encrypted $\mathbf{E}(W_{\text{global}})$ from the server, and perform decryption to have W_{global}. Then, the gradient vector $G^{(i)}$ obtained after each execution of the neural network with W_{global} and a local data batch at the participant i is multiplied by the learning rate α. The encrypted $\mathbf{E}(-\alpha \cdot G^{(i)})$ from each learning participant is sent to the server.

The server task is to recursively update the encrypted weight parameters, utilizing the additively homomorphic property of encryption $\mathbf{E}$. In particular, the server computes

$$\mathbf{E}(W_{\text{global}}) + \mathbf{E}(-\alpha \cdot G^{(i)}),$$

which equals $\mathbf{E}(W_{\text{global}} - \alpha \cdot G^{(i)})$ by the homomorphic encryption $\mathbf{E}$. Therefore, the weight W_{global} is updated as $W_{\text{global}} - \alpha \cdot G^{(i)}$, or notationally $W_{\text{global}} \leftarrow W_{\text{global}} - \alpha \cdot G^{(i)}$, which is identical to SGD.

It is worth noting that the encryption $\mathbf{E}$ above is only required to be additively homomorphic, and can be both public-key-based and secret-key-based. The former instantiations are described at length in Ref. [6]. The latter can be constructed in an one-time-pad type as follows: $\mathbf{E}_K(W) = W + \mathbf{PRF}_K(\mathsf{iter})$ in which K is a secret-key shared among the participants and K is unknown to the server; **PRF** is a pseudo-random function; and iter is the unique communication round index known to all parties. The use of secret-key encryption even without a homomorphic property is given in Ref. [7], which additionally describes how to protect the weight in relatively involved scenarios such as dishonest participants and/or the dishonest collusion of participants and the server.

3. Data Management Issues in the Demonstration Experiments and Our Approach

In this section, we show some data management issues in handling the transaction data from banks in the demonstration experiments, and introduce our approach as far as we can disclose.

The main issue is that transaction data are covered by the Act on the Protection of Personal Information in Japan and the data management rules of each bank, and we should comply with them in handling the data. We did not require the actual transaction data as they are and the banks provided us anonymized data by deleting or modifying personal information so that they should not violate the law and minimize the risk of personal data breaches. Our purpose of data collection is to verify whether our privacy-preserving federated learning protocol for FFT detection works well on the real transaction data and is superior to cases when the model is built using data from a single bank. We conducted the demonstration experiments via business consignment with banks, and then our data collection was not treated as a third-party provision of personal data. Notably, the experiments were conducted with the approval of the Personal Data Handling Research and Development Council of the National Institute of Information and Communications Technology, Japan, where we got some advice from outside professionals such as lawyers.

We also had an issue with the physical location to manage the data. Technically, we do not have to collect the actual transac-

tion data from banks because we proposed a privacy-preserving federated learning protocol, DeepProtect. That is, each bank only needs to send an encrypted gradient to the central server, and then no actual data are sent outside the bank (even encrypted ones). This situation complies with the Act on the Protection of Personal Information in Japan. However, it was difficult to ask all the participating banks to connect to the external networks and prepare a local server in the bank; some banks did not have sufficient local environment for running a machine learning. Thus, we needed to prepare a secure environment for machine learning execution.

Initially, we went all the way to a bank facility to analyze the data. However, some banks are located far from NICT in Tokyo. Thus, to store and analyze the data securely, we prepared in NICT a physically secure isolation room employing a biometric fingerprint access control system. We set our central server in the room, where we locally ran DeepProtect.

4. Experimental Results

4.1 Detecting Fraudulent Transactions in Victims' Accounts

First, we show the experimental results for detecting fraudulent transactions in customers' (victims') bank accounts. We detect fraudulent transactions such as cases where a victim her/himself withdraws big money caused by phone frauds or a criminal withdraws cash using a stolen bank card. This can be considered as an anomaly detection. To verify whether our privacy-preserving federated learning protocol, DeepProtect, is superior to the model built using data from a single bank, we compared the detection ratio (recall) between (1) the model built using data from two banks (DeepProtect) and (2) the model built using data from a single bank (Individual Learning). The results are shown in **Fig. 2**. As aforementioned, in the former case, we do not show the underlying machine learning method due to our contracts. By employing DeepProtect, the detection ratio (recall) was improved. In particular, when the number of alerts is more than 600 per day, the detection ratio is more than 80%, which was our target performance of this project. Besides the detection ratio, we also found some fraudulent transactions that could not be found by the model built using data from a single bank.

4.2 Detecting Criminals' Bank Accounts

Next, we show the results for detecting criminals' bank accounts. In this experiment we detect bank accounts where illegal money collected from victims is deposited. More precisely, we detect the bank accounts that were used for usual purposes previously, but at some point, sold or assigned to a group of criminals and abused (for refund scams etc.), and finally frozen by the bank. In this experiment we compared the detection ratio (recall) between (1) the combination of the federated learning model built using data from four banks and the individual learning model (Hybrid) and (2) the model built using data from a single bank (Individual Learning). The results are shown in **Fig. 3**. The hybrid model showed high performance. As aforementioned, we do not show the underlying machine learning method for individual learning. For the former case, we considered a hybrid model generated by employing both machine learning with data from a single bank and DeepProtect that runs SGD in a federated learning manner with data from four banks. The reason why we employed the hybrid model is explained as follows. First, the amount of data from each bank was imbalanced, and several attributes were not provided by some banks. Thus, the performance of a bank could be validated depending on the positive/negative ratio in the training data and the rate of missing values. Therefore, a bank with good performance might be affected by the model updates in the federated learning that is based on the less useful information of other banks. Moreover, the hybrid model only combines the prediction results provided by the individual models for the banks. Therefore, a reliable prediction by a bank with good performance tends to be selected in the hybrid model, resulting in better performance than the federated learning. We evaluated the advantages of the model by not only the detection ratio but also the detection timing, i.e., we checked how early the accounts

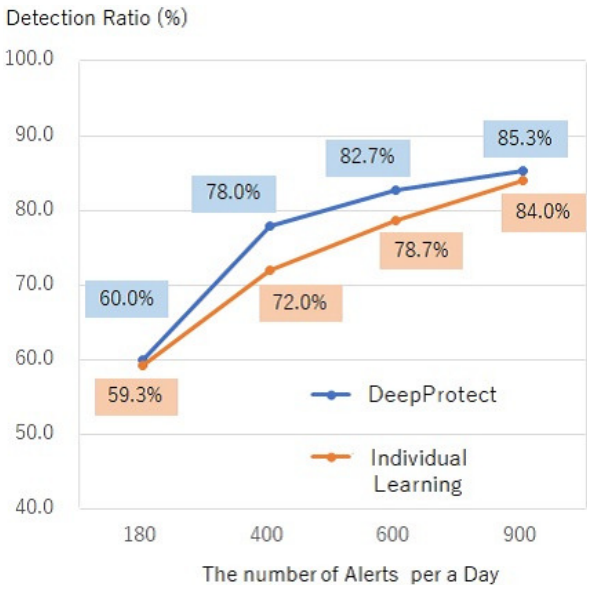


Fig. 2 Detecting fraudulent transactions in victims' accounts.

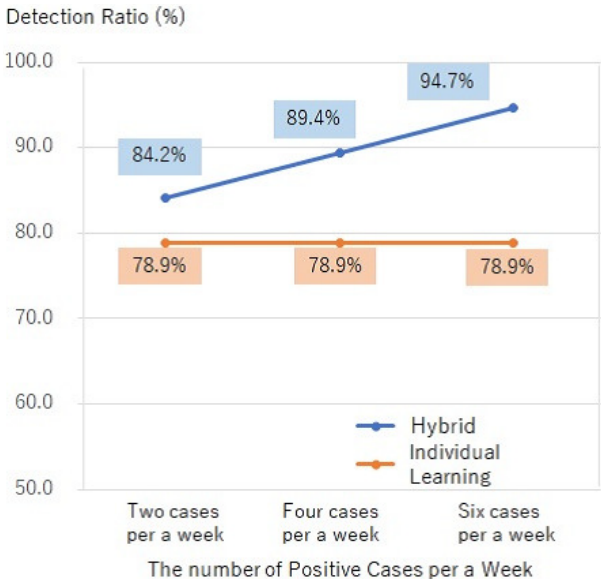


Fig. 3 Detecting criminals' bank accounts.

were detected compared with the timing when the fraudulent accounts were actually frozen by the banks. As the result, the hybrid model showed higher performance than the individual learning model, achieving a detection rate (recall) of over 80%. Furthermore, we found that our model could detect fraudulent accounts 20–50 weeks earlier than actually frozen by the bank.

5. Conclusion and Future Work

In this paper, we presented our demonstration experimental results using privacy-preserving federated learning with five banks in Japan. We showed that our federated learning system detected criminals' bank accounts before the bank actually froze them and detected FFTs that could not be detected by the model built using the dataset from a single bank.

In the experiments, we employed `DeepProtect` as a privacy-preserving federated learning system. From the viewpoint of explainability of AI, we also considered employing two privacy-preserving federated learning protocols for Gradient Boosting Decision Trees (GBDT), FL-XGBoost [9], and eFL-Boost [8], which are briefly described as follows (here FL stands for federated learning). FL-XGBoost [9] introduces a method called model selection, which selects a tree to be added to a global model based on some indices, such as average gradient value, from local models constructed by individual organizations. Particularly, model selection based on gradient values may sometimes suppress the training of specific data owners depending on the difficulty of classification tasks imposed. eFL-Boost [8] focuses on the appropriate allocation of local and global calculations in tree construction. Because each tree in the GBDT is allowed to be a weak learner, eFL-Boost can compensate for the accuracy loss caused by local computation. In the performance evaluation with several public datasets, eFL-Boost showed higher accuracy than those of FL-XGBoost. Employing eFL-Boost to detect FFTs is left as a future work.

We also need to consider how to decide attributes/features in a privacy preserving way. That is, currently we have no choice but to sign a contract with the consent of banks, and we selected attributes/features under the non-disclosure agreement. For familiarizing a federated FFT detection system, standardization of common training data format might be effective because all banks do not always consider the same attributes/features, and deciding on attributes/features is a tough task.

Acknowledgments We would like to express our deepest gratitude to Dr. Yusuke Maruyama and Dr. Chaw Thet Zan of EAGLYS Inc. for their cooperation. This work was supported by JST CREST Grant Number JPMJCR19F6 and JST AIP Accelerated Program Grant Number JPMJCR22U5, Japan.

References

[1] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A. and Vaikuntanathan, V.: Homomorphic Encryption Security Standard, Technical Report, HomomorphicEncryption.org (2018).

[2] Amari, S.: A Theory of Adaptive Pattern Classifiers, *IEEE Trans. Electronic Computers*, Vol.16, No.3, pp.299–307 (1967).

[3] Chen, Z., Khoa, L.D.V., Teoh, E.N., Nazir, A., Karuppiah, E.K. and Lam, K.S.: Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review, *Knowledge and Information Systems*, Vol.57, No.2, pp.245–285 (2018).

[4] Lindell, Y.: Secure multiparty computation, *Comm. ACM*, Vol.64, No.1, pp.86–96 (2021).

[5] Pandey, K., Sachan, P., Shakti and Ganpatrao, N.G.: A Review of Credit Card Fraud Detection Techniques, *2021 5th International Conference on Computing Methodologies and Communication* (*ICCMC*), pp.1645–1653 (online), DOI: 10.1109/ICCMC51019.2021.9418024 (2021).

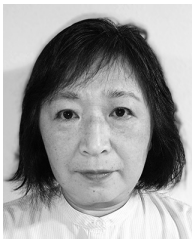
[6] Phong, L.T., Aono, Y., Hayashi, T., Wang, L. and Moriai, S.: Privacy-Preserving Deep Learning via Additively Homomorphic Encryption, *IEEE Trans. Information Forensics and Security*, Vol.13, No.5, pp.1333–1345 (2018).

[7] Phong, L.T. and Phuong, T.T.: Privacy-Preserving Deep Learning via Weight Transmission, *IEEE Trans. Information Forensics and Security*, Vol.14, No.11, pp.3003–3015 (2019).

[8] Yamamoto, F., Ozawa, S. and Wang, L.: eFL-Boost: Efficient Federated Learning for Gradient Boosting Decision Trees, *IEEE Access*, Vol.10, pp.43954–43963 (online), DOI: 10.1109/ACCESS.2022.3169502 (2022).

[9] Yamamoto, F., Wang, L. and Ozawa, S.: New Approaches to Federated XGBoost Learning for Privacy-Preserving Data Analysis, *ICONIP*, Lecture Notes in Computer Science, Vol.12533, pp.558–569, Springer (2020).

Sachiko Kanamori is a technical researcher of National Institute of Information and Communications Technology (NICT) in Japan. She received her bachelor's degree in Literature from Aoyama Gakuin University in 1984. Her research interests include usable security and privacy.



Taeko Abe is a technical researcher of National Institute of Information and Communications Technology (NICT) in Japan. She received her bachelor's degree in Physics from Chuo University in 1984. Her research interests include k-anonymization, cryptography and so on.

Takuma Ito received his B.S., M.S., and Ph.D. in Science from Tokyo Metropolitan University in 2015, 2017, and 2022, respectively. He is currently a researcher of National Institute of Information and Communications Technology (NICT). He received the Best Paper Award at IWSEC 2019 (the 14th International Workshop on Security 2019).

Keita Emura received his M.E. degree from Kanazawa University in 2004. He was with Fujitsu Hokuriku Systems Ltd., from 2004 to 2006. He received his Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST) in 2010, where he was with the Center for Highly Dependable Embedded Systems Technology as a post-doctoral researcher in 2010-2012. He has been a researcher with the National Institute of Information and Communications Technology (NICT) since 2012, has been a senior researcher at NICT since 2014, and has been a research manager at NICT since 2021. His research interests include public-key cryptography and information security. He was a recipient of the SCIS Innovation Paper Award from IEICE in 2012, the CSS Best Paper Award from IPSJ in 2016, and the IPSJ Yamashita SIG Research Award in 2017. He is a member of IEICE, IPSJ, and IACR.

Lihua Wang received her B.S. degree in mathematics from Northeast Normal University, China, in 1988, her M.S. degree in mathematics from the Harbin Institute of Technology, China, in 1994, and her Ph.D. degree in engineering from the University of Tsukuba, Japan, in 2006. She is currently a senior researcher with the Cybersecurity Research Institute, National Institute of Information and Communications Technology (NICT), Japan. Her research interests include cryptography and its applications on privacy-preserving machine learning.

Shuntaro Yamamoto is a manager of General Planning Office, Cybersecurity Research Institute, NICT. He is a manager of Project of Co-Creation Design, Innovation Design Initiative, NICT. He is the chairperson of Networking committee, University Network for Innovation and Technology Transfer (UNITT). He is a 1st grade Certified Specialist of Intellectual Property Management.

Le Trieu Phong received his B.S. from the University of Natural Sciences - Ho Chi Minh City, Viet Nam, in 2002, and his M.Sc. and Ph.D. from Tokyo Institute of Technology in 2006 and 2009 respectively. He is a senior researcher at National Institute of Information and Communications Technology, Japan. His current research interests are cryptography and privacy-preserving data mining.

Kaien Abe received her B.E. degree in Biomedical Engineering, her M.E. degree and her Ph.D. degree in Electrical Engineering from Chongqing University, China, in 1992, 1994, 2002 respectively, and became an associate professor in 2003. During 2003–2006 and 2019–2022, she was affiliated with Tohoku University and Kobe University as a research staff in electromagnetic field calculation and machine learning. Since 2015, she has been a Ph.D. student in Kobe University, simultaneously engaged in software development and big data analysis in company. Her current research interests include computational algebraic geometry and Deep Learning.

Sangwook Kim received his B.E., M.E., and Ph.D. from Kyungpook National University, South Korea, in 2010, 2012, and 2017, respectively. He is currently an assistant professor in the Electrical and Electronic Engineering department at Kobe University, Japan. His current research interests include computer security, information theory, intelligent robots, and machine learning.

Ryo Nojima is a director of Security Fundamental Laboratory, Cybersecurity Research Institute, National Institute of Information and Communications Technology (NICT) in Japan. He received Ph.D. degree from NAIST in 2005. He was a postdoctoral fellow of the university of Tokyo in 2006. He was a Program co-Chairs of IWSEC2021. Contact him at ryo-no@nict.go.jp.

Seiichi Ozawa received his Dr. Eng. degree in computer science from Kobe University, Japan. He is currently the Director of the Center for Mathematical and Data Sciences along with a Full Professor with the Department of Electrical and Electronic Engineering, Graduate School of Engineering, and the Center for Advanced Medical Engineering Research & Development, Kobe University. He has published more than 160 journals and conference papers, and book chapters/monographs. His current research interests include machine learning, incremental learning, big data analytics, cybersecurity, text mining, computer vision, and privacy-preserving machine learning. He is currently an Associate Editor of IEEE Transaction on Neural Networks and Learning Systems, IEEE Transaction on Cybernetics, and two international journals. He is the Vice-President of Membership of International Neural Network Society, the President of Asia Pacific Neural Network Society, and the Vice-President of Japan Neural Network Society. He is a member of Neural Networks TC of IEEE CI Society.

Shiho Moriai is the Director General of Cybersecurity Research Institute, NICT. She received her B.E. degree from Kyoto University in 1993 and Ph.D. in engineering from the University of Tokyo in 2003. She has worked for NTT Laboratories, Sony Computer Entertainment, Inc. as a research scientist, and Sony Corporation as a distinguished researcher. Currently she oversees R&D on cryptography, privacy enhancing technology, and cybersecurity. She was awarded IPSJ Industrial Achievement Award in 2006, Minister's Award of The Ministry of Economy, Trade and Industry, the Industrial Standardization Awards in 2011, and Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology in 2014.