BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Semiconductor Science and Information Devices
https://ojs.bilpublishing.com/index.php/ssid

EDITORIAL

Challenges and Opportunities for Privacy Computing

Jianhong Zhang* **Chenghe Dong**

School of Information, North China University of Technology, Beijing, China

ARTICLE INFO

Article history
Received:22 April 2022
Revised: 30 April 2022
Accepted: 05 May 2022
Published Online: 16 May 2022

There's a lot of value in data. The collection, fusion and mining of multi-source data will release the potential of data and bring into play the value of data. At the same time, due to their respective interests and risks of privacy exposure, there are obstacles in the development of multi-data fusion, and the phenomenon of "isolated data island" is common, which hinders the development of data fusion.

Privacy computing [1] is an effective way to solve the data island effect. Privacy computing is to separate the concrete information part of visible data from the invisible value part of calculation, and realize "Data is available but not visible", so as to eliminate the worry of data security and privacy leakage among various data collaborators, in order to solve the problem of "Isolated data island" effectively by means of technology, the essence of which is a technology of joint computation by multiple participants under the condition of security trust, each participant can calculate and analyze the data jointly through the mechanism of encryption and collaboration without disclosing their original data and commercial privacy, so as to realize the value of data fusion, let data intelligence evolve from local insight to global insight.

From a global perspective, privacy computing has been used effectively in many scenarios, especially financial fraud risk control [2], joint modeling, medical data applications and so on. In financial fraud risk management, multinational financial services companies involved in privacy computing can improve their fraud detection and risk models by processing more data; in joint modeling, any party can calculate the privacy of all parties' data (banking and financial institutions, insurance, network platform users' data), and train a more accurate user model with the combination of features, such as Credit Score, risk, etc.

*Corresponding Author:
Jianhong Zhang,
School of Information, North China University of Technology, Beijing, China;
Email: zjhncut@163.com

DOI: https://doi.org/10.30564/ssid.v4i1.4659

However, it has to be acknowledged that privacy computing still faces a powerful challenge [3] to data compliance.

First, "will stimulation". That is, data processors of all parties need to be willing to share the data they have, if there is no mandatory disclosure of public data in general, or if there is a financial incentive to do so, for prudent data compliance reasons, no data processor is willing to include itself in providing the source data. In addition, it is difficult to support large-scale data training because privacy computing introduces many cryptographic operations, such as communication problems of MPC and computing performance problems of homomorphic encryption.

Second, "user consent". Even though the source data is not out of the library, but data processors still produce calculations based on specific "Processing" of the subject's data (for example, by analyzing the user data of different network platforms to determine the income level of the platform's users). According to the "Personal Information Protection Law", in the case of satisfying the disclosure, still have to obtain the user's consent for the processing of the personal information.

Third, "data collusive attacks". In privacy computing, if some participants break the rules of computing and conspire, it may lead to data leakage of other participants.

Fourth, "malicious data pollution". Privacy Computing is performed on the assumption that all parties are capable of providing real and valid data, but in fact this is too idealistic, data participants may contaminate the data based on their own data problems or on intent (such as a competitor pretending to participate) or negligence, and input the wrong source data, which will lead to inaccurate multi-party calculations, which affects the quality of the data.

Fifth, "data rights" recognition. Privacy computing results from data sources provided by many parties, and all parties benefit from it. However, it still faces the situation that the magnitude or quality of data input from various parties is different, and the proportion of contributions from various parties is difficult to balance, whether the parties wish to obtain the result of the calculation, whether the data interest of the result belongs to the common, whether the attribution is confirmed by contract, or whether the secondary utilization will be disputed, still depends on the parties to make it clear by agreement.

Sixth, "data subject rights and interests response". For users, who have the right to know the details of the data processing to meet the transparency requirements under the Personal Information Protection Act, in this case, there may still be uncertainty as to whether a user's platform needs to disclose specific information on multiple participants.

Conflict of Interest

There is no conflict of interest.

References

[1] Yan, Sh., Lv, A.L., 2021. Overview of the development of privacy preserving computing. Information and Communications Technology and Policy. 47(6), 1-11. (In Chinese)
DOI: https://doi.org/10.12267/j.issn.2096-5931.2021.06.001

[2] Qiu, J.X., 2022. Financial Applications of privacy computing. Financial Technology Time. 30(04), 42-45. (In Chinese)
DOI: https://doi.org/CNKI:SUN:HNRD.0.2022-04-010

[3] Wang, S.Y., Yan, Sh., 2022. Challenges and trends of privacy computing. Communications World. (In Chinese)
DOI: https://doi.org/10.13571/j.cnki.cww.2022.02.007