Peer-to-Peer Networking and Applications (2021) 14:1348–1352
https://doi.org/10.1007/s12083-021-01110-9

Advances in privacy-preserving computing

Kaiping Xue[1] · Zhe Liu[2] · Haojin Zhu[3] · Miao Pan[4] · David S. L. Wei[5]

Accepted: 24 February 2021 / Published online: 30 March 2021

The development of advanced technologies in cloud computing, Internet of Things, big data processing, and 5G enables service providers to efficiently and effectively process diverse and massive data and in turn provide users with more diversified and personalized services. However, in the process of data collection and processing, a large number of private data such as a user's identity, a user's location at different times, and even a user's personal medical/financial information is often required. More and more people are concerned about the issue of the privacy disclosure of their own data. In order to solve this problem, the concept of privacy-preserving computing has been proposed and become an important research hotspot gradually. However, there is a contradiction between the utility of data and privacy preservation. How to address this contradiction and to achieve an effective compromise between the two aspects has become the primary concern by researchers from industries and academia. Till now, various cryptographic technologies and security mechanisms have been introduced to provide feasible solutions.

This special issue focuses on the research challenges and issues in privacy-preserving computing. Totally 52 research articles have been received for this SI and 23 of them have been accepted after 2–3 round regular rigorous peer reviews as a witness of ongoing research ideas and solutions related to privacy-preserving computing. A brief view of each of the articles follows.

The first article by Li Chen and Ke Zhang on 'Privacy-Aware Smart Card Based Biometric Authentication Scheme for E-health' identifies that Al-Saggaf et al.'s scheme is vulnerable to the impersonation attack and lacks user anonymity, and further puts forth a privacy-aware smart card based biometric authentication (PSBA) scheme for e-health, which provides more desired security properties as well as defending various possible attacks.

The second article by Yinghui Zhang et al. on 'Efficient Privacy-Preserving Authentication for V2G Networks' designs an anonymous authentication scheme for vehicle-to-grid (V2G) networks to ensure that electric vehicles (EVs) securely access services provided by the grid. Security analysis and performance evaluation show that the proposed scheme not only protects the privacy of EV, but also reduces the computation cost of charging station and EV. Experimental results demonstrate that the scheme is fit for the application of V2G networks.

The third article by Qianjun Wei et al. on 'Privacy-Preserving Two-parties Logistic Regression on Vertically Partitioned Data using Asynchronous Gradient Sharing' proposes a computing protocol that can complete logistic regression training for vertically partitioned data with the participation of two parties, and then constructs the protocol using gradient sharing and optimize the protocol process. The experiments demonstrate that gradient sharing after local rounds calculation has little impact on training results, and the number of local training rounds is appropriately increased to improve training efficiency significantly. Besides, the calculation in ciphertext does not affect the training accuracy.

This article belongs to the Topical Collection: *Special Issue on Privacy-Preserving Computing*
Guest Editors: Kaiping Xue, Zhe Liu, Haojin Zhu, Miao Pan and David S.L. Wei

✉ Kaiping Xue
kpxue@ustc.edu.cn

Zhe Liu
zhe.liu@nuaa.edu.cn

Haojin Zhu
zhu-hj@cs.sjtu.edu.cn

Miao Pan
mpan2@uh.edu

David S. L. Wei
dsl.wei01@gmail.com

[1] University of Science and Technology of China, Hefei, China

[2] Nanjing University of Aeronautics and Astronautics, Nanjing, China

[3] Shanghai Jiao Tong University, Shanghai, China

[4] University of Houston, Houston, TX, USA

[5] Fordham University, Bronx, NY, USA

The fourth article by Xin Ye et al. on 'A Location Privacy Protection Scheme for Convoy Driving in Autonomous Driving Era' proposes a new dynamic mix zone scheme based on autonomous convoy in the convoy driving scenario, which introduces the priority request of the convoy to establish a mix zone to protect the location privacy of autonomous vehicles in the convoy. In the scheme, autonomous vehicles are allowed to use multiple pseudonyms in the case of low location privacy, so as to prevent syntactic join attacks of pseudonym, and consecutive connectable pseudonyms are introduced to trace the violation of anonymous autonomous vehicles.

The fifth article by Xiaofei Bu et al. on 'A Novel Spread Estimation Based Abnormal Flow Detection in High-speed Networks' studies a novel problem, called spread estimation among multi-periods, to measure the total number of distinct elements or the number of distinct k-persistent elements in a flow among multiple traffic measurement periods. In the scheme, an on-chip/off-chip model is used to record the per-flow traffic information, which uses an small on-chip memory to filter out the duplicates, sample the elements, and store the sampled traffic data in off-chip memory. By performing the set operations on the sampled traffic data,the total number of distinct elements and the number of distinct k-persistent elements among multiple periods can be derived based on probability analysis.

The sixth article by Yi Xu on 'High-Throughput Secure Multiparty Multiplication Protocol via Bipartite Graph Partitioning' designs a secure multiparty multiplication protocol with only a single round interaction and simple computation by using replicated sharing, which is generated according to the partition of all cross-terms in the sharing-based multiplication operation. Furthermore, in order to implement the optimal communication for each round, this article models all cross-terms of the sharing-based multiplication operation as a bipartite graph, and proposes a bipartite graph partitioning algorithm. Due to the bipartite graph model, the optimal partition of the cross-terms can be reduced to partition the bipartite graph into n independent subgraphs with the least number of vertices in each subgraph.

The seventh article by Yuqi Fang et al. on 'Three-Stage Stackelberg Game Based Edge Computing Resource Management for Mobile Blockchain' formulates a three-stage Stackelberg game for optimal pricing-based edge computing resource management, and proves the existence and uniqueness of the Stackelberg game equilibrium and derived the miners' optimal amount of computing resources to purchase. This article also proposes a simple yet effective Stackelberg game equilibrium search algorithm based on the golden section search (SES) for resource pricing.

The eighth article by Cong Yu et al. on'An Improved Steganography without Embedding Based on Attention GAN' proposes a new steganography without embedding (SwE) based on attention-GAN model, with carefully designed generator, discriminator and extractor, as well as their loss functions and optimized training mode. The generative model utilizes the attention method to improve the correlation among pixels and to correct errors such as image distortion and background abnormality. The soft margin discriminator is used to improve the compatibility of information recovery and fault tolerance of image generation. Experimental evaluations show that the proposed method can achieve a very high information recovery accuracy and at the same time improve the stenography capacity and image quality.

The ninth article by Mingfu Xue et al. on 'Backdoors Hidden in Facial Features: A Novel Invisible Backdoor Attack against Face Recognition Systems' proposes two novel stealthy backdoor attack methods, BHF2 (Backdoor Hidden in Facial Features) and BHF2N (Backdoor Hidden in Facial Features Naturally), which hide the generated backdoors into facial features (eyebrows and beard) for the first time. The proposed methods greatly guarantee the concealment of backdoor attacks, and can be applied for the strict identity authentication scenarios. The attackers can launch the attacks with simple makeup, rather than wearing eye-catching accessories.

The tenth article by Bang Tran and Xiaohui Liang on 'Exploiting Peer-to-peer Communications for Query Privacy Preservation in Voice Assistant Systems' proposes a novel anonymizer on the voice assistant devices for protecting users' voice data from being linked to their accounts by the service provider. The anonymizer aims to mix the queries from multiple VAS users' devices, hiding the source of queries and hiding the relay's real queries. To achieve effective anonymity, this article proposes a privacy-preserving pattern matching scheme, which the anonymizer is equipped with and is run with the help from a semi-trusted server so as to find the most effective relay for the requester based on their pattern similarity. Meanwhile, to enhance the effectiveness of the anonymity protection, this article proposes anonymity evaluation modules, which allow both requester and relay to evaluate the real-time query generated at requester. The matching scheme will be run periodically or when the rejecting rate at relay is non-tolerable.

The eleventh article by Jin Gu et al. on 'A Robust and Secure Multi-Authority Access Control System for Cloud Storage' proposes a robust multi-authority based ciphertext policy attribute based encryption (CP-ABE) scheme for cloud storage, in which multiple authorities jointly manage the whole attribute set. In the proposed scheme, attribute associated keys can be distributed if and only if the active authorities involved in the procedure exceed a specified threshold (t). The proposed scheme is proved to be secure and robust, which can tolerate less than t authorities being compromised or no more than $n - t$ authorities being crashed, where n denotes the total number of authorities.

The twelfth article by Edgar Batista and Agusti Solanas on 'A Uniformization-based Approach to Preserve Individuals' Privacy during Process Mining Analyses' presents a uniformization-based PPPM technique, named u-PPPM, which distorts attributes distributions in event logs, and averts distribution-based re-identification. By defining a privacy level and an individuals selection strategy (four strategies have been defined in this article), the proposed method conducts a group-based anonymization that exchanges events among individuals with the aim to distort these potentially identifiable distributions, thus rendering the attackers background knowledge useless.

The thirteenth article by Yabin Xu and Bin Shi on 'Copyright Protection Method of Big Data Based on Nash Equilibrium and Constraint Optimization' establishes a Nash equilibrium model between watermark robustness and data quality, which is based on game theory and takes the conflicting factors of robustness and data quality into consideration to solve the optimal number of data group. Then, this article establishes the mapping relationship between data group and watermark bit by using secure hash algorithm. Finally, this article proposes an improved particle swarm optimization algorithm to solve the optimal solution of data change for each data group, and then change the data accordingly to complete the embedding of watermark bit.

The fourteenth article by Zihao Zhu et al. on 'A Reputation-based Cooperative Content Delivery with Parking Vehicles in Vehicular Ad-hoc Networks' proposes a reputation-based cooperative content delivery mechanism to improve the efficiency and security of content delivery. This article formulates the relationships among mobile vehicles (MVs), roadside units (RSUs), and parking vehicles PVs as the two-layer auction game, and presents a dynamic reputation evaluation model, which can incentivize the honest PVs and isolates the malicious PVs so as to improve the security of content delivery. Finally, simulation results show that the proposed mechanism can not only improve the effectiveness of content delivery in vehicular ad-hoc network (VANET), but also avoid the attacks of malicious PVs.

The fifteenth article by Diksha Rangwani et al. on 'A Robust Provable-Secure Privacy-Preserving Authentication Protocol for Industrial Internet of Things' proposes a remote user authentication scheme for the Industrial Internet of Things (IIoT) network so as to overcome some limitations and enhance efficiency based on the application of Elliptic Curve Cryptography (ECC) and one-direction hash trivial operations. The proposed scheme maintains a proper balance among safety and functionalities which is hard to achieve.

The sixteenth article by Manojkumar Vivekanandan et al. on 'Blockchain based Privacy Preserving User Authentication Protocol for Distributed Mobile Cloud Environment' proposes a blockchain based privacy preserving user authentication protocol for distributed mobile cloud environment, which provides a single-time registration of the mobile user using blockchain to access multiple cloud service providers (CSPs).

The seventeenth article by Yuanming Zhang et al. on 'A Machine Learning Based Approach for User Privacy Preservation in Social Networks' develops a machine learning-based approach in online social networks (OSNs) to efficiently correlate the leaked datasets and accurately learn millions of users' confidential information. Moreover, the article develops a trust evaluation model in OSNs to identify malicious service providers and secure users' social activities via direct trust computing and indirect trust computing.

The eighteenth article by Shashidhar Virupaksha and Venkatesulu Dondeti on 'Anonymized Noise Addition in Subspaces for Privacy Preserved Data Mining in High Dimensional Continuous Data' proposes a novel technique about anonymized noise addition in subspaces (ANAS), which reduces data loss, information loss and enhances identification of clusters and privacy.

The nineteenth article by Andrew Onesimu et al. on 'An Efficient Clustering-Based Anonymization Scheme for Privacy-Preserving Data Collection in IoT based Healthcare Services' proposes an efficient privacy-preserving data collection scheme based on the clustering-based anonymity model for IoT based healthcare services, which addresses the privacy violations of data collection through a client/server-to-user model.

The twentieth article by Hemkumar Medar et al. on 'Impact of Data Correlation on Privacy Budget Allocation in Continuous Publication of Location Statistics' proposes a privacy budget allocation (PBA) method for allocating an adequate amount of privacy budget to each successive timestamp under the protection of ϵ-differential privacy, which can protect any w length user stream that contains temporally correlated data-points.

The twenty-first article by Luis Bernardo Pulido-Gaytan et al. on 'Privacy-Preserving Neural Networks with Homomorphic Encryption: Challenges and Opportunities' gives a survey about privacy-preserving Neural Network (NN) models via Homomorphic Encryption (NN-HE), which focuses on the privacy-preserving homomorphic encryption crypto-systems targeted at neural networks identifying current solutions, open issues, challenges, opportunities, and potential research directions.

The twenty-second article by Longfei Zheng et al. on 'ASFGNN: Automated Separated-Federated Graph Neural Network' proposes an automated separated-federated Graph Neural Network (ASFGNN) learning paradigm in the Non-Independent and Identically Distributed (Non-IID) isolated scenario. The article first proposes a separated-federated GNN learning model, which decoupled the training of GNN into two parts: the message passing part is done by clients separately, and the loss computing part is learnt by clients

federally. To handle the time-consuming problem, the article further leverages the Bayesian optimization technique to automatically tune the hyper-parameters of all the clients.

The twenty-third article by William Croft et al. on 'Obfuscation of Images via Differential Privacy: From Facial Images to General Images' develops a framework and derived the configuration of Laplace mechanism through which a formal differentially private guarantee for the obfuscation of facial images in generative machine learning models can be obtained. The approach preserves the privacy guarantee in the presence of attackers with background knowledge, provides resistance to composition attacks and removes the requirement for a gallery of input images. The article also uses a more general mechanism to obfuscate any image directly in pixel-space, which allows for greater versatility in the obfuscation of images.

Finally, we would like to appreciate all authors who submitted high-quality manuscripts for consideration, and all the anonymous reviewers for their criticism and time to help us making final decisions in time. Without their valuable and strong supports, we cannot make this special issue successful. We would like to also thank Prof. Xuemin (Sherman) Shen, the Editor-in-Chief of Peer-to-Peer Networking and Applications, and the Springer Journal Editorial Office for helping us to presenting this special issue to readers. We hope that the readers will find the articles published in this special issue interesting and helpful with further research in privacy-preserving computing.

Kaiping Xue received his bachelor's degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2003 and received his Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2007. From May 2012 to May 2013, he was a postdoctoral researcher with Department of Electrical and Computer Engineering, University of Florida. Currently, he is a Professor in the School of Cyber Security and the Department of EEIS, USTC. His research interests include next-generation Internet, distributed networks and network security. Dr. Xue has authored and co-authored more than 100 technical papers in the areas of communication networks and network security. His work won best paper awards in IEEE MSN 2017, IEEE HotICN 2019, and best paper runner-up award in IEEE MASS 2018. He serves on the Editorial Board of several journals, including the IEEE Transactions on Wireless Communications (TWC), the IEEE Transactions on Network and Service Management (TNSM), and Ad Hoc Networks.

Zhe Liu received the B.S. and M.S. degrees from Shandong University, Jinan, China, in 2008 and 2011, respectively, and the Ph.D. degree from the Laboratory of Algorithmics, Cryptology and Security, University of Luxembourg, Luxembourg City, Luxembourg, in 2015. He was a Researcher with SnT, University of Luxembourg. He is a full Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. He has co-authored over 70 research peer-reviewed journal and conference papers. His current research interests include computer arithmetic and information security. Dr. Liu was a recipient of the Prestigious FNR Awards 2016—Outstanding Ph.D. Thesis Award for his contributions in cryptographic engineering on IoT devices. His research interests include computer arithmetic and cryptographic engineering for pre-quantum and post-quantum cryptography.

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc.(2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. He is currently a professor with Computer Science & Engineering department in Shanghai Jiao Tong University and serving as the Deputy Department Head. His current research interests include network security and privacy enhancing technologies. He published more than 50 international journal papers, including JSAC, TDSC, TPDS, TMC, TIFS, TWC, TVT, and 80 international conference papers, including IEEE S&P, ACM CCS, NDSS, ACM MOBICOM, ACM MOBIHOC, IEEE INFOCOM, and IEEE ICDCS. He received a number of awards including: Natural Science Award of Ministry of Education (2018), IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award (2014), Top 100 Most Cited Chinese Papers Published in International Journals (2014), Supervisor of Shanghai Excellent Master Thesis Award (2014), Distinguished Member of the IEEE INFOCOM Technical Program Committee (2015). He was a co-recipient of best paper awards of IEEE ICC (2007) and Chinacom (2008), IEEE GLOBECOM Best Paper Nomination (2014), WASA Best Paper Runner-up Award (2017). He received Young Scholar Award of Changjiang Scholar Program by Ministry of Education of P.R. China in 2016.

Miao Pan received his BSc degree in Electrical Engineering from Dalian University of Technology, China, in 2004, MASc degree in electrical and computer engineering from Beijing University of Posts and Telecommunications, China, in 2007 and Ph.D. degree in Electrical and Computer Engineering from the University of Florida in 2012, respectively. He is now an Associate Professor in the Department of Electrical and Computer Engineering at University of Houston. He was a recipient of NSF CAREER Award in 2014. His research interests include cybersecurity, deep learning privacy, big data privacy, cyber-physical systems, and cognitive radio networks. His work won IEEE TCGCC (Technical Committee on Green Communications and Computing) Best Conference Paper Awards 2019, and Best Paper Awards in ICC 2019, VTC 2018, Globecom 2017 and Globecom 2015, respectively. Dr. Pan is an Associate Editor for IEEE Internet of Things (IoT) Journal from 2015 to 2018. He has also been serving as a Technical Organizing Committee for several conferences such as TPC Co-Chair for Mobiquitous 2019, ACM WUWNet 2019.

David S. L. Wei received his Ph.D. degree in Computer and Information Science from the University of Pennsylvania in 1991. He is currently a Full Professor of Computer and Information Science Department at Fordham University. From May 1993 to August 1997 he was on the Faculty of Computer Science and Engineering at the University of Aizu, Japan (as an Associate Professor and then a Full Professor). Dr. Wei has authored and co-authored more than 120 technical papers in the areas of parallel and distributed processing, wireless networks and mobile computing, optical networks, P2P communications, big data, cloud computing, and IoT in various archival journals and conference proceedings. He served on the program committee and was a session chair for several reputed international conferences. Dr. Wei is presently an associate editor of IEEE Journal on Selected Areas in Communications for the Series on Network Softwarization & Enablers, and ever served as an associate editor and lead guest editor for some leading journals, such as IEEE J-SAC, IEEE TCC, IEEE TBD, etc. Currently, Dr. Wei focuses his research efforts on cloud and edge computing, IoT, 5G, big data, and machine learning.