SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain

Yuntao Wang, Zhou Su, Ning Zhang, *Senior Member, IEEE*, Jianfei Chen, Xin Sun, Zhiyuan Ye, and Zhenyu Zhou, *Senior Member, IEEE*

***Abstract*—The exponential growth of data generated from increasing smart meters and smart appliances brings about huge potentials for more efficient energy production, pricing, and personalized energy services in smart grids. However, it also causes severe concerns due to improper use of individuals' private data, as well as the lack of transparency and auditability for data usage. To bridge this gap, in this article, we propose a secure and auditable private data sharing (SPDS) scheme under data processing-as-a-service mode in smart grid. Specifically, we first present a novel blockchain-based framework for trust-free private data computation and data usage tracking, where smart contracts are employed to specify fine-grained data usage policies (i.e., who can access what kinds of data, for what purposes, at what price) while the distributed ledgers keep an immutable and transparent record of data usage. A trusted execution environment based off-chain smart contract execution mechanism is exploited as well to process confidential user datasets and relieve the computation overhead in blockchain systems. A two-phase atomic delivery protocol is designed to ensure the atomicity of data transactions in computing result release and payment. Furthermore, based on contract theory, the optimal contracts are designed under information asymmetry to stimulate user's participation and high-quality data sharing while optimizing the payoff of the energy service provider. Extensive simulation results demonstrate that the proposed SPDS can effectively improve the payoffs of participants, compared with conventional schemes.**

***Index Terms*—Blockchain, off-chain, private data sharing, smart contract, smart grid, trusted computing.**

Manuscript received July 30, 2020; revised October 12, 2020; accepted November 17, 2020. Date of publication November 24, 2020; date of current version July 26, 2021. This work was supported in part by the National Natural Science Foundation under Grant U1808207 and Grant 91746114 and in part by the Project of Shanghai Municipal Science and Technology Commission under Grant 18510761000. Paper no. TII-20-3701. *(Corresponding author: Zhou Su.)*

Yuntao Wang is with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 200240, China (e-mail: yuntao.wang@stu.xjtu.edu.cn).

Zhou Su is with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 200240, China, and also with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: zhousu@ieee.org).

Ning Zhang is with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada (e-mail: ning.zhang@uwindsor.ca).

Jianfei Chen is with the State Grid Zhejiang Electric Power Company, Hangzhou 310007, China (e-mail: chenjf730@163.com).

Xin Sun is with the State Grid Shandong Electric Power Company, Jinan 250001, China (e-mail: advancesun@163.com).

Zhiyuan Ye is with Anhui Jiyuan Software Company, Ltd., Hefei 100100, China (e-mail: ye_zhiyuan@foxmail.com).

Zhenyu Zhou is with the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China (e-mail: zhenyu_zhou@ncepu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2020.3040171.

Digital Object Identifier 10.1109/TII.2020.3040171

I. Introduction

With the prevalence of smart meters and smart appliances, the last decades have witnessed a surge of data generated in smart home and smart grid [1], [2]. Empowered by big data analytics and artificial intelligence technologies, these rich data collected from individual smart devices can be exploited to improve system performance and user experience [3], [4]. For example, utility companies can reduce peak load and electricity production cost, and realize dynamic pricing based on users' load consumption data, while users can better know their energy usage profiles and make personalized energy plans. However, sharing private data with energy service providers (ESPs), e.g., utility companies, in exchange for customized energy services and improved energy efficiency, also raises increasing concerns on user privacy violation and data misuse [5]–[7]. Once private data is shared, the data owner may lose control over the data, and the utility company may mine users' sensitive information or sell it to other third parties without users' consent.

As an effort to bring full control back to data owners, the General Data Protection Regulation (GDPR) legislations [8] have been enforced by the European Union since 2018. To be GDPR compliant, as shown in Fig. 1, conventional approaches for personal energy data management, such as OAuth2 standard [9], mainly rely on the truthfulness of the ESP as it is the only authority for entity authentication and authorisation, data access control, data provenance, and data usage tracking. Thereby, such mechanisms lack transparency and verifiability and are prone to single point of failure. Meanwhile, it is challenging for ESPs to declare their legality in private data processing in face of the investigation of the supervisory authority. Besides, only simple prespecified usage policies are enabled

1551-3203 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

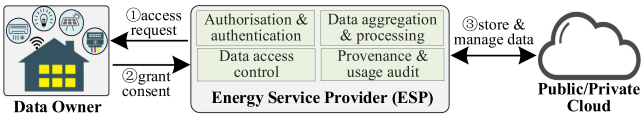


Fig. 1. Simplified process of conventional personal energy data management. (① ESP requests to access the user's personal data to offer services. ② Data owner grants a set of permissions for data access and processing. ③ ESP stores the data in the private/public cloud for processing.)

for users (i.e., data owners) to share their private data with different entities. As a result, it is pressing to design a secure private data sharing scheme in smart grid with fine-grained data access control, auditable data usage, and traceable data provenance.

The emerging blockchain and smart contract technologies offer a decentralized solution to facilitate trustworthy interactions between data owners and energy service providers for personal data sharing and data usage auditing with transparency and provenance traceability while complying with GDPR legislation. In [10], by utilizing blockchain, a decentralized data access control mechanism is designed to ensure that only authorized agents can access the compressed personal data. Besides, a fine-granular private data management framework with GDPR compliance is developed in [11] for data owners to specify user-centric access policies via programmable smart contracts. Meanwhile, in [12], a blockchain-empowered heterogeneous encrypted data sharing scheme is devised for privacy-preserving tucker decomposition in knowledge extraction via homomorphic encryption approaches. However, existing works mainly focus on the data access control to regulate that the private data can be accessed by whom with what policy, while the data usage control regarding the shared data can only be used for intended purposes is absent. For example, the shared private data may be misused for unintended or illegal purposes (e.g., privacy mining) by an authorized ESP driven by economic force. Moreover, current researches mainly build on the data hosting/exchange-as-a-service mode [13], where the entire dataset is delivered to authorized requesters. As a complement of existing data sharing ecosystems, few works consider the data processing-as-a-service (DPaaS) mode, where only the data processing results (i.e., extracted knowledge) are shared. Besides, as the data and computation involved in smart contracts need to be replicated on all nodes in the blockchain for public audit, existing blockchain and smart contract systems not only lack confidentiality in storing and computing sensitive data, but also suffer from poor performance due to constrained resource of user devices. In addition, few works consider the joint secure data access and usage control and incentives in sharing high-quality energy data for users with personalized privacy preferences in smart grid. Hence, it is still an open and vital issue to secure private data management in smart grid while motivating users' high-quality data sharing under the blockchain framework.

In this article, we develop a secure and auditable private data sharing (SPDS) scheme in smart grid. In specific, a novel blockchain-based framework is devised for trust-free private data computation and data usage tracking, where smart contracts specify fine-grained data usage policies (i.e., who can access what kind of data, with what intended purpose, and at what price) while the distributed ledgers keep an immutable and transparent record of data usage. Our framework built on DPaaS mode can be a complement to the existing data sharing ecosystem where only the data processing results are shared to the authorized service providers, instead of delivering the raw data. We also develop an off-chain private data storage and computation mechanism to resolve the confidentiality and poor performance in smart contract execution, where the actual user data is stored in the cloud in the encrypted form while the computation of sensitive user data in smart contracts is moved to the trusted execution environment (TEE) such as Intel SGX. Furthermore, based on contract theory, the optimal contract items (i.e., data utility and price) are designed under information asymmetry to motivate user (i.e., data owner)'s participation and high-quality data sharing while optimizing the payoff of the utility company (i.e., data consumer). The main contributions of this article are threefold as follows.

1) By leveraging blockchain and smart contract technologies, we present a secure personal data sharing framework in smart grid for fine-grained data access control, traceable data usage management, and privacy-preserving data computation. With the proposed framework, users can take full control of their shared private data and ensure: 1) their data can only be accessed and processed by authorized entities for intended purposes, 2) nonrepudiable data usage recording, and 3) verifiable proof of policy compliance.
2) To address the data privacy as well as computation overhead in smart contract systems, we utilize the TEE for off-chain smart contract execution to process confidential user data. To harness the potential of blockchain-TEE systems, the remote attestation is used to guarantee the correctness and consensus of contract execution. A two-phase atomic delivery protocol is designed to ensure the atomicity of data transaction in computing result release and payment. Besides, the off-chain data storage mechanism is adopted for reducing the blockchain burden by moving raw user data in a cloud repository while remaining the metadata on chain.
3) We propose a contract theoretical model for optimal contract design in a monopolized data market to meet users' distinct privacy preferences in personal data sharing. The optimal contract menus, which maximize the utility company's payoff are derived using optimal control theory. Furthermore, extensive simulations are conducted, which demonstrate that our approach can significantly improve the profits of users and the utility company, compared with conventional schemes.

The remainder of this article is organized as follows. In Section II, we discuss the related works. Section III introduces the system model. In Section IV, we present the proposed SPDS scheme for secure personal energy data sharing. In Section V, we evaluate the performance of SPDS scheme. Finally, Section VI concludes this article.

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

II. Related Works

In this section, we first review the blockchain-based approaches for personal data management, and then discuss the incentive mechanisms for data sharing.

A. Blockchain for Personal Data Management

Recently, a number of works have been reported by using blockchain technologies to secure personal data management. Zyskind *et al.* [14] proposed a blockchain-based decentralized personal data management framework to establish trustworthy data access control with improved transparency and auditability, where the compound identities and off-chain key-value data store are implemented. Fan *et al.* [15] presented a secure one-to-many data sharing mechanism in vehicular social networks, where the blockchain is employed for transparent and verifiable access policy recording. Liu *et al.* [16] exploited Ethereum blockchains to safeguard sensing data sharing among distrustful mobile devices in crowdsensing through tamper-resistant ledgers, where deep reinforcement learning techniques are employed to maximize data collection ratio. However, in these works, since the original personal data can be directly accessed and processed by authorized service providers, data owners can have little control over how their data is used by these parties. For example, they may misuse the data by handing over to other third parties for business purposes. Besides, many current works have focused on cryptographic approaches in blockchain for private data sharing. Kosba *et al.* [17] developed Hawk to address the lack of on-chain transactional privacy in smart contracts based on zero-knowledge proofs. Shen *et al.* [18] devised a privacy-preserving SVM model training algorithm in Internet of Things (IoT), where the homomorphic cryptosystem is used to compute on the encrypted data stored in blockchain ledgers. Nonetheless, these approaches suffer from significant performance overhead and can only be applied for relatively simple computations.

B. Incentive Mechanisms for Data Sharing

In the literature, there has been a number of recent works on incentives for data sharing. Chen *et al.* [19] devised a double auction mechanism to motivate selfish vehicle users to share data in blockchain-based Internet of Vehicles (IoV) by designing optimal data pricing strategies. Liu *et al.* [20] presented a two-stage Stackelberg game-theoretical model for efficient IoT data sharing via optimal data pricing in the blockchain-based competitive data market. Based on coalition game, Shen *et al.* [21] presented a collaborative data sharing framework for efficient reward distribution in multiple private/public clouds using Shapley values. Chen *et al.* [22] developed a reverse auction game-based framework to optimize the quality of collected data and social welfare in off-chain data stores in IoV. By formulating the data sharing issue as a maximum weighted independent set problem, Luo *et al.* [23] proposed a graph theory based data sharing algorithm in software-defined IoV. However, existing incentive mechanisms are mainly built on the data hosting/exchange-as-a-service mode by directly sharing the entire dataset, while few works consider the DPaaS mode. Besides, one can observe that the personalized privacy preferences of distinct users and the presence of asymmetric information between data owners and data consumers are not fully taken into account to develop optimal incentive mechanisms for data sharing in smart grid.

Distinguished from existing works, our work applies the blockchain and trusted computing technologies to resolve the fine-grained data access control and transparent data usage auditing for personal data sharing in smart grids. Besides, we exploit the contract theory and optimal control theory to develop optimal data pricing strategies in the smart contracts with consideration of distinct privacy compensations under information asymmetry and DPaaS mode.

TABLE I
Key Notations

Notations	Description
$\mathbb{I}$	The set of individual DOs.
$\mathbb{J}$	The set of aggregators.
$\mathbb{I}_j$	The set of individual DOs in the coverage of aggregator j.
$\mathbb{A}$	The set of DO types.
$\mathbb{D}_i$	Personal energy dataset possessed by DO i.
$\widetilde{\mathbb{D}}_i$	Encrypted form of raw dataset $\mathbb{D}_i$.
L_i	Number of sub-datasets owned by DO i.
$L_\hbar$	Number of UC $\hbar$'s requested datasets owned by DO i.
$ID_{i,l}$	Hash digest of dataset $\mathbb{D}_{i,l}$.
(pk_n, sk_n)	Public/secret key pair of authorized node n.
$k_{i,l}$	Symmetric key for encryption/decryption of dataset $\mathbb{D}_{i,l}$.
k_{CA}	Symmetric key generated by CA for encrypting computing results inside TEE.
$accPolicy$	Access and usage policy designed by DO.
op	Authorized operations over dataset $\widetilde{\mathbb{D}}_{i,\hbar}$.
α_i	Privacy preference or the type of DO i.
$\overline{\alpha}, \underline{\alpha}$	Maximum/minimum privacy preference of DOs.
$g(\alpha)$	Probability density function (PDF) of DO's type α.
$G(\alpha)$	Cumulative distribution function (CDF) of DO's type α.
γ_i	Data sanitization level (DSL) of DO i.
D_i	Quantity of personal energy data owned by DO i.
q_i	Quality of personal energy data owned by DO i.
Φ	Contract menus (i.e., the utility-payment combinations) offered by UC.
$u(\alpha_i)$	Data utility of type-α_i DO.
$p(\alpha_i)$	Payment offered by UC to type-α_i DO.
$\pi(\alpha_i)$	Normalized data utility of type-α_i DO.
$u_{\max}$	Maximum data utility that each DO can contribute.
$\Im(\alpha_i)$	Payoff of DO i if selecting contract item $(\pi(\alpha_i), p(\alpha_i))$.
$\Re$	Expected payoff of UC in data trading with all DOs in $\mathbb{I}$.
$\Re(\alpha_i)$	Payoff of UC when trading with type-α_i DO.

III. System Model

In this section, we first give the system overview of SPDS, and then introduce the adversary model and security assumptions. Finally, we present the design goals of SPDS. Table I summarizes the key notations used.

A. System Overview

Fig. 2 depicts the scenario of blockchain-enabled personal energy data management in smart grids, which includes the following key entities.

Data owners (DOs): The DO is the owner of the smart home and possesses a wide range of heterogeneous energy data collected from her home appliances, smart meters, electric vehicles, etc. The set of individual DOs in the network is denoted as $\mathbb{I} = \{1, \ldots, i, \ldots, I\}$. The personal energy dataset (i.e., a collection of time-stamped energy records with various data sources)

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

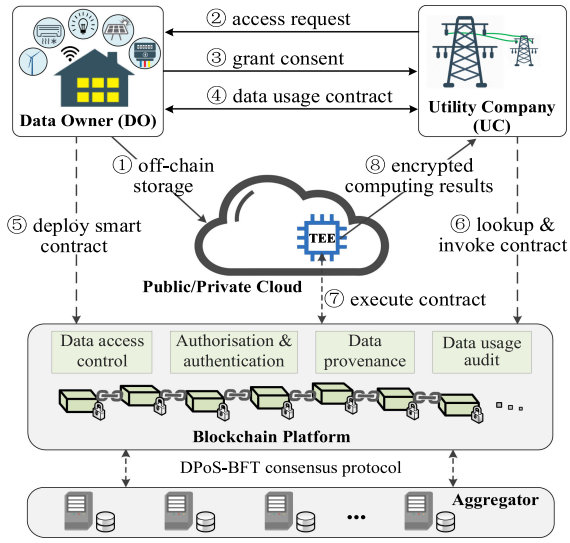


Fig. 2. System overview of blockchain-based personal energy data management with smart contract and TEE.

possessed by DO $i \in \mathbb{I}$ is defined as $\mathbb{D}_i$, which can be further partitioned into a group of subdatasets. For example, divided by the time window (e.g., a week or a month), the data source (e.g., air conditioners or electric vehicles), or both of them. Here, $\mathbb{D}_i$ can be denoted as $\mathbb{D}_i = \{\mathbb{D}_{i,1}, \ldots, \mathbb{D}_{i,l}, \ldots, \mathbb{D}_{i,L_i}\}$, where L_i is the number of subdatasets owned by DO i.

Utility company (UC): The UC (denoted by $\hbar$) is the energy service provider in the smart grid. On one hand, it collects and processes DOs' private energy data to improve the service quality and reduce the energy cost. On the other hand, it delivers personalized and contextual energy services to users (i.e., DOs). Besides, to stimulate DOs to contribute their private energy data, UC offers a series of contract menus, i.e., the utility-payment combinations $\Phi = \{(u_i, p_i), \forall i \in \mathbb{I}\}$, to compensate users' privacy losses in data sharing. Here, p_i is the payment offered by UC for the energy data contributed by DO i with data utility u_i.

Aggregators: A group of aggregators are distributed in the network, the set of which is denoted as $\mathbb{J} = \{1, \ldots, j, \ldots, J\}$. Each aggregator serves as the edge computing node in a community composed of multiple smart homes [24]. Let $\mathbb{I}_j = \{1, \ldots, i, \ldots, I_j\}$ be the set of DOs in the coverage of aggregator $j \in \mathbb{J}$. Each aggregator j can provide proximal edge computing services and wireless communications for I_j DOs in its coverage. Besides, aggregators perform as the full nodes in the blockchain, which store all ledger data and are responsible for consensus management, while DOs only need to store the block header and receive blockchain services from aggregators by acting as lightweight nodes.

TEE Enclave: Instead of delivering the sensitive raw data, the TEE implemented by Intel SGX hosted on the cloud enables that only the computing results (i.e., extracted knowledge) of raw data are delivered to the service provider via efficient off-chain smart contract execution. TEE provides hardware-level guarantees for integrity and confidentiality of computations on sensitive data. The loaded key codes and sensitive information are processed in a secure container (i.e., enclave) [7]. The correctness of configurations and program execution within the enclave can be checked via remote attestation [25], [26] by establishing encrypted and authenticated channels between the enclave and users.

Cloud server: The cloud server (e.g., AWS and Azure) hosts unlimited data storage space and powerful computing capacity for off-chain data storage and processing. For efficient data lookup and matching, a distributed key-value table is maintained by the cloud, where the key refers to the unique hash pointer of the stored private dataset.

Certificate authority (CA): The CA is a trusted agent in the consortium blockchain network, which is responsible for membership enrollment and key distribution. Only authorized nodes after registration with their true identities can join in the blockchain network [27]. Each authorized node n attains its public/secret key pair (pk_n, sk_n), wallet w_n, and certificate cer_n. The role of CA is decided in the genius file of blockchain, and a certificate repository is managed by CA to track and reveal the true identity of any adversary under disputes [28].

The framework of blockchain and TEE based private data sharing illustrated in Fig. 2 is summarized as follows.

1) First, DO uploads the encrypted private datasets in the cloud storage and generates an off-chain data storage transaction with the metadata of datasets (step ①).
2) Then, after receiving data requests, individual DOs can define their own access and usage policies (including the authorized program of a certain service provider, and the intended operations on data) for personal datasets. Once the UC and DO further reach an agreement on data utility and payment, a data access and usage smart contract (DAUC) is created in the form of executable computer codes and is signed by both parties (steps ②−④).
3) Next, when the transaction built by the smart contract code is mutually verified by the majority of full nodes, a contract account of DAUC is created and all nodes in blockchain can access it. UC can lookup the DAUC contract and invoke it by sending enough deposits to the contract account (steps ⑤−⑥).
4) Afterwards, to tackle the confidentiality and poor performance in smart contracts, the execution of DAUC contract is separated into the on-chain state tracking part and off-chain TEE computation part. The correctness and integrity of TEE execution are ensured by the issued proofs (i.e., attestations), while the atomicity of operations (i.e., either both computing result delivery and payment are completed or none of them) is acquired by the proposed two-step atomic delivery protocol (step ⑦).
5) Finally, when the TEE execution finishes, the computation results are delivered to the UC while the financial settlement is performed automatically. Thereafter, the smart contract ends and the states (e.g., account balance) of involved parties are updated (step ⑧).

In general, individuals have distinct privacy preferences in sharing their personal energy data. In other words, users may suffer different privacy losses in sharing the same data. We use $\alpha_i \in \mathbb{A} = [\underline{\alpha}, \overline{\alpha}]$ to capture the essential privacy preference or

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

the type of DO i, where $0 \leq \underline{\alpha} \leq \overline{\alpha} \leq 1$. A higher α_i indicates DO i cares more about privacy. To preserve the data privacy in the delivered computing results to UC during knowledge extraction, the data anonymization technique is adopted to sanitize the raw private data. Let $\gamma_i \in [0, 1]$ be the data sanitization level (DSL) of DO i realized by anonymization, which is directly proportional to α_i, i.e., $\gamma_i = \varsigma\alpha_i$. Here, ς is the normalization factor. Next, let u_i be the data utility of certain datasets owned by DO i, which is associated with the number of data records D_i, data quality q_i, and DSL γ_i [29]. Intuitively, a higher DSL indicates a higher privacy protection level and can cause a larger decrease in data utility. Based on the experiments in [30], the accuracy of the trained model is a concave function concerning the amount of training data. Besides, according to [28] and [31], the high-quality training data shared by participants can significantly improve the accuracy and efficiency of model training in data analysis. As such, the larger data quantity and quality lead to improved data utility. Based on [28]–[31], the data utility u_i can be defined as

$$u_i(\gamma_i, q_i, D_i) = [\mu_1(1-\gamma_i)^{\mu_2} + \mu_3] \cdot q_i \cdot \log(1 + D_i) \quad (1)$$

where μ_k $(k = 1, 2, 3)$ are positive parameters. Here, q_i is determined by multiple factors, such as the level of data cleaning and the average accuracy level of involved energy meters in generating the shared datasets.

B. Adversary Model and Assumptions

The potential adversaries considered during private energy data sharing are presented as follows.

1) *Honest-but-curious cloud:* The cloud is assumed to be honest-but-curious, which honestly executes each operation required in the system for the storage of source data and computing results, while is curious about the stored data.
2) *Repudiation and fraud attack:* On one hand, malicious individuals (i.e., DOs) may attempt to sell fake, redundant, or irrelevant data in pursuit of profits. On the other hand, the malicious UC (i.e., ESP) will conduct the repudiation and fraud attack by denying the data usage record and refuse to pay.
3) *Misuse of shared personal data:* The shared private energy datasets may be misused by the self-interested UC. The sensitive user information, such as living habits, arrival time, and leaving time from home, and even driving routes, may be mined and disclosed. In addition, the shared user's energy datasets may be handed over to other third parties for business purposes.

Besides, the following security assumptions are made in the design of SPDS.

1) The enclave inside TEE (i.e., SGX) is assumed to be secure for off-chain smart contract execution via remote attestations. Besides, the sealed data (e.g., keys and program codes) in the enclave of SGX is assumed to be secure, namely, it is infeasible for any entity other than the SGX to decrypt the sealed data. Although evidences [32] show the potentials of side-channel privacy leakage in SGX, these attacks are not considered in this work and existing works [32], [33] can be employed in SPDS to prevent them.
2) The maximum faulty aggregators (i.e., f) in the consensus committee of blockchain is assumed to be less than or equal to $\frac{1}{3}M$, where M is the total number of validators in the consensus committee.

C. Design Goals

1) *User-centric fine-grained data access and usage control:* SPDS aims to bring full control of personal data back to DOs by enabling individual users to specify fine-granular access and usage policies including who can access what kind of data, for what intended purpose, under what conditions, and at what price.
2) *Confidentiality of user private data:* On one hand, the encryption/decryption of personal data should be controlled by users other than service providers. On the other hand, the sensitive data should be protected from being publicly viewed during smart contract execution.
3) *Transparency, auditability, and provenance traceability:* Each DO should have a transparent view over to whom her data are shared and how her data is used and processed. The recorded data usage activities and the ownership of personal data should be auditable and non-repudiable. Besides, verifiable proof of policy compliance should be available in face of investigations.
4) *Data economy:* SPDS should offer well-designed benign impetuses or incentives to encourage users' participation and high-quality data sharing in data market by compensating for their privacy losses.

IV. Proposed SPDS Scheme

In this section, we present the detailed design of SPDS, which is a blockchain-based system for secure and auditable private energy data sharing in smart grids.

A. Off-Chain Data Storage

To alleviate the storage overhead while improving the scalability of blockchain, the off-chain storage mechanism is applied by moving the large volume of private energy datasets to an external online repository and retaining the metadata (including a hash pointer) of each raw dataset on the blockchain. The cloud database (DB) with powerful computing and storage capacity is employed as the off-chain repository. Each DO i encrypts her personal energy datasets before storing them in the cloud DB. Then, an off-chain data storage transaction (dsTx) is generated in the form as

$$\text{dsTx} = \left\langle \widetilde{\mathbb{D}}_i || \mathbf{meta}_i || t\text{Stamp} || pk_i || pk_{\text{DB}} || \mathcal{MS}_{\{sk_i, sk_{\text{DB}}\}}(\psi_d) \right\rangle, \quad (2)$$

where $\widetilde{\mathbb{D}}_i = \{\widetilde{\mathbb{D}}_{i,1}, \ldots, \widetilde{\mathbb{D}}_{i,l}, \ldots, \widetilde{\mathbb{D}}_{i,L_i}\}$ is the encrypted form of the raw dataset $\mathbb{D}_i$, $\mathbf{meta}_i = \{\text{meta}_{i,1}, \ldots, \text{meta}_{i,l}, \ldots, \text{meta}_{i,L_i}\}$ is the metadata of dataset $\mathbb{D}_i$, tStamp is the timestamp of dsTx creation, $\mathcal{MS}(.)$ is the multisignature function, $(pk_{\text{DB}}, sk_{\text{DB}})$ is the public/secret key pair of the cloud

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

DB, and ψ_d is the hash digest of dsTx. In specific, the metadata of subdataset $\mathbb{D}_{i,l}$ is denoted as a 3-tuple

$$\text{meta}_{i,l} = \langle ID_{i,l} || \text{desc}_{i,l} || \mathcal{H}(k_{i,l}) \rangle \tag{3}$$

where $ID_{i,l} = \mathcal{H}(\mathbb{D}_{i,l})$ is the unique identity (i.e., hash digest) of dataset $\mathbb{D}_{i,l}$, $\mathcal{H}(.)$ is the secure hash function (i.e., SHA256), $\text{desc}_{i,l}$ is the description of dataset $\mathbb{D}_{i,l}$ generated by DO i, and $k_{i,l}$ is the symmetric key for encryption/decryption of dataset $\mathbb{D}_{i,l}$. We have $\widetilde{\mathbb{D}}_{i,l} = \mathcal{E}_{k_{i,l}}(\mathbb{D}_{i,l})$, where $\mathcal{E}(.)$ is the encryption function. The Boneh–Lynn–Shacham (BLS) multisignature [34], which is developed based on the well-known BLS short signature [35], is adopted as the default multisignature function. By aggregating the multiple signatures on the same information, we can reduce the signature size as well as the storage and communication cost in blockchain. In addition, the blockchain platform maintains a globally accessible user interface, which gives an overview of all shared personal energy datasets based on the recorded dsTx transactions to facilitate interest matching and data trading.

B. Data Access and Usage Control With Smart Contract

When UC finds its interested subdatasets $\widetilde{\mathbb{D}}_{i,\hbar} = \{\widetilde{\mathbb{D}}_{i,1}, \ldots, \widetilde{\mathbb{D}}_{i,l}, \ldots, \widetilde{\mathbb{D}}_{i,L_\hbar}\}$ of DO i, it sends a request to DO i for data access and usage as follows:

$$reqMsg = \langle pk_i || pk_\hbar || contractMenu || t\text{Stamp} || \mathcal{S}_{sk_\hbar}(\psi_r) \rangle \tag{4}$$

where $L_\hbar$ is the number of requested datasets owned by DO i, $(pk_\hbar, sk_\hbar)$ is the public/secret key pair of UC $\hbar$, $contractMenu$ is a set of contract menus (i.e., data utility and payment combinations) for all types of DOs, tStamp is the timestamp of reqMsg creation, $\mathcal{S}(.)$ is the BLS short signature function, and ψ_r is the hash digest of $reqMsg$. The data access policies specify who can access what kind of data at what price, while the data usage policies specify how the data can be processed. If DO i grants consent to the UC and selects a contract item $(u(\alpha), p(\alpha))$, an access and usage policy can be generated as:

$$\begin{aligned} accPolicy = \langle & ID_{i,\hbar} || \mathcal{H}(api) || op || pk_i || pk_\hbar || \\ & u(\alpha) || p(\alpha) || e\text{Time} || i\text{Time} || \psi_a \rangle \end{aligned} \tag{5}$$

where $ID_{i,\hbar} = \{ID_{i,1}, \ldots, ID_{i,l}, \ldots, ID_{i,L_\hbar}\}$ is the identity set of dataset $\widetilde{\mathbb{D}}_{i,\hbar}$. *api* is the authorized application programming interface (API) of a certain energy service (e.g., load forecasting and dynamic pricing) provided by UC $\hbar$. *op* is the authorized operations over dataset $\widetilde{\mathbb{D}}_{i,\hbar}$ and is coded into computer programs due to the complex logic flow. eTime and iTime are the expire and issue time of $accPolicy$, respectively. ψ_a is the hash digest of $accPolicy$.

After DO i and UC $\hbar$ sign on the policy $accPolicy$ with their secret keys, the data access and usage smart contract (DAUC) is created, which is written in the form of program codes. A contract creation transaction (ccTx) can be built on the basis of smart contract code attached with the signatures of both parties. After the ccTx transaction is successfully validated by full nodes via consensus process, ccTx can be recorded in the blockchain and a contract account of DAUC (i.e., A_{DAUC}) is created which is publicly accessible for all nodes in the blockchain. The DAUC creation and deployment process is shown in the *Create* function in Algorithm 1. Here, all full nodes (i.e., aggregators) run the hybrid delegated proof of stake and Byzantine fault tolerance (DPoS-BFT) consensus protocol independently to make an agreement on the new transactions to be recorded in the blockchain. In DPoS-BFT, the M validators form the consensus committee and they are elected via a traditional stakeholder voting mechanism. Then, each of the validators takes turns to serve as the block producer for the new block generation. The newly built block is appended into the blockchain if it passes the BFT condition (i.e., it receives more than $\frac{2}{3}M$ confirm messages from distinct validators).

All the access and usage policies of personal datasets are stored in the key-value form and managed by all validators via consensus operations based on the recorded transactions. The access and usage policy A_{policy} between DO i and a certain API

Algorithm 1: Data Access and Usage Smart Contract.

Create():
Input: $accPolicy$, multi-signature $\mathcal{MS}_{\{sk_i, sk_\hbar\}}(\psi_a)$
parse $accPolicy$ as $(pk_i, pk_\hbar, \mathcal{H}(api), ID_{i,\hbar}, op, u, p, eTime)$;
if Verify$(\{pk_i, pk_\hbar\}, \mathcal{MS}_{\{sk_i, sk_\hbar\}}(\psi_a)) = true$ **then**
  $iTime \leftarrow$Time.now(), $num \leftarrow 0$, $status \leftarrow 1$;
  $A_{policy}[DO = pk_i, ESP = pk_\hbar, ID_{api} = \mathcal{H}(api)]$.append$(ID_{i,\hbar}, op, u, p, eTime, iTime, num, status)$;
  generate contract account A_{DAUC};
endif
Invoke():
Input: $deposit_\hbar$, $(pk_i, pk_\hbar, \mathcal{H}(api))$
$policy \leftarrow A_{policy}[pk_i, pk_\hbar, \mathcal{H}(api)]$.getPolicy();
$iTime \leftarrow policy$.getIssuedTime();
$eTime \leftarrow policy$.getExpireTime();
$p \leftarrow policy$.getPayment();
if Time.now() – $iTime \leq eTime$ && Verify$(deposit_\hbar \geq p)$ && isAthorized$(policy)$ **then**
  freeze $deposit_\hbar$;
endif
Complete():
$p \leftarrow A_{policy}[pk_i, pk_\hbar, \mathcal{H}(api)]$.getPolicy().getPayment();
receive σ_{comp} from blockchain;
if Verify$(\sigma_{comp}) = true$ **then**
  send(w_i, p);
  send$(w_\hbar, deposit_\hbar - p)$;
  $A_{policy}[pk_i, pk_\hbar, \mathcal{H}(api)]$.update$(num \mathrel{+}= 1)$;
end if
Revoke():
Input: $(pk_i, pk_\hbar, \mathcal{H}(api))$, $\mathcal{S}_{sk_i}$
if Verify$(pk_i, \mathcal{S}_{sk_i}) = true$ **then**
  $A_{policy}[pk_i, pk_\hbar, \mathcal{H}(api)]$.update$(status = 0)$;
  self-destruct;
end if

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

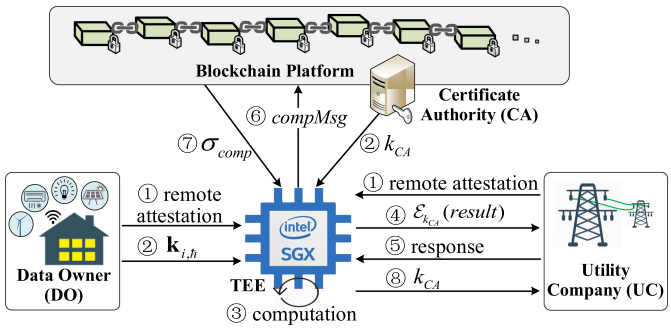


Fig. 3. Workflow of off-chain smart contract execution with TEE.

of UC is denoted as

$$A_{\text{policy}} = \Big\{ \underbrace{\{pk_i||pk_\hbar||\mathcal{H}(api)\}}_{\text{key}}, \underbrace{\{ID_{i,\hbar}||op||u||p||e\text{Time}||i\text{Time}||num||status\}}_{\text{value}} \Big\} \tag{6}$$

where num is the usage count. $status = \{0, 1\}$ is a binary variable, where 1 means the policy is approved while 0 indicates it is revoked. The UC can lookup the DAUC contract and check its policy status by synchronizing the latest blockchain data. Then, to invoke the DAUC contract, UC can send a deposit transaction to the contract account A_{DAUC} by moving enough deposits from its account to A_{DAUC}. After that, the accounts of involved entities are locked and frozen. The DAUC invocation process is shown in the *invoke* function in Algorithm 1.

C. Off-Chain Smart Contract Execution With TEE

In the existing blockchain, data and computation involved in smart contracts (e.g., user input and contract state) need to be replicated for all validators to publicly verify whether the contract is correctly executed. As the user input, e.g., private energy data, generally contains sensitive user information, the lack of privacy fundamentally impedes the adoption of smart contracts for personal data computation. A TEE-based off-chain smart contract execution mechanism is proposed to tackle this challenge. Here, the computation of sensitive personal data is executed within the TEE enclave to ensure data confidentiality, and the delivery of computing results and data payment can be facilitated with the smart contract. The detailed workflow is illustrated in Fig. 3.

The orchestration of blockchain and TEE faces two critical challenges. The first is the correct execution of smart contract functions in TEE. To efficiently authenticate the loaded program and data in the TEE enclave, we use the concept of "local consensus" by employing remote attestation between the contracting parties, namely, the DO as data provider and the UC as data consumer. In traditional approaches, the correctness of contract computation requires the acknowledgment of the entire network, which contradicts with our privacy protection goals if the private datasets are directly accessible to all entities. Based on the observation in work [36], the correctness of off-chain contract computation only matters to the contracting parties involved in the data trading. Accordingly, the consensus process can be narrowed only to the contracting participants by using software remote attestation to remotely verify the authenticity of the loaded program and data in the TEE enclave.

In remote attestation [25], a proof of correct configuration and execution (i.e., a digital signature using a secret key which is only known by the hardware) can be generated by the TEE. Attestation is a type of challenge-response protocol, where the enclave generates a digital signature on the current configuration and replies to the challenger, meanwhile the challenger can verify the authenticity of the signature and check whether configurations are as expected. By establishing encrypted and authenticated channels to the enclave, both sides of contracting entities can remotely attest the loaded program and data[1] (including smart contract configurations, API program (from the UC), encrypted private subdatasets (from the cloud), and the computation to be executed) in TEE and validate its correctness and authenticity. Only if both DO and UC reach an agreement on the loaded program and data and the compliances of operations to be performed within the TEE enclave via remote attestation (step ①), the off-chain smart contract execution will continue. Then, DO delivers its decryption keys $\mathbf{k}_{i,\hbar} = \{k_{i,1}, \ldots, k_{i,l}, \ldots, k_{i,L_\hbar}\}$ of the encrypted datasets $\widetilde{\mathbb{D}}_{i,\hbar}$ to TEE, and CA delivers the symmetric key k_{CA} to TEE for encryption of computing results (step ②). Next, TEE performs the off-chain contract execution and obtains the computing results result (i.e., extracted knowledge from the personal datasets) (step ③). Here, result $= op(\mathcal{D}_{\mathbf{k}_{i,\hbar}}(\widetilde{\mathbb{D}}_{i,\hbar}))$, where op is the contractual operations for data processing, and $\mathcal{D}(.)$ is the decryption function.

The next challenge is the atomic delivery of computing result $result$ to UC and payment $p(\alpha)$ to DO. To prevent UC from acquiring the computing results without finishing the payment to DO, a two-phase atomic delivery protocol is developed as follows. When off-chain computation ends, the TEE delivers the encrypted results $\mathcal{E}_{k_{\text{CA}}}(result)$ with its signature to the UC via a secure channel (step ④). After UC checks the authenticity of the signature and sends a response message as an acknowledgment of the receipt (step ⑤), the TEE sends a computation completion message $compMsg$ with its signature to the blockchain (step ⑥). Finally, after observing a proof of publication of $compMsg$, i.e., σ_{comp} (step ⑦), TEE sends the decryption key k_{CA} to UC (step ⑧). Here, σ_{comp} is the multisignature of validators on $compMsg$, and it is valid after signed by over two thirds of validators. As TEE's delivery of $compMsg$ can be verified by σ_{comp}, only if σ_{comp} has been generated (i.e., DO will get the payment according to the DAUC contract), the description key is then released (i.e., UC acquires the computing results). Thereby,

[1]It is worth noting that, due to the memory limit of SGX enclave in the current design, considerable performance degradation may occur when the running codes exceed the working memory. Existing works such as SCONE [37] and Occlumency [38] can be employed to alleviate memory usage in knowledge extraction with guaranteed security. Besides, as shown in [7], SPDS would still be much more efficient than homomorphic cryptosystems, even in the case of memory exceeding.

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

the atomic delivery can be ensured. The DAUC completion process is shown in the *Complete* function in Algorithm 1. Besides, for better control of private energy data, DO i can revoke the granted access and usage permissions, as shown in the *Revoke* function in Algorithm 1. Besides, to prevent malicious DOs from sharing falsified datasets, existing reputation mechanisms [31] can be utilized to identify dishonest DOs via feedback aggregation and trustworthiness evaluation.

D. Security Analysis

The proposed SPDS approach can effectively defend against the adversaries defined in Section III-B during private energy data sharing.

In SPDS, since the personal energy datasets are encrypted by each DO before storing in the cloud database, and the symmetric key for encryption/decryption is generated by the DO herself and keeps secret to others, the cloud server can only access the encrypted version of user's private data. As a consequence, the risks arisen from *honest-but-curious cloud* in off-chain data storage can be prevented.

In SPDS, the exchange of cryptocurrency and processing outcome between each DO and the UC is automatically and atomically executed by the DAUC smart contract in a prescribed fashion. Meanwhile, as the data usage activities of UC are publicly recorded in the immutable blockchain ledgers, the UC cannot repudiate them and refuse to pay. Additionally, the dishonest DOs who trade fake and irrelevant datasets can suffer a considerable reputation decrease and be penalized by the reputation mechanisms. Accordingly, the *repudiation and fraud attack* can be effectively defended.

In SPDS, the shared private energy data can only be accessed by authorized entities (i.e., API of ESPs) and processed under intended purposes, where the fine-granular user-defined access policies are enforced by the DAUC smart contract. The historical data usage activities are recorded in the form of transactions (as verifiable proof) and transparently stored in the unforgeable ledgers, which are publicly auditable for policy compliance. By adopting DPaaS mode, only the processed results instead of the source data are shared to the ESP; meanwhile, all involved keys and intermediate results in TEE-based off-chain smart contract execution can be securely erased via remote attestation when data computation ends. As a result, the control of shared private data can be fully brought back to individual DOs, and the privacy breaches due to *misuse of shared personal data* can be effectively prevented.

E. Optimal Incentive Mechanism Design

To stimulate users' participation and high-quality data sharing, the monopolistic ESP (i.e., UC) offers a group of contract menus $\Phi = \{(u(\alpha_i), p(\alpha_i)), \forall \alpha_i \in \mathbb{A}\}$ for DOs in set $\mathbb{I}$ with distinct privacy preferences (i.e., types α_i). Here, $u(\alpha_i)$ is the data utility of the shared private data of type-α_i DO, and $p(\alpha_i)$ is the corresponding payment to her as a compensation for the privacy loss in data sharing. For ease of interpretability of the contract, we define the normalized data utility $\pi(\alpha_i) \triangleq u(\alpha_i)/u_{\max}$ as a replacement of the contract item, where $u_{\max}$ is the maximum data utility that each DO can contribute. If DO i selects the contract item $(\pi(\alpha_i), p(\alpha_i))$, her payoff can be given as

$$\Im(\alpha_i) = p(\alpha_i) - \varpi_p \alpha_i \pi(\alpha_i) u_{\max} \tag{7}$$

where $\alpha_i u(\alpha_i)$ represents the expected value of privacy loss of DO i in data sharing, and ϖ_p is an adjustment coefficient to balance the income and privacy cost. The DO's privacy preference α is private and only known by the DO herself, while the probability density function (PDF) $g(\alpha)$ and cumulative distribution function (CDF) $G(\alpha)$ can be known by UC [39], [40]. The expected payoff of UC in data trading with all DOs in set $\mathbb{I}$ can be defined as

$$\Re = I \int_{\underline{\alpha}}^{\overline{\alpha}} [\varpi_s \ln(1 + \pi(\alpha) u_{\max}) - p(\alpha)] g(\alpha) d\alpha \tag{8}$$

where the first item inside the integral (i.e., $\ln(1 + u(\alpha))$) means the satisfaction of UC in acquiring data utility $u(\alpha)$ when trading with type-α DO. ϖ_s is an adjustment coefficient to balance the satisfaction and payment. Here, based on [19], [20], and [41], the natural logarithmic function, which is widely adopted in modeling user satisfaction, is applied in our work to formulate the relationship between UC's satisfaction and the acquired data utility. According to the contract theory, the effective contracts need to guarantee that each DO will accept the contract designed for her (referred as *incentive compatible (IC) constraint*) and obtain a nonnegative payoff (referred as *individual rationality (IR) constraint*).

Definition 1 (IC): A contract satisfies IC if the best response of type-α DO is to truthfully choose the contract for its type rather than other contracts, i.e., $\forall(\alpha, \hat{\alpha}) \in \mathbb{A}$,

$$p(\alpha) - \varpi_p \alpha \pi(\alpha) u_{\max} \geq p(\hat{\alpha}) - \varpi_p \alpha \pi(\hat{\alpha}) u_{\max}. \tag{9}$$

Definition 2 (IR): A contract satisfies IR if it yields a nonnegative payoff for each type of DO, i.e.,

$$p(\alpha) - \varpi_p \alpha \pi(\alpha) u_{\max} \geq 0, \forall \alpha \in \mathbb{A}. \tag{10}$$

Apart from IC and IR constraints, in order to ensure the accuracy of computing results and derive meaningful insights from the shared data, the total data utility contributed by a set of DOs should be no less than the minimum requirement u_{req}. For the sake of simplicity, based on work [29], the summation of each DO's data utility is employed to represent the total data utility. As such, a feasible contract should meet the following isoperimetric constraint:

$$I \int_{\underline{\alpha}}^{\overline{\alpha}} \pi(\alpha) u_{\max} g(\alpha) d\alpha = u_{\text{req}}. \tag{11}$$

Besides, the data utility contributed by each DO should be bounded, i.e.,

$$0 \leq \pi(\alpha) \leq 1. \tag{12}$$

The objective of UC is to design the optimal contract menus which maximize its payoff while meeting the abovementioned constraints. The optimization problem is formulated as follows:

$$\begin{aligned} (\mathbf{P1}) \quad & \max_{\{(\pi(\alpha), p(\alpha))\}} \Re \\ & \text{s.t. } (9), (10), (11), (12). \end{aligned} \tag{13}$$

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

Due to the complexity of IC and IR constraints, it is nontrivial to directly solve the problem $\mathbf{P1}$. First, we need to simplify the IC and IR constraints.

Theorem 1: The IC constraints can be reduced to a monotonicity constraint and a differential equation as follows:

$$\begin{cases} \dot{\pi}(\alpha) \leq 0 & (14) \\ \dot{\Im}(\alpha) = -\varpi_p \pi(\alpha) u_{\max} & (15) \end{cases}.$$

Proof: 1) Necessity: Suppose $p(\alpha)$ and $\pi(\alpha)$ are differentiable. According to IC constraints in (9), given α, the function $\Pi(\hat{\alpha}) \triangleq p(\hat{\alpha}) - \varpi_p \alpha u(\hat{\alpha}) u_{\max}$ attains its maximized value at $\hat{\alpha} = \alpha$. As such, the following two conditions hold:

$$\frac{d\Pi(\hat{\alpha})}{d\hat{\alpha}}|_{\hat{\alpha}=\alpha} = \frac{dp(\alpha)}{d\alpha} - \varpi_p \alpha \frac{du(\alpha)}{d\alpha} u_{\max} = 0 \quad (16)$$

$$\frac{d^2\Pi(\hat{\alpha})}{d\hat{\alpha}^2}|_{\hat{\alpha}=\alpha} = \frac{d^2p(\alpha)}{d\alpha^2} - \varpi_p \alpha \frac{d^2u(\alpha)}{d\alpha^2} u_{\max} \leq 0. \quad (17)$$

By differentiating (16) with respect to α, formula (17) can be rewritten as $\frac{d\pi(\alpha)}{d\alpha} \leq 0$. Substituting (16) into (7), (16) can be expressed in a concise manner, i.e., $\frac{d\Im(\alpha)}{d\alpha} = -\varpi_p u(\alpha) u_{\max}$.

2) Sufficiency: Suppose that there exists at least a contract for type-α DO that violates IC constraint, i.e., $p(\alpha) - \varpi_p \alpha \pi(\alpha) u_{\max} < p(\hat{\alpha}) - \varpi_p \alpha \pi(\hat{\alpha}) u_{\max}$, $\hat{\alpha} \neq \alpha$. It can be expressed in the form of integration

$$\Theta = \int_{\alpha}^{\hat{\alpha}} \left(\frac{dp(\nu)}{d\nu} - \varpi_p \alpha u_{\max} \frac{d\pi(\nu)}{d\nu} \right) d\nu > 0. \quad (18)$$

Here, we assume $\hat{\alpha} > \alpha$, as the other case $\hat{\alpha} < \alpha$ can be analyzed similarly. According to (7), (14), and (15), we have $\frac{dp(\nu)}{d\nu} = \varpi_p \nu u_{\max} \frac{d\pi(\nu)}{d\nu}$ and $\frac{d\pi(\nu)}{d\nu} \leq 0$. For $\nu \in [\alpha, \hat{\alpha}]$, we attain $\Theta = \int_{\alpha}^{\hat{\alpha}} (\varpi_p u_{\max}(\nu - \alpha) \frac{d\pi(\nu)}{d\nu}) d\nu \leq 0$, where a contradiction occurs. As such, IC constraints hold for all types of DOs. Theorem 1 is proved. ■

According to (15), we have $\frac{d\Im(\alpha)}{d\alpha} \leq 0$. Hence, the IR constraints in formula (10) can be simplified as

$$\Im(\overline{\alpha}) \geq 0. \quad (19)$$

Then, the optimization problem $\mathbf{P1}$ can be rewritten as

$$(\mathbf{P2}) \max_{\{(\pi(\alpha), \Im(\alpha))\}} \int_{\underline{\alpha}}^{\overline{\alpha}} \begin{bmatrix} \varpi_s \ln(1 + \pi(\alpha) u_{\max}) \\ -\Im(\alpha) - \varpi_p \alpha \pi(\alpha) u_{\max} \end{bmatrix} g(\alpha) d\alpha$$
$$\text{s.t.} \quad (14), (15), (19), (11), (12). \quad (20)$$

In $\mathbf{P2}$, we focus on the design of contract $(\pi(\alpha), \Im(\alpha))$, as the optimal $p(\alpha)$ can be easily obtained when the optimal $\pi(\alpha)$ and $\Im(\alpha)$ are derived. According to the optimal control theory, in $\mathbf{P2}$, $\Im(\alpha)$ can be seen as the state variable, while $\pi(\alpha)$ can be regarded as the control variable. For ease of expression, we define $x_1(\alpha) \triangleq \Im(\alpha)$ and $y(\alpha) \triangleq \pi(\alpha)$. Besides, another state variable $x_2(\alpha)$ is defined to cope with the constraint (11) such that $\dot{x}_2(\alpha) \triangleq y(\alpha) g(\alpha) u_{\max}$. The upper boundary condition of $x_2(\alpha)$ is $x_2(\overline{\alpha}) = u_{\text{req}}/I$. The Hamiltonian function of problem $\mathbf{P2}$ can be formulated as

$$\begin{aligned} &F(\alpha, \boldsymbol{x}(\alpha), y(\alpha), \boldsymbol{\lambda}(\alpha)) \\ &= [\varpi_s \ln(1 + y(\alpha) u_{\max}) - x_1(\alpha) - \varpi_p \alpha y(\alpha) u_{\max}] g(\alpha) \\ &\quad - \lambda_1(\alpha) \varpi_p y(\alpha) u_{\max} + \lambda_2(\alpha) y(\alpha) g(\alpha) u_{\max} \end{aligned} \quad (21)$$

where $\lambda_1(\alpha)$ and $\lambda_2(\alpha)$ are costate variables. Furthermore, we define $\boldsymbol{x}(\alpha) = [x_1(\alpha), x_2(\alpha)]^{\mathrm{T}}$ and $\boldsymbol{\lambda}(\alpha) = [\lambda_1(\alpha), \lambda_2(\alpha)]^{\mathrm{T}}$. Based on the Pontryagin minimum principle, the optimal solution $[\boldsymbol{x}^*(\alpha), y^*(\alpha)]$ of problem $\mathbf{P2}$ should meet the following conditions:

$$\begin{cases} \dot{x}_1^*(\alpha) = \dfrac{\partial F(\alpha, \boldsymbol{x}^*(\alpha), y^*(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial \lambda_1(\alpha)} = -\varpi_p y^*(\alpha) u_{\max} & (22) \\ \dot{x}_2^*(\alpha) = \dfrac{\partial F(\alpha, \boldsymbol{x}^*(\alpha), y^*(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial \lambda_2(\alpha)} = y^*(\alpha) g(\alpha) u_{\max} & (23) \\ \dot{\lambda}_1^*(\alpha) = -\dfrac{\partial F(\alpha, \boldsymbol{x}^*(\alpha), y^*(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial x_1(\alpha)} = g(\alpha) & (24) \\ \dot{\lambda}_2^*(\alpha) = -\dfrac{\partial F(\alpha, \boldsymbol{x}^*(\alpha), y^*(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial x_2(\alpha)} = 0 & (25) \\ \lambda_1^*(\underline{\alpha}) = 0 & (26) \\ F(\alpha, \boldsymbol{x}^*(\alpha), y^*(\alpha), \boldsymbol{\lambda}^*(\alpha)) \geq F(\alpha, \boldsymbol{x}^*(\alpha), y(\alpha), \boldsymbol{\lambda}^*(\alpha)). & (27) \end{cases}$$

Combing (24) with (26), we can obtain $\lambda_1^*(\alpha) = G(\alpha)$. From (25), we have $\lambda_2^*(\alpha) = \beta$, where β is a constant. Next, we solve the optimal unbounded $\tilde{y}^*(\alpha)$ without the boundary constraint (12). We follow [39], [40] in supposing that the type of DO follows the uniform distribution, i.e., $g(\alpha) = \frac{1}{\overline{\alpha} - \underline{\alpha}}$ and $G(\alpha) = \frac{\alpha - \underline{\alpha}}{\overline{\alpha} - \underline{\alpha}}$. To derive the optimal contracts, we first give the following two lemmas.

Lemma 1: The optimal data utility function $\pi^*(\alpha)$ exactly equals to its unbounded form $\tilde{y}^*(\alpha)$, i.e., $\pi^*(\alpha) = \tilde{y}^*(\alpha)$, if the following condition holds:

$$\frac{\varpi_s}{\varpi_s - 2\varpi_p(\overline{\alpha} - \underline{\alpha})} \leq \Lambda \leq \frac{2\varpi_p(1 + u_{\max})(\overline{\alpha} - \underline{\alpha})}{\varpi_s} + 1 \quad (28)$$

where $\Lambda = e^{\frac{2\varpi_p}{\varpi_s}(\overline{\alpha} - \underline{\alpha})(\frac{u_{req}}{I} + 1)}$.

Proof: In (21), the second derivative of $F(\alpha, \boldsymbol{x}(\alpha), y(\alpha), \boldsymbol{\lambda}(\alpha))$ with respect to y satisfies: $\frac{\partial^2 F(\alpha, \boldsymbol{x}^*(\alpha), y(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial y^2}|_{y=\tilde{y}^*} < 0$. Under the first-order optimality condition

$$\frac{\partial F(\alpha, \boldsymbol{x}^*(\alpha), y(\alpha), \boldsymbol{\lambda}^*(\alpha))}{\partial y}|_{y=\tilde{y}^*} = 0 \quad (29)$$

we can obtain $\tilde{y}^*(\alpha) = \frac{\varpi_s}{(2\alpha - \underline{\alpha})\varpi_p u_{\max} - \beta} - 1$. According to (11), we can derive

$$\beta = \frac{\varpi_p u_{\max}}{\Lambda - 1}(\Lambda \underline{\alpha} + \underline{\alpha} - 2\overline{\alpha}). \quad (30)$$

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

Then, $\tilde{y}^*(\alpha)$ can be simplified as

$$\tilde{y}^*(\alpha) = \frac{\varpi_s(\Lambda-1)}{2\varpi_p u_{\max}\left[(\Lambda-1)\alpha+\overline{\alpha}-\Lambda\underline{\alpha}\right]} - \frac{1}{u_{\max}}. \quad (31)$$

Note that $\Lambda > 1$ and $\tilde{y}^*(\alpha)$ is monotonically decreasing with respect to α. Let α_θ^1 and α_θ^2 be the intersection points of $\tilde{y}^*(\alpha)$ with lines $y(\alpha)=1$ and $y(\alpha)=0$, respectively. By adjusting system parameters, we can ensure that $\alpha_\theta^1 \le \underline{\alpha}$ and $\alpha_\theta^2 \ge \overline{\alpha}$ hold simultaneously. The corresponding condition for them can be derived as shown in formula (28). In this case, the optimal data utility function $\pi^*(\alpha)$ exactly equals to its unbounded form $\tilde{y}^*(\alpha)$, i.e., $\pi^*(\alpha) = \tilde{y}^*(\alpha)$. Thus, Lemma 1 is proved. ■

Lemma 2: The constraint (19) must be binding at the optimum, i.e., $\Im^*(\overline{\alpha}) = 0$.

Proof: We prove this lemma by contradiction. Suppose that $\Im^*(\overline{\alpha}) > 0$. Then, UC can decrease $\Im^*(\overline{\alpha})$ by a small amount while making $\pi^*(\alpha)$ unchanged. Hence, the payoff of UC can be increased, which contradicts with the optimality of $\Im^*(\overline{\alpha})$. As such, $\Im^*(\overline{\alpha})$ should equal to zero and Lemma 2 is proved. ■

Based on Lemmas 1 and 2, by using (22), the optimal $\Im^*(\alpha)$ can be derived as

$$\Im^*(\alpha) = \frac{\varpi_s u_{\max}}{2} \ln\left[\frac{\Lambda(\overline{\alpha}-\underline{\alpha})}{(\Lambda-1)\alpha+\overline{\alpha}-\Lambda\underline{\alpha}}\right] - \varpi_p(\overline{\alpha}-\underline{\alpha}). \quad (32)$$

By using (7), the optimal payment function $p^*(\alpha)$ is attained by

$$p^*(\alpha) = \Im^*(\alpha) + \varpi_p \alpha \pi^*(\alpha) u_{\max}. \quad (33)$$

Based on (32) and (33), the UC can design the optimal contract items, i.e., $\Phi^* = \{(\Im^*(\alpha), p^*(\alpha)), \forall \alpha \in \mathbb{A}\}$, for all types of DOs.

V. Performance Evaluation

In this section, the simulation setup is first introduced, followed by the discussion of numerical results.

A. Simulation Setup

We consider a simulation scenario of personal data sharing in smart grid with $I = 500$ individuals (i.e., DOs) and one UC. The type of DOs is uniformly distributed between $\underline{\alpha} = 0$ and $\overline{\alpha} = 1$. For the data utility model, we set $\mu_1 = 0.4804$, $\mu_2 = 0.2789$, $\mu_3 = 1-\mu_1$, and $u_{\max} = 10$. For the payoff models, we set $\varpi_p = 0.3$ and $\varpi_s = 6.5$. For comparison, we choose different u_{req} from the set $\{0.6Iu_{\max}, 0.7Iu_{\max}, 0.8Iu_{\max}\}$. The inside integral in (8), i.e., $\Re(\alpha) = \varpi_s \ln(1+\pi(\alpha)u_{\max}) - p(\alpha)$, is used to evaluate the payoff of UC when trading with type-α DO. Besides, we compare the performance of our proposed scheme with two conventional schemes as follows.

1) *Linear contract scheme (LC):* In LC scheme, the payment in contract is in linear proportion to the contributed data utility for each type of DO.
2) *Fixed price scheme (FP):* In FP scheme, UC specifies the same unit price of data utility for all types of DOs.

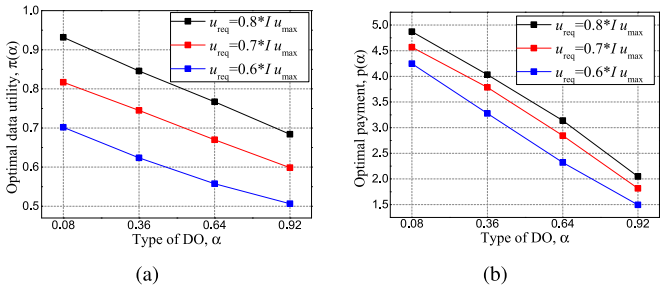


Fig. 4. (a) Optimal data utility versus type of DO. (b) Optimal payment versus type of DO.

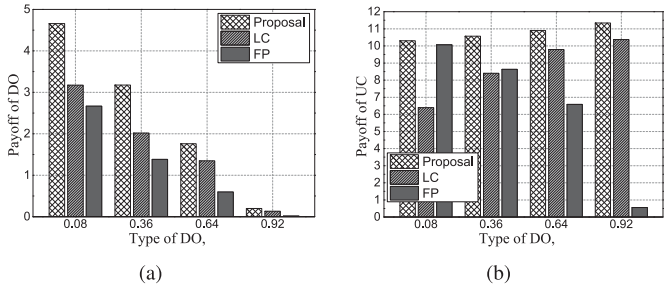


Fig. 5. Comparison of proposed scheme with LC and FP schemes in terms of (a) optimal data utility; (b) optimal payment, where $u_{\text{req}} = 0.8Iu_{\max}$.

B. Numerical Results

Fig. 4 shows the optimal data utility and optimal payment in contracts when the type of DO (i.e., α) increases from 0.08 to 0.92. Here, three values of u_{req} are exploited, i.e., $0.6Iu_{\max}$, $0.7Iu_{\max}$, and $0.8Iu_{\max}$, respectively. As depicted in Fig. 4(a) and (b), both the data utility and payment in the optimal contracts decrease with the increase of DO's type. The reason is that the higher type of DO indicates higher privacy preference and higher DSL, which results in reduced data utility and the corresponding lower payment to DO. Besides, we can observe that with the increase of u_{req}, both the optimal data utility and optimal payment increase. The reason is that to meet the high data utility requirement, UC intends to increase the payments to DOs to motivate their high data utility contribution.

Fig. 5 shows the comparison of the proposed scheme with two conventional schemes in terms of the payoffs of DOs and UC, where the type of DO increases from 0.08 to 0.92. Here, we set $u_{\text{req}} = 0.8Iu_{\max}$. From Fig. 5(a) and (b), we can see that, given different α, our proposed scheme outperforms the LC and FP schemes in attaining higher payoffs for both DO and UC. It can be explained as follows. In the FP scheme, since the identical and fixed unit price is offered to all types of DOs, the UC cannot improve its payoff by adjusting the unit price. In the LC scheme, the payment to DO is linear with her contributed data utility, leading to a slow improvement of UC's payoff. Besides, in the LC scheme, data contributors can relatively improve their payoffs than the FP scheme as the unit price for each DO type is adjustable. In the proposed scheme, due to the nonlinear relationship between data payment and contributed data utility, both the data consumer and data contributor can

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

attain optimal payoffs by designing and selecting the optimal contract menus, respectively. In addition, as seen in Fig. 5(a) and (b), with an increase of α, the payoff of DO drops while that of UC keeps increasing. The reason is that DO with large type tends to share data with low utility, resulting in a low payment and a corresponding low payoff, which accords with the theoretical analysis in (32). Besides, under the system parameter setting, the derivation of optimal payoff function $\Re(\alpha)$ with respect to α is positive, leading to an increased $\Re(\alpha)$ when α grows.

VI. Conclusion

In this article, we proposed a novel blockchain-based solution for secure and auditable private data sharing in smart grids. First, by leveraging blockchain and smart contracts, a trust-free framework was presented for privacy-preserving data computation, fine-grained data access and usage control, nonrepudiable data usage tracking, and verifiable proof of policy compliance. Second, a TEE-enabled off-chain smart contract execution mechanism with atomic operation guarantee was developed for confidential user data processing and the alleviation of computation overhead in blockchain. Furthermore, a contract theoretical incentive model was devised in the presence of information asymmetry to stimulate user's participation and high-quality data sharing by designing optimal contracts. Extensive simulations demonstrated the effectiveness of the proposed scheme in terms of improved payoffs for participants, compared with conventional approaches. For the future work, the blockchain-based collaborative learning mechanism for data sharing, the memory-efficient inference algorithm for knowledge extraction in TEEs, and the optimal contract design without prior knowledge of user type distribution will be investigated.

References

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019.

[2] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.

[3] Y. Liu, Z. Su, K. Zhang, A. Benslimane, and D. Fang, "Defending malicious check-in using big data analysis of indoor positioning system: An access point selection approach," *IEEE Trans. Netw. Sci. Eng.*, early access, doi: 10.1109/TNSE.2020.3014384.

[4] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[5] J. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin, "Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 247–257, Jan. 2020.

[6] W. Li, Z. Su, K. Zhang, and X. Qi, "Abnormal crowd traffic detection with crowdsourcing-based rss fingerprint position in heterogeneous communications networks," *IEEE Trans. Netw. Sci. Eng.*, early access, doi: 10.1109/TNSE.2020.3014380.

[7] S. Li, K. Xue, D. S. L. Wei, H. Yue, N. Yu, and P. Hong, "Secgrid: A secure and efficient SGX-enabled smart grid system with rich functionalities," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1318–1330, 2020.

[8] "General data protection regulation," GDPR, May 2018. [Online]. Available: https://gdpr-info.eu/

[9] D. Hardt, "The OAuth 2.0 authorization framework," Jul. 2012. [Online]. Available: https://tools.ietf.org/id/draft-ietf-oauth-v2-31.html

[10] S. Qi, Y. Lu, Y. Zheng, Y. Li, and X. Chen, "CPDs: Enabling compressed and private data sharing for industrial IoT over blockchain," *IEEE Trans. Ind.l Informat.*, to be published.

[11] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1746–1761, 2020.

[12] J. Feng, L. T. Yang, R. Zhang, and B. S. Gavuna, "Privacy preserving tucker train decomposition over blockchain-based encrypted industrial IoT data," *IEEE Trans. Ind.l Informat.*, to be published.

[13] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 725–737, 2020.

[14] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, 2015, pp. 180–184.

[15] K. Fan *et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020.

[16] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[17] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy*, 2016, pp. 839–858.

[18] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[19] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[20] K. Liu, X. Qiu, W. Chen, X. Chen, and Z. Zheng, "Optimal pricing mechanism for data market in blockchain-enhanced Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9748–9761, Dec. 2019.

[21] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1229–1241, Jun. 2020.

[22] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward secure data sharing for the iov: A quality-driven incentive mechanism with on-chain and off-chain guarantees," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1625–1640, Mar. 2020.

[23] G. Luo *et al.*, "Software defined cooperative data sharing in edge computing assisted 5G-VANET," *IEEE Trans. Mobile Comput.*, to be published.

[24] Y. Wang, Z. Su, Q. Xu, T. Yang, and N. Zhang, "A novel charging scheme for electric vehicles with smart communities in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8487–8501, Sep. 2019.

[25] I. Anati, S. Gueron, S. P. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," *ACM*, New York, NY, USA, vol. 13, p. 7, 2013.

[26] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptology ePrint Archive*, vol. 2016, no. 86, pp. 1–118, 2016. [Online]. Available: https://eprint.iacr.org/2016/086.pdf

[27] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secure Comput.*, to be published.

[28] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, to be published.

[29] L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? A contract theoretic approach," *IEEE J. Sel. Top. Signal Process.*, vol. 9, no. 7, pp. 1256–1269, Oct. 2015.

[30] Y. Zhan, P. Li, Z. Qu, D. Zeng, and S. Guo, "A learning-based incentive mechanism for federated learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6360–6368, Jul. 2020.

[31] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 700–10 714, Dec. 2019.

[32] W. Wang *et al.*, "Leaky cauldron on the dark land: Understanding memory side-channel hazards in SGX," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2017, pp. 2421–2434.

[33] J. V. Bulck *et al.*, "Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution," in *Proc. USENIX Secur. Symp.*, Baltimore, MD, USA, Aug. 2018, pp. 991–1008.

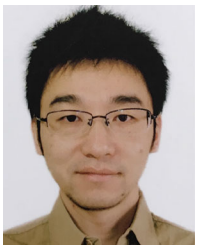
[34] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *Advances in Cryptology – ASIACRYPT 2018*. Berlin, Germany: Springer, 2018, pp. 435–464.

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.

[35] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.
[36] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Privacyguard: Enforcing private data usage control with blockchain and attested off-chain contract execution," in *Computer Security – ESORICS 2020*. Berlin, Germany: Springer, 2020, pp. 610–629.
[37] S. Arnautov *et al.*, "SCONE: Secure linux containers with intel SGX," in *Proc. USENIX Symp. Operating Syst. Des. Implementation*, Savannah, GA, USA, Nov. 2016, pp. 689–703.
[38] T. Lee *et al.*, "Occlumency: Privacy-preserving remote deep-learning inference using SGX," in *Proc. 25th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, 2019.
[39] Z. Zheng, Y. Peng, F. Wu, S. Tang, and G. Chen, "Trading data in the crowd: Profit-driven data acquisition for mobile crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 2, pp. 486–501, Feb. 2017.
[40] Z. Su, Q. Xu, J. Luo, H. Pu, Y. Peng, and R. Lu, "A secure content caching scheme for disaster backup in fog computing enabled mobile social networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4579–4589, Oct. 2018.
[41] H. Oh, S. Park, G. M. Lee, J. K. Choi, and S. Noh, "Competitive data trading model with privacy valuation for multiple stakeholders in iot data markets," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3623–3639, Apr. 2020.

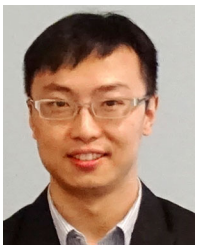
Yuntao Wang is working toward the Ph.D. degree with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China.

His research interests include security and privacy in wireless network architecture and vehicular networks.



Zhou Su received the Ph.D degree from Waseda University, Tokyo, Japan, in 2003.

Prof. Su received the best paper award of IEEE International Conference on Communications 2020, IEEE International Conference on Big Data 2019, IEEE Cyber Science and Technology Congress 2017, and Conference on Wireless Internet 2016. He is an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, and IEEE Open Journal of Computer Society. He is the Chair of the Multimedia Services and Applications over Emerging Networks Interest Group of the IEEE Comsoc Society, the Multimedia Communications Technical Committee.



Ning Zhang (Senior Member, IEEE) received the Ph.D. degree from University of Waterloo, Waterloo, ON, Canada, in 2015.

He was a Postdoc Research Fellow with the University of Waterloo and the University of Toronto, Canada, respectively. He is currently an Associate Professor with the University of Windsor, Canada.

Dr. Zhang received the Best Paper Awards from IEEE Globecom in 2014, IEEE International Conference on Wireless Communications and Signal Processing in 2015, and Journal of Communications and Information Networks in 2018, IEEE International Conference on Communications in 2019, IEEE Technical Committee on Transmission Access and Optical Systems in 2019, and IEEE International Conference on Computer and Communications in 2019, respectively. He was an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE ACCESS, and *IET Communications*, and *Vehicular Communications* (Elsevier); and a Guest Editor of several international journals, such as IEEE Wireless Communications, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He also serves/served as a track chair for several international conferences and a Co-Chair for several international workshops.

Jianfei Chen received the master's degree from Peking University, Beijing, China, in 2013.

He is currently a Researcher with State Grid Shandong Electric Power Company. His current research interests include data security and IoT security.

Xin Sun received the master's degree from Zhejiang University, Hangzhou, China, in 2006.

He is currently a Researcher with State Grid Zhejiang Electric Power Company. His current research interests include penatration test and IoT security.

Zhiyuan Ye received the master's degree from the University of Science and Technology of China, Hefei, China, in 2015.

He is currently a Senior Engineer with the Anhui Jiyuan Software Company, Ltd. His current research interests include industrial Internet of Things, 5G, software defined networking, and cloud computing.

Zhenyu Zhou (Senior Member, IEEE) received the M.E. and Ph.D. degree from Waseda University, Tokyo, Japan, in 2008 and 2011, respectively.

From September 2012 to April 2019, he was an Associate Professor with the School of Electrical and Electronic Engineering, North China Electric Power University, China. Since April 2019, he has been a Full Professor with the same university. His research interests include resource allocation in device-to-device communications, machine-to-machine communications, smart grid communications, and Internet of Things.

Prof. Zhou was the recipient of the IET Premium Award in 2017, the IEEE Globecom 2018 Best Paper Award, the IEEE International Wireless Communications and Mobile Computing Conference 2019 Best Paper Award, and the IEEE Communications Society Asia-Pacific Board Outstanding Young Researcher. He is a senior member of Chinese Institute of Electronics and China Institute of Communications. He was an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE ACCESS, *EURASIP Journal on Wireless Communications and Networking*, and a Guest Editor for the *IEEE Communications Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and Transactions on Emerging Telecommunications Technologies.

Authorized licensed use limited to: VIT University. Downloaded on September 17,2023 at 09:46:26 UTC from IEEE Xplore. Restrictions apply.