A Survey of Game Theoretical Privacy Preservation for Data Sharing and Publishing

Datong Wu[1], Xiaotong Wu[2(✉)], Jiaquan Gao[2], Genlin Ji[2], Taotao Wu[3], Xuyun Zhang[4], and Wanchun Dou[5]

[1] Changzhou University, Changzhou, China
wudatong@cczu.edu.cn
[2] School of Computer Science and Technology, Nanjing Normal University, Nanjing, China
{wuxiaotong,73025,glji}@njnu.edu.cn
[3] Huawei Company, Shenzhen, China
wutaotaoxpy@gmail.com
[4] Department of Computing, Macquarie University, Macquarie Park, Australia
xuyun.zhang@mq.edu.au
[5] The State Key Lab for Novel Software Technology, Nanjing University, Nanjing, China
douwc@nju.edu.cn

Abstract. Privacy preservation has been one of the biggest concerns in data sharing and publishing. The wide-spread application of data sharing and publishing contributes to the utilization of data, but brings a severe risk of privacy leakage. Although the corresponding privacy preservation techniques have been proposed, it is inevitable to decrease the accuracy of data. More importantly, it is a challenge to analyze the behaviors and interactions among different participants, including data owners, collectors and adversaries. For data owners and collectors, they need to select proper privacy preservation mechanisms and parameters to maximize their utility under a certain amount of privacy guarantee. For data adversaries, their objective is to get the sensitive information by various attack measurements. In this paper, we survey the related work of game theory-based privacy preservation under data sharing and publishing. We also discuss the possible trends and challenges of the future research. Our survey provides a systematic and comprehensive understanding about privacy preservation problems under data sharing and publishing.

Keywords: Game theory · Data privacy · Nash equilibrium · Data sharing and publishing

1 Introduction

With the fast development of communications and infrastructures, there is a huge volume of data generated by various devices, including smart phones and

S. Yu et al. (Eds.): SPDE 2020, CCIS 1268, pp. 205–216, 2020.
https://doi.org/10.1007/978-981-15-9129-7_15

wearable devices [24]. Data sharing and publishing greatly improve the convenience of the daily life of peoples by data analysis techniques, such as service recommendation and data mining [5,9,19–23,44]. For example, some mobile user sends his/her health information collected by a smart watch to medical experts and gets a scientific sport plan. Mobile users also take advantage of their own data to get others' applications and services, such as GPS navigation, shopping and takeaway. The data collectors (e.g., hospitals) share medical data to disease prevention departments to predict possible infectious diseases (e.g., coronavirus disease 2019, COVID-19 [39]). Although users benefit from the applications and services, it brings a certain amount of leakage risk of their sensitive information. Since data sent to service providers is left from data owners (e.g., mobile users), they cannot control the usage of the data. The risk may cause monetary or reputation loss of users to hinder data sharing and publishing [38,40].

In recent years, there have been a series of research works to propose various private metrics and algorithms, including k-anonymity [31], ℓ-diversity [14], t-closeness [11], differential privacy (DP) [7,8,34], local differential privacy (LDP) [6]. k-anonymity requires that each record in a perturbed dataset at least $k-1$ same records. Differential privacy is a rigorous mathematical definition that uses a privacy parameter ϵ to limit the probability to distinguish any two datasets. Different from DP, LDP is an extended version, which is suited to the local setting. There are a lot of randomized mechanisms to satisfy DP and LDP, including the Laplace mechanism [8], the exponential mechanism [16], the Randomized Response mechanism [37]. Different private metrics and mechanisms are suitable to different scenes. Although these private metrics and mechanisms protect privacy of users, it decreases the accuracy of data and thus degrades the service quality of users.

Although there are a lot of effective private metrics and mechanisms, it is a challenge for users and data collectors (e.g., service providers) to choose proper private mechanisms and parameters and interact with the other key participants. On one hand, users and data collectors need to consider the balance between utility and privacy. On the other hand, they also analyze the influence of important factors, including attack strength of adversaries and the privacy degree of the other users and collectors. To this end, game theory is an efficient theoretical tool to research the behavior of various participants [17]. In actually, there have been a series of works to utilize game theory to analyze the interactions among multiple participants for privacy. Meanwhile, the game theoretical analysis contributes to improving efficiency of protection and reducing the cost of privacy.

However, to the best of our knowledge, there are few works to survey the related work about game theory-based privacy analysis for data sharing and publishing. In the previous surveys [4,15,18,25,42,43], most of them focus on the survey of information security rather than the game theory-based privacy analysis. For example, Manshaei et al. [15] and Pawlick et al. [18] mainly focus on game theory-based network security and privacy. Therefore, this paper tries to survey the game theory-based privacy in data sharing and publishing. We first

introduce the preliminaries about scenes, privacy metrics, players and model of games. Then, we survey the existing works about privacy preservation in data sharing and publishing. Finally, we discuss the possible future research directions.

The remaining part of the paper is organized as follows. Section 2 introduces the preliminaries about the key elements based on game theory. Section 3 surveys the existing game theoretical works for privacy analysis. Section 4 discusses the existing works and present the possible future research directions. Section 5 concludes the main work of the paper.

2 Preliminaries

In this section, we introduce the preliminaries about scenes, privacy metrics, game players and models.

2.1 Scenes

In this paper, we focus on two scenes, including data sharing and data releasing [26]. In these two scenes, data can be used for monetary reward and for service. For the former, users send their data to the data collector and get the monetary reward (i.e., data trading). For the latter, users send their data to service providers and get corresponding services. In detail, they are listed as follows:

- **Data Sharing.** In order to get some service (e.g., location-based service, medical service), sensitive information (e.g., location, health information) of some user is shared to the third party.
- **Data Publishing.** The third party collects a huge volume of data from users. Meanwhile, he/she may publish or share the perturbed data to the public or the organization.

For data sharing, either users need to perturb their data so as to protect their privacy. For data publishing, data collectors (e.g., service providers) needs to prevent users' data from privacy leakage.

2.2 Privacy Metrics

There have been a series of privacy metrics and mechanisms to protect privacy, including $k-$anonymity [31], differential privacy [8] and local differential privacy [6]. Here, we present the definitions of the above privacy metrics as follows.

Definition 1 ($k-$anonymity [31]). *A perturbed mechanism $\mathcal{M}$ satisfies k-anonymity if after perturbation of some dataset D, each record has at least $k-1$ same records.*

Both DP and LDP are rigorous mathematical definitions and suitable to different scenes. DP is used for the central setting, while LDP is for the local setting.

Definition 2 (Differential Privacy [8]). *A randomized mechanism $\mathcal{M}$ satisfies ϵ-differential privacy if for any two datasets D_i and D_j which have at most one different record and the domain $\mathcal{O}$ of mechanism $\mathcal{M}$, the output should satisfy the following requirement:*

$$\Pr[\mathcal{M}(D_i) \in \mathcal{O}] \leq \exp(\epsilon) \cdot \Pr[\mathcal{M}(D_j) \in \mathcal{O}] \tag{1}$$

Definition 3 (Local Differential Privacy [6]). *A randomized mechanism $\mathcal{M}$ satisfies ϵ-local differential privacy if for any two value v_i and v_j and the domain $\mathcal{O}$ of mechanism $\mathcal{M}$, the output should satisfy the following requirement:*

$$\Pr[\mathcal{M}(v_i) \in \mathcal{O}] \leq \exp(\epsilon) \cdot \Pr[\mathcal{M}(v_j) \in \mathcal{O}] \tag{2}$$

2.3 Players

In the privacy games, there are three key participants listed as follows:

- **Data Owners (DO).** In order to get some service, the players share their personal information (e.g., trajectory, medical information) to data collectors. When the data collectors are untrusted, the owners should prevent their information from the leakage by some private mechanisms.
- **Data Collectors (DC).** The data collectors collect data from a large number of users. For trusted data collectors, they should protect users' data and avoid the possible leakage. For untrusted data collectors, they are adversaries.
- **Data Adversaries (DA).** The objective of data adversaries is to get sensitive information of data owners. On one hand, they get side information by illegal measurements (e.g., eavesdropping devices, tracking) to launch inference attack. On the other hand, they may be untrusted collectors and get perturbed data from users.

For DOs and trusted DCs, their objective is to protect data from leakage. For untrusted DCs and DAs, their objective is to get sensitive information of DOs.

2.4 Game Model

According to different participants, the existing works about game theory-based privacy analysis are classified into four types as follows:

- **Data Owner vs. Collector (DOC).** In this case, data collectors are not trusted, so that data owners need to adopt preservation mechanisms to protect their privacy. However, it brings a certain amount of utility loss, varying from privacy parameters. Therefore, the objective of data owners is to minimize the utility loss, while the objective of the latter is to get sensitive information as much as possible.

- **Data Owner vs. Owner (DOO).** In some privacy metric (e.g., k-anonymity), the privacy decision of some data owner influences his own privacy, but also the privacy of the others. That is, some data owner benefits from the other's privacy protection, which may lead to the unwillingness to protect privacy.
- **Data Collector vs. Adversary (DCA).** Data collectors get a huge volume of data from users and have the responsibility to prevent privacy leakage against the adversaries. Therefore, there is the defense and attack between data collectors and adversaries.
- **Data Collector vs. Collector (DCC).** Due to the privacy correlation of different datasets, the privacy degree of some dataset is influenced by its own privacy requirements and the others' privacy parameters. Therefore, there is the interactions between multiple data collectors.

3 Privacy Games in Data Sharing and Publishing

According to different game models in Sect. 2.4, we present the detailed works of DOC, DOO, DCA and DCC.

3.1 DOC

In order to get high-quality service, the data owners get the optimal utility under a privacy requirement.

Shokri [29] considers a common scene, in which data owners share their personal information to a untrusted third party (i.e., data collector). Under a joint guarantee of differential privacy and distortion privacy, the objective of data owners is to minimize their utility loss. As an adversary, the data collector attempts to find the data owners' secret by an inference attack. Therefore, it causes defense and attack between data owners and adversaries. In order to analyze the actions of different participants, Shokri [29] constructs a Stackelberg privacy game. In detail, the data owner first chooses a protection mechanism and then the adversary follows by designing an optimal inference attack. Shokri demonstrates that the optimal inference attack results in the same privacy for the data owner. In addition, it proposes linear program solutions for game analysis, in which each participant tries to get the optimal utility. The game result shows that the joint guarantee of differential privacy and distortion privacy is better than differential privacy and distortion privacy.

In order to get users' data, the data collector either provides some specified service or offers the payment to the data owner. Different from the previous scenes, Chessa et al. [3] propose a special case, in which the data collector take the results of data analysis as a public good. The authors construct a game theory-based model, in which each data owner contributes a part of or all of data at a self-chosen level of precision. The data collector controls the degree of data precision. Chessa et al. [3] discuss two cases, i.e., homogeneous and heterogeneous

individuals. The authors demonstrate that the data collector can decrease the bound on the precision of the data to increase the population estimate's accuracy.

On the other hand, the data collector offers payments to incentivize data owners to report their real information.

Similar to [29], Wang et al. [36] consider the scheme of data for monetary reward. The data collector doesn't know the privacy cost of data owners and tries to design a payment strategy to spend the minimal payment to get the desired accurate objective. The authors construct a Bayesian game model and analyze Nash equilibrium points. Meanwhile, a sequence of mechanisms are designed to increase the number of data owners, who report their real information. More importantly, the designed mechanism is asymptotically optimal.

Wang et al. [35] considers a case, in which an untrusted data collector offers payments for noisy data due to privacy concerns of data owners. Although it protects privacy of data owners, it degrades the quality of data. Therefore, it causes an interaction between the data collector and data owners. In order to get a desired quality of noisy data, Wang et al. [35] construct a game model to design a payment mechanism. The privacy requirement of each data owner is controlled by privacy parameter ϵ in differential privacy. Meanwhile, the privacy parameter also influences the quality of perturbed data. The authors design a payment mechanism and analyze Nash equilibrium of the game. In the payment mechanism, for each data owner, the probability to report the real data as a best strategy is $\frac{e^\epsilon}{e^\epsilon+1}$. As a result, the payment mechanism satisfies ϵ-differential privacy due to $\frac{e^\epsilon}{e^\epsilon+1}/\frac{1}{e^\epsilon+1} = e^\epsilon$.

Sooksatra et al. [30] propose a novel challenge: how to design a scheme that benefits both data owners and collectors and promotes their cooperation to prevent data secondary use (e.g., data releasing). The purpose of the scheme is to make data owners report their accurate information and the data collector not resell data. The authors consider two cases, i.e., data for services and data for monetary reward. Sooksatra et al. [30] construct an iterated data trading game model with asymmetric incomplete information. Then, the authors reveal the data trading dilemma problem, including two aspects. The first one is whether or not data owners report their data and face a risk of data release by the data collector. The second one is whether or not the data collector resell data to the others. To this end, the authors propose a zero-determinant strategy to promote data owners and collectors to cooperate rather than defection.

In the above literatures, none of them consider the privacy correlation of data owners' data. Since the social correlation of data owners, it implies that their data is correlated. As a result, the privacy degree of some data owner is influenced by his/her and the other's privacy requirement. Liao et al. [13] construct a two-stage Stackelberg game, in which the data collector chooses a certain number of data owners that report their perturbed data. The authors derive that at Nash equilibrium, only one data owner considers the privacy correlation and the others send their real data. For the data collector, the authors present an optimal privacy protection mechanism.

Sfar et al. [28] discuss the privacy preservation problem in Internet of Things. The data owners (e.g., drivers and vehicles) send their data to the data collector (e.g., data requester). The authors construct a game model to analyze the behaviors of data owners to get the optimal privacy mechanism.

The mobile crowd sensing (MCS) system is one of the most common applications in data sharing. In the MCS system, noisy sensory data is sent to the data collector. In order to motive data owners to report their true data, Jin et al. [10] propose a payment mechanism and construct a Bayesian game model to analyze the behaviors between data collectors and owners. As a result, the authors propose a truth discovery algorithm to motive data owners to maximize their efforts. Meanwhile, the algorithm satisfies individual rationality and budget feasibility.

3.2 DOO

Kumari et al. [33] consider privacy game in data publishing, in which each data owner reports his/her real or dummy data to the data collector. Under the privacy requirement of k-anonymity, the privacy degree of each data owner is influenced by the others' privacy decision. The authors construct a cooperative privacy game (CoPG), in which each player considers a real value called cooperative value. At Nash equilibrium, the authors use information loss metric to evaluate the efficiency of anonymization process.

3.3 DCA

Chen et al. [2] propose an interesting problem: what is the behavior of a data owner to maximize his/her utility in a case with clear privacy costs? The authors construct an interaction game between a data owner and an adversary. The latter attempts to get the real value of the former's data. In detail, for each data owner, he/she has a value $v \in \{0, 1\}$ and then reports the randomized value v' to the data collector. The purpose of the data collector is to get the accurate value v. Since the data collector doesn't know the private value of the data owner, the authors construct a Bayesian game and analyze Bayesian Nash equilibrium. According to different payment functions, the authors discuss three cases and derive that the behavior of the data owner takes a randomized strategy.

Vakilinia et al. [32] consider a cyber threat information sharing scene to have proactive knowledge on the cybersecurity devices and improve the defense efficiency. Although the data collector gets the payment, they face the risk of privacy leakage. To this end, the authors construct a dynamic game model between the data collector and the adversary. In detail, the objective of the adversary is to maximize his/her utility by attacking, while the data collector needs to decide the amount of information. The authors propose 3-way game model with three main components, including CYBEX, data collectors and an adversary. They also derive an optimal strategy of how much sanitation an data collector choose to maximize his/her utility.

3.4 DCC

When there are multiple datasets, their privacy is correlated with each other. It implies that the privacy degree of some data collector is influenced by both his/her and the others' privacy protection. To this end, Wu et al. [41] firstly present a novel definition of correlated differential privacy to describe the privacy relationship between different datasets. Then, the authors construct a game model, in which each data collector publishes the dataset and decides the proper privacy parameter ϵ under differential privacy. They also analyze the existence and uniqueness of the pure Nash equilibrium.

For cybersecurity, multiple organizations share their network data to improve the defense of the whole network. Rawat et al. [27] introduce the idea of Blockchain concept to propose a novel information sharing system, i.e., iShare. The authors construct a Stackelberg game model to analyze the behaviors of organizations.

4 Discussion and Future Research Directions

In this section, we briefly discuss the privacy games in Sect. 3 and then present the possible research directions in the future.

4.1 Discussion

By the description in Sect. 3, we find that most of the existing works focus on DOC and DCA. In these two game models, they consists of three key participants, including data owners, collectors and adversaries. In particular, data collectors are the most important participants. A large number of works usually assume that the data collector is untrusted in a game model. The basic strategy is to take privacy as a commodity and evaluate its price. Then, the data collector offers a certain amount of payment or service as the compensation for privacy risk. When the data collector is trusted, the objective of data collectors is to maximize the utility of perturbed data under a certain amount of privacy guarantee. The brief description of privacy games under data sharing and publishing is shown in Table 1.

4.2 Future Research Directions

Game Model for Local Differential Privacy. Local differential privacy is a novel privacy metric in a local setting. In the previous works, there are few works to utilize local differential privacy to construct the privacy game models. It is interesting that some works (e.g., [35]) have been taken advantage of the similar idea of LDP to construct game models. In fact, with the fast development of Internet of Things and mobile cloud computing, a lot of efficient privacy mechanisms have been proposed to satisfy local differential privacy, including RR [37] and k-RR [1,12]. Therefore, it is a possible research direction to utilize these mechanisms to construct the game model in the local setting.

Table 1. Brief description of privacy games under data sharing and publishing

	Game Model	Privacy Problems	Classification	Technique
Shokri [29]	Stackelberg game	Data sharing	DOC	Differential privacy
Chessa et al. [3]	Non-cooperative game	Data sharing	DOC	–
Wang et al. [36]	Bayesian game	Data sharing	DOC	Differential privacy
Wang et al. [35]	Non-cooperative game	Data sharing	DOC	Differential privacy
Sooksatra et al. [30]	Non-cooperative game	Data publishing	DOC	–
Liao et al. [13]	Stackelberg game	Data sharing	DOC	Correlated differential privacy
Sfar et al. [28]	Non-cooperative game	Data sharing	DOC	–
Jin et al. [10]	Bayesian game	Data sharing	DOC	–
Kumari et al. [33]	Cooperative game	Data sharing	DOO	k-anonymity
Chen et al. [2]	Bayesian game	Data publishing	DCA	Differential privacy
Vakilinia et al. [32]	Non-cooperative game	Data publishing	DCA	Differential privacy
Wu et al. [41]	Non-cooperative game	Data publishing	DCC	Correlated differential privacy
Rawat et al. [27]	Stackelberg game	Data sharing	DOO	–

Game Analysis for DOO and DCC. Relatively speaking, there are few works about DOO and DCC for data sharing and publishing. At present, the condition to construct such privacy game is that there exists the privacy correlation between owners or collectors. The privacy correlation indicates two aspects: (i) some data owner/collector improves the degree of privacy preservation to increase the privacy degree of the others; and (ii) due to the correlation of data, the risk is higher with the addition of more data owners. It is a challenge to define a proper privacy metric to compute the correlation of privacy.

Multiple-Agents for Privacy Game. In the existing privacy games, there are usually two agents to interact with each other. However, in the real environments, there are more than two agents to participate in the game. For example, data collectors receive data from data owners and then sell them to the third party. It implies that the privacy model considers the interaction not only between data owners and collectors, but also between data collectors and the third party. It is more challenging to construct the privacy model and analyze Nash equilibrium points.

5 Conclusion

This paper surveys the related work about privacy games in data sharing and publishing. We have classified privacy games into four types, i.e., DOO, DOC, DCA and DCC. We have presented a certain number of literatures based on game theory to analyze the behaviors of different participants for data privacy. Our object is to help readers to understand the existing works and the possible future directions.

References

1. Bun, M., Nelson, J., Stemmer, U.: Heavy hitters and the structure of local privacy. ACM Trans. Algorithms **15**(4), 51:1–51:40 (2019)
2. Chen, Y., Sheffet, O., Vadhan, S.: Privacy games. In: Liu, T.-Y., Qi, Q., Ye, Y. (eds.) WINE 2014. LNCS, vol. 8877, pp. 371–385. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13129-0_30
3. Chessa, M., Grossklags, J., Loiseau, P.: A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications. In: Proceedings of 28th Computer Security Foundations Symposium, CSF, pp. 90–104. IEEE (2015)
4. Do, C.T., et al.: Game theory for cyber security and privacy. ACM Comput. Surv. **50**(2), 30:1–30:37 (2017)
5. Dou, W., Qi, L., Zhang, X., Chen, J.: An evaluation method of outsourcing services for developing an elastic cloud platform. J. Supercomput. **63**(1), 1–23 (2013). https://doi.org/10.1007/s11227-010-0491-2
6. Duchi, J.C., Jordan, M.I., Wainwright, M.J.: Local privacy and statistical minimax rates. In: Proceedings of 54th Annual Symposium on Foundations of Computer Science, FOCS, pp. 429–438. IEEE (2013)
7. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 265–284. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_14
8. Dwork, C., McSherry, F., Nissim, K., Smith, A.D.: Calibrating noise to sensitivity in private data analysis. J. Priv. Confidentiality **7**(3), 17–51 (2016)
9. Fung, B.C.M., Wang, K., Chen, R., Yu, P.S.: Privacy-preserving data publishing: a survey of recent developments. ACM Comput. Surv. **42**(4), 14:1–14:53 (2010)
10. Jin, H., Su, L., Nahrstedt, K.: Theseus: Incentivizing truth discovery in mobile crowd sensing systems. In: Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017, pp. 1:1–1:10. ACM (2017)
11. Li, N., Li, T., Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity. In: Proceedings of the 23rd International Conference on Data Engineering, ICDE, pp. 106–115. IEEE (2007)
12. Li, N., Ye, Q.: Mobile data collection and analysis with local differential privacy. In: Proceedings of IEEE 20th International Conference on Mobile Data Management (MDM), pp. 4–7 (2019)
13. Liao, G., Chen, X., Huang, J.: Social-aware privacy-preserving correlated data collection. In: Proceedings of the Nineteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2018, Los Angeles, CA, USA, 26–29 June 2018, pp. 11–20. ACM (2018)
14. Machanavajjhala, A., Gehrke, J., Kifer, D., Venkitasubramaniam, M.: l-diversity: Privacy beyond k-anonymity. In: Proceedings of the 22nd International Conference on Data Engineering, ICDE, p. 24. IEEE (2006)
15. Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T., Hubaux, J.: Game theory meets network security and privacy. ACM Comput. Surv. **45**(3), 25:1–25:39 (2013)
16. McSherry, F., Talwar, K.: Mechanism design via differential privacy. In: Proceedings of 48th Annual Symposium on Foundations of Computer Science (FOCS), pp. 94–103. IEEE (2007)
17. Osborne, M.J., Rubinstein, A.: A Course in Game Theory. MIT Press, Cambridge (1994)

18. Pawlick, J., Colbert, E., Zhu, Q.: A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ACM Comput. Surv. **52**(4), 82:1–82:28 (2019)
19. Qi, L., Dai, P., Yu, J., Zhou, Z., Xu, Y.: "time-location-frequency"-aware Internet of Things service selection based on historical records. IJDSN **13**(1), 1–9 (2017)
20. Qi, L., Xiang, H., Dou, W., Yang, C., Qin, Y., Zhang, X.: Privacy-preserving distributed service recommendation based on locality-sensitive hashing. In: Proceedings of International Conference on Web Services, ICWS, pp. 49–56. IEEE (2017)
21. Qi, L., Yu, J., Zhou, Z.: An invocation cost optimization method for web services in cloud environment. Sci. Program. **2017**, 4358536:1–4358536:9 (2017)
22. Qi, L., Zhou, Z., Yu, J., Liu, Q.: Data-sparsity tolerant web service recommendation approach based on improved collaborative filtering. IEICE Trans. Inf. Syst. **100–D**(9), 2092–2099 (2017)
23. Qu, Y., Gao, L., Luan, T.H., Xiang, Y., Yu, S., Li, B., Zheng, G.: Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. **7**(6), 5171–5183 (2020)
24. Qu, Y., Yu, S., Gao, L., Zhou, W., Peng, S.: A hybrid privacy protection scheme in cyber-physical social networks. IEEE Trans. Comput. Soc. Syst. **5**(3), 773–784 (2018)
25. Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G., Xiao, K.: Privacy of things: emerging challenges and opportunities in wireless Internet of Things. IEEE Wirel. Commun. **25**(6), 91–97 (2018)
26. Qu, Y., Yu, S., Zhou, W., Tian, Y.: Gan-driven personalized spatial-temporal private data sharing in cyber-physical social systems. IEEE Trans. Netw. Sci. Eng. 1 (2020). https://doi.org/10.1109/TNSE.2020.3001061
27. Rawat, D.B., Njilla, L., Kwiat, K.A., Kamhoua, C.A.: ishare: blockchain-based privacy-aware multi-agent information sharing games for cybersecurity. In: Proceedings of International Conference on Computing, Networking and Communications, ICNC, pp. 425–431. IEEE Computer Society (2018)
28. Riahi, A., Challal, Y., Moyal, P., Natalizio, E.: A game theoretic approach for privacy preserving model in IoT-based transportation. IEEE Trans. Intell. Transp. Syst. **20**(12), 4405–4414 (2019)
29. Shokri, R.: Privacy games: optimal user-centric data obfuscation. PoPETs **2015**(2), 299–315 (2015)
30. Sooksatra, K., Li, W., Mei, B., Alrawais, A., Wang, S., Yu, J.: Solving data trading dilemma with asymmetric incomplete information using zero-determinant strategy. In: Chellappan, S., Cheng, W., Li, W. (eds.) WASA 2018. LNCS, vol. 10874, pp. 425–437. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94268-1_35
31. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowl. Syst. **10**(5), 557–570 (2002)
32. Vakilinia, I., Tosh, D.K., Sengupta, S.: 3-way game model for privacy-preserving cybersecurity information exchange framework. In: Proceedings of Military Communications Conference, MILCOM, pp. 829–834. IEEE (2017)
33. Kumari, V., Chakravarthy, S.: Cooperative privacy game: a novel strategy for preserving privacy in data publishing. Hum. Centric Comput. Inf. Sci. **6**(1), 1–20 (2016). https://doi.org/10.1186/s13673-016-0069-y
34. Wang, M., Xu, C., Chen, X., Hao, H., Zhong, L., Yu, S.: Differential privacy oriented distributed online learning for mobile social video prefetching. IEEE Trans. Multimedia **21**(3), 636–651 (2019)

35. Wang, W., Ying, L., Zhang, J.: A game-theoretic approach to quality control for collecting privacy-preserving data. In: Proceedings of 53rd Annual Allerton Conference on Communication, Control, and Computing, pp. 474–479. IEEE (2015)
36. Wang, W., Ying, L., Zhang, J.: Buying data from privacy-aware individuals: the effect of negative payments. In: Cai, Y., Vetta, A. (eds.) WINE 2016. LNCS, vol. 10123, pp. 87–101. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-54110-4_7
37. Warner, S.L.: Randomized response: a survey technique for eliminating evasive answer bias. J. Am. Stat. Assoc. **60**(309), 63–69 (1965)
38. Williams, M., Nurse, J.R.C., Creese, S.: Smartwatch games: encouraging privacy-protective behaviour in a longitudinal study. Comput. Hum. Behav. **99**, 38–54 (2019)
39. Wu, F., et al.: A new coronavirus associated with human respiratory disease in China. Nature **579**(7798), 265–269 (2020)
40. Wu, X., Li, S., Yang, J., Dou, W.: A cost sharing mechanism for location privacy preservation in big trajectory data. In: Proceedings of International Conference on Communications, ICC, pp. 1–6. IEEE (2017)
41. Wu, X., Wu, T., Khan, M., Ni, Q., Dou, W.: Game theory based correlated privacy preserving analysis in big data. IEEE Trans. Big Data (2017). https://doi.org/10.1109/TBDATA.2017.2701817
42. Yu, S.: Big privacy: challenges and opportunities of privacy study in the age of big data. IEEE Access **4**, 2751–2763 (2016)
43. Yu, S., Liu, M., Dou, W., Liu, X., Zhou, S.: Networking for big data: a survey. IEEE Commun. Surv. Tutorials **19**(1), 531–549 (2017)
44. Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H., Zhang, Y.: Privacy-preserving federated learning in fog computing. IEEE Internet Things J. 1 (2020). https://doi.org/10.1109/JIOT.2020.2987958