Hindawi
Security and Communication Networks
Volume 2023, Article ID 9621839, 11 pages
https://doi.org/10.1155/2023/9621839

Research Article

Blockchain-Based Privacy-Preserving Sensor Data Sharing with Fine-Grained Authorization in Microgrid

Jinhu Yu, Yue Han, Kai Zhang, Siyuan Chen, and Jinguo Li

College of Computer Science and Technology, Shanghai University of Electric Power China, Shanghai, China

Correspondence should be addressed to Jinguo Li; lijg@shiep.edu.cn

Received 28 July 2022; Revised 7 September 2022; Accepted 3 October 2022; Published 11 May 2023

Academic Editor: Zheng Yang

Microgrid is a power system that includes various energy sources (e.g., solar panels and wind turbines), where a number of device status and sensing data are collected and transmitted by smart sensors. Based on sensing-as-a-service in microgrid, sensor owners and sensor data consumers can effectively perform data sharing operations. However, the state-of-the-art sensor data sharing works in microgrid have the following two limitations: (i) cannot support fine-grained authorization for sensor owners and sensor data consumers and (ii) fail to simultaneously consider confidentiality and authenticity for sensor data sharing. To address the problems, in this article, we propose a lightweight privacy-preserving sensing data sharing system with fine-grained authorization in microgrid. Technically, we employed attribute-based signature methodology to design a fined-grained authorization mechanism for sensor data users. Moreover, a lightweight hyper elliptic curve-based signcryption scheme is employed to provide confidentiality and authenticity for sensor data sharing. To clarify the feasibility of our proposed system, we implement the system and evaluate the performance. The experimental results show that the system achieves small communication and time overhead, as well as highly acceptable gas consumption of smart contract.

1. Introduction

With the access of multiple energy sources and numerous power loads, the traditional power system is rapidly evolving into a microgrid [1]. Specifically, a microgrid is a self-sufficient power system that includes distributed power sources, energy storage devices, transmission grids, and user loads. Due to the rapid development and wide employment of 5G and Internet of Things (IoT) [2], the microgrid system can perform measurement operations (e.g., data collection, data transmission, and data analysis) based on smart IoT devices. Hence, the information of microgrid operation status, equipment status, and energy data are effectively sensed and monitored by these smart sensors, which provides a guarantee of safe operation for microgrid. According to an IHS analysis, the smart grid or microgrid-related sensor market has grown nearly tenfold between 2014 and 2021, reaching 350 million dollars, which is expected that there will be 41.6 billion IoT sensing devices by 2025.

There are amounts of sensors and connected devices that is deployed in microgrid, which is followed by the large-scale data perception and processing tasks. This motivates the employment of Sensor-as-a-Service (SaaS) [3] into the microgrid (as illustrated in Figure 1), which is driven and influenced by cloud computing service. In SaaS, sensor owner can collect, packet, and process sensing data, thus data consumers can reuse and acquire sensing data with relatively low cost. As a result, sensor owners and data consumers can securely and effectively perform data sharing and trading [4]. Since the fairness of data sharing and transactions in traditional SaaS model only relies on the service provider. Once the trust of service providers is lost, the security and fairness of data sharing may become a serious challenge.

In data sharing service, the primary security goal and fairness is to ensure that the real identities of users and transmitted data are not leaked, and third-party involvement should be avoided as far as possible in the transaction process to maximize the interests of both parties. To achieve data privacy and fairness, blockchain [5] was introduced into

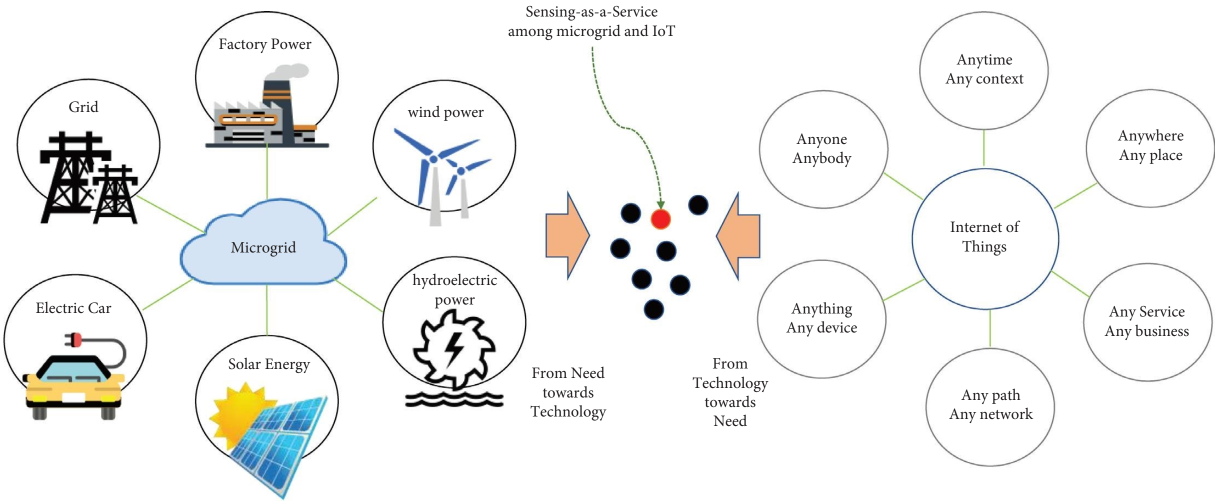

Figure 1: Relationship among sensing as a service model, microgrid, and internet of things.

data sharing services. Blockchain is a decentralized platform that combines peer-to-peer networks, cryptographic protocols, distributed data storage, and consensus mechanisms, where a number of transactions that used for recording data interaction is created and packaged into a block and added to the blockchain by miners. After that, every peer node can verify the validity of data transactions through cryptographic algorithms and consensus protocols. Due to these positive characteristics, blockchain technology has been extensively researched and deployed in practical data sharing services [4, 6–9].

The recent proposed blockchain-based data sharing systems [6, 7, 9] considered different properties of privacy-preserving in data sharing services, such as fairness, anonymity, and traceability. To enable users more willing to participate in data sharing, Samuel et al. [8] combined access control module with differential privacy and thus gave a blockchain-based fair data sharing for deregulated smart grids. By combining the advantages of IoT and SaaS in smart city, Lin et al. [4] presented an effective blockchain-based data sharing system based on symmetrical encryption and signature, Paillier encryption, and Σ-protocol. Nevertheless, these blockchain-based data sharing systems cannot be directly used in microgrid driven by sensing-as-a-service. This is because of the following reasons:

(i) The sensor devices in microgrid are usually equipped with more constrained computation and storage resources

(ii) The number of sensor owners and data consumers are large that require fine-grained access control strategies

(iii) The shared sensor data is usually provided with either data confidentiality guarantee or data authenticity guarantee

1.1. Our Results

1.1.1. Motivation. To address the problems, we proposed an effective blockchain-based sensor data sharing system in microgrid, which considers practical efficiency and security requirements. Generally, the service provider can perform fine-grained authorization over data user registration and achieve lightweight enhanced privacy-preserving of data confidentiality and data authenticity for the shared sensor data.

In particular, the contributions of this work can be summarized as follows:

(1) Fine-grained authorization. To enable the system to perform fine-grained authorization to sensor owner and data consumers, we design a fine-grained authorization mechanism based on attribute-based signature for user registration. In particular, a registered user is granted with a corresponding number of pseudonyms. As a result, not only the real identity of the user is preserved, but also the fine-grained access control of user registration is realized.

(2) Enhanced privacy-preserving data sharing. To provide enhanced privacy guarantee for the blockchain-based data sharing platform, we use a lightweight hyper elliptic curve-based signcryption scheme to achieve both confidentiality and authenticity for the shared sensor data. In particular, we employed a key encapsulation mechanism into our sensor data sharing system, where the sensor data is encrypted by AES and the key of AES is signcrypted by the lightweight hyper elliptic curve-based signcryption scheme.

(3) Reputation-based sensor owner selection. To prevent much manual intervention for a sensor owner selection, we employed a blockchain platform with constructing an effective and efficient sensor owner selection model based on reputation calculation. In particular, we designed smart contracts and formulate a reputation calculation function for each sensor owner, where the function considers the following factors, such as transaction frequency,

positive and negative reviews, and the real-time nature of reviews.

In addition, we write the codes and deploy the corresponding smart contracts in Remix Rem. Particularly, we designed 8 functions in smart contracts and evaluate their gas cost, where the cost is all below 2.0×10^6Gwei. Moreover, we evaluate the communication cost and computational overhead of AES, attribute-based signature, and signcryption that are used in our proposed system, where the cost is highly acceptable due to simple AES and lightweight hyper elliptic curve-based signcryption scheme.

1.1.2. Organization. Section 2 reviews some background knowledge and Section 3 formalizes the system model and security requirements. In Sections 4 and 5, we presented the construction and security analysis of the proposed sensor data sharing system in microgrid. Section 7 surveys recent related works and Section 8 finally concludes this work.

2. Preliminaries

2.1. Blockchain and Smart Contract. Blockchain is a decentralized distributed ledger that can record, store, and update data in a distributed manner. Transactions, in a blockchain, are the most basic activities that miners create, record, and approve in a block. Miners who with accounting rights send the blocks they create to each peer node in the system via a consensus algorithm. When received by other nodes, blocks are verified for hash, signature, and transaction validity, and after the consensus is formed, they are added locally. Furthermore, when the preparatory conditions are met, smart contracts execute, which are stored on the blockchain. They typically act as protocols enforced by specific rules that are predefined by computer code and replicated and enforced by all network nodes.

2.2. Attribute-Based Signature. Li et al. [10] initiates the notion of attribute-based signature (ABS), in which a sensor owner can sign messages with any policy that composed up of a number of attributes. Correspondingly, only the specified policy is revealed to the public while the user's identity is kept in privacy.

(1) ABS.Setup: This algorithm takes a security parameter λ as input and generates a public parameter PP and a master key MK.

(2) ABS.KeyGen: This algorithm takes PP and MK and a data user's attributes Γ as inputs and generates a private key SK_Γ for the user.

(3) ABS.Sign: This algorithm takes PP, a message M, a data user's SK_Γ, a policy Λ that accepts Γ, and finally signs the message M to output a signature δ.

(4) ABS.Verify: This algorithm takes PP and δ and attributes Γ as inputs, and outputs 1 if δ is a valid signature.

2.3. A Signcryption Scheme Based on Hyper Elliptic Curve. The work in [11] gave a highly efficient signcryption scheme based on hyper elliptic curve, where the signcryption algorithm and unsigncryption algorithm are described as follows:

(i) Signcryption (k, d_a, m, P_b, P_a)

  (a) Randomly selects an integer $k \in [1, n-1]$
  (b) $(K_1) = h(\phi(kD))$
  (c) $(K_2) = h(\phi(kD))$
  (d) $C = E_{K_2}(m)$
  (e) Compute $r = h_{K_1}$ (m‖bind info)
  (f) Compute $s = (K/(r + d_a)) \mod n$
  (g) Compute $R = rD$
  (1) Thus, the signcrypted transmitted text is (c, R, s).

(ii) Unsigncryption $(P_b, P_a, d_b, h, c, R, s)$

  (a) Compute (K_1, K_2)
  (b) $(K_1) = H(\phi(s(P_a + R)))$
  (c) $(K_2) = H(\phi(s(d_b(P_a + R))))$
  (d) Compute $m = D_{K_2}(c)$
  (e) Compute $r = h_{K_1}$ (m‖bind info)
  (f) Check $rD \overset{?}{=} R$, if true accept the message, else reject.

3. Problem Formulation

In this section, we formalized the system model and security requirements for our proposed sensor data sharing system in microgrid.

3.1. System Model. There are three main entities that is considered in our proposed data sharing system: sensor owners, data consumers, and service providers, as shown in Figure 2. In particular, the formal descriptions of these entities are as follows:

(1) Sensor owners: Sensors usually refer to devices that are connected to various energy equipments for measuring, sensing, and presenting data information (e.g., temperature, humidity, and electricity). In particular, the sensors can satisfy the requirements of information transmission, processing, storage, display, recording, and its characteristics, such as miniaturization, intelligence, networking, and other characteristics. Generally, the sensor owners are independent parties who have these sensors in possession and a sensor owner may own one or more sensors. If the sensor owner is willing to share the data in the sensor, paid, or free, then they can publish the sales information in the system.

(2) Data consumers: Data consumers (e.g., energy companies, scientific research teams, and schools) may purchase the sensing data by Saas model. In the system, data consumers can send requests for

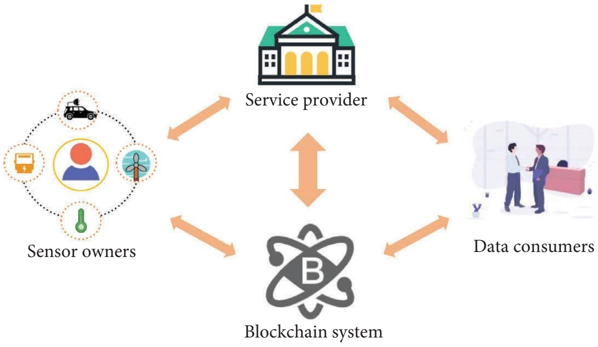

Figure 2: System model of data sharing.

matching candidate sensor data that is contributed by different sensor owners. If data consumers intend to purchase shared sensor data, they may pay a deposit to the sensor owner in advance, and then pay the corresponding balance after obtaining all sensor data. Moreover, all transaction processes are automatically completed via the smart contracts in the system.

(3) Service provider: The honest and curious service provider runs registration service for sensor owners and data consumers, where only the registered parties can conduct data transactions in the system. Note that the registration service is completed based on the deployed smart contracts in the system. In addition, the service provider stores the data to be shared on its behalf, and after the transaction takes place, transmits the data to the data consumer.

3.2. High-Level Overview. As shown in Figure 3, we presented a high-level overview of the system as follows:

Step 0: Sensor owners or data consumers who want to join in the system should complete the registration procedure with the service provider at first.

Step 1: A sensor owner uses a wireless connection with the service provider for data transmission, where it needs to transmit the sales information and the AES-encrypted sensor data to the service provider.

Step 2: After the service provider reviewed the sales information and received the encrypted data, it publishes the sales information on the blockchain platform.

Step 3: A data consumer selects a target seller based on its own interests and the sensor owner's reputation. After that, it needs to upload its request information (e.g., public key and pseudonym) to the smart contract and pay the deposit.

Step 4: If a sensor owner agrees to sell sensing data to a data consumer, it first accepts the data consumer's request and later encrypts the data key by employing a signcryption algorithm, and finally uploads it to the smart contract.

Step 5: The data consumer downloads the corresponding file from the platform, decrypts it to obtain the data key, where the balance is automatically deducted from the data consumer's account.

Step 6: The service provider transmits the encrypted data to the data consumer, and the data consumer uses the key to decrypt the encrypted data. If the data consumer finds that the key is invalid, it may submit an appeal to the service provider.

3.3. Design Goals and Security Requirements. The following are the design goals and security requirements that is considered in our proposed system.

(1) Privacy-preserving. Sensor owners and data consumers should have a certain number of pseudonyms in the system that they use to use sensor services, and their real identities should be hidden.

(2) Unlinkability and revocability. All pseudonyms registered on the service platform by sensor owners and consumers using their real identities cannot be connected. But when users seriously violate the rules, the system should have the right to reveal the real identity behind the pseudonym and revoke their right to use the service.

(3) Data integrity and reliability. When the sensor owner encrypts and sends the data to the service provider, the service provider does not have the decryption key, so it only temporarily stores the data and cannot tamper or delete the data without permission. Therefore, the integrity and reliability of the data are guaranteed.

(4) Fairness. On one hand, data consumers cannot obtain sensor data without paying a corresponding deposit. On the other hand, sensor owners should be caught and penalized if they provide invalid sensor data to sensor data consumers.

4. System Design

For our proposed sensor data sharing system in microgrid, we gave a formal description of the system running flow.

4.1. Running Flow. The running flow of the system consists of initialization, registration, publication, request, response, retrieval, guarantee, and evaluation phase. In addition, the

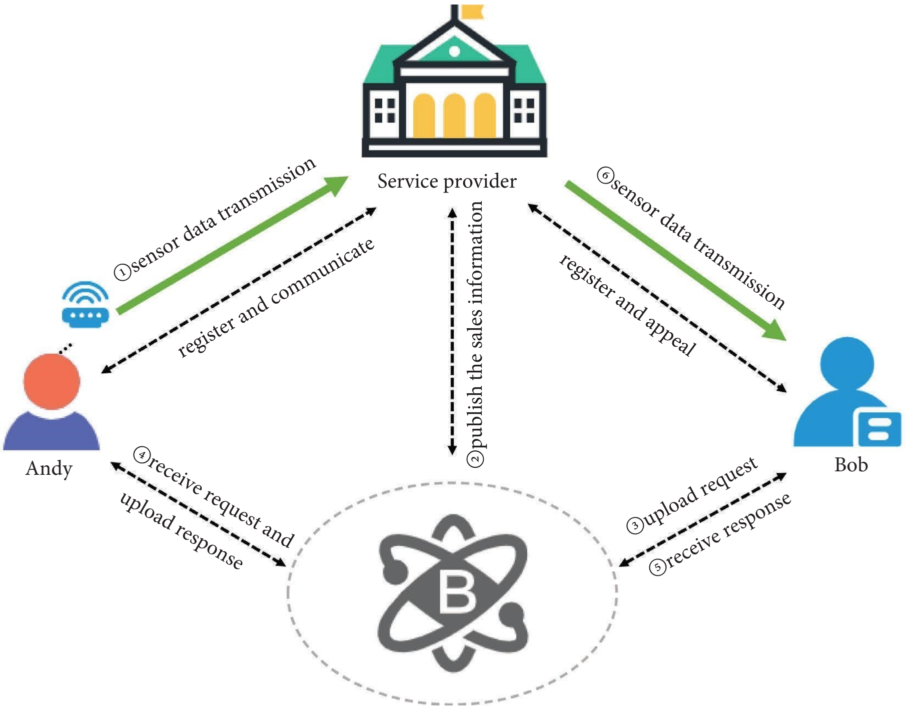

Figure 3: System instantiation scene.

functions in the smart contract includes uploadRegInfo, publishSales, uploadRequest, getRequest, uploadRes, getRes, submitAppeal, and calReputation. In particular, these functions are mainly focused on uploading registration information, publishing sales information, uploading purchase requests, receiving purchase requests, uploading responses information, receiving responses, submitting appeals, and calculating reputation in the above process. In particular, the formal descriptions of the proposed system are as follows:

4.1.1. Initialization. The users (sensor owners and data consumers) are authenticated by the ABS algorithm before they participate in the system. Specifically, the system calls ABS.Setup() to set public parameter PP and master key MK, and sends the access structure T to the user, while the user needs to submit its attribute set γ_u that satisfies T. Then, ABS.KeyGen() inputs MK, PP, and γ to generate the user's private key SK_γ. Finally, the algorithm ABS.Sign() outputs a signature σ_u that satisfies the condition.

4.1.2. Registration. The service provider in the system provides registration service. Both the sensor owner and the sensor data consumer must complete the registration in the service provider. Only the registered entities can enjoy the services in the system. First, the registration entity submits the corresponding information (γ_u, rid, and σ_u) to the service provider(rid is the real identity of the registered user). Then, the service provider calls the ABS.verify() to verify the authenticity of the registration information. Only those who have passed the verification can complete the registration, otherwise the registration will fail. Then, the system automatically generates a certain number of pseudonyms pid_u based on the attribute set of the registered user to protect their privacy. Finally, γ_u and pid_u will be submitted to the blockchain through uploadRegInfo. The registration and uploadReginfo algorithm is described in Algorithm 1. Note that the service provider locally stores the real identity of the registered user for subsequent tracking of requirements.

4.1.3. Publication. When a sensor owner wants to publish data sales information, he first needs to call the AES.enc$(\mathrm{k}, \mathrm{m_d})$ to encrypt the data into ciphertext c_d, and then transmit it to the service provider through the sensor (each sensor has a corresponding ID sid). The service provider receives the ciphertext and publishes the sales information through publishSales in the smart contract (as shown in Algorithm 2). The published information includes the seller's pseudonym pid_i, the information info of the sensor data info, and the expected price p.

4.1.4. Request. Sensor consumers can choose the data they are interested in or want to buy based on the published sales information. If the sensor consumer selects a certain sensor owner, that is, the seller, upload the consumer's own public key P_b, its own pseudonym pid_j, the seller's pseudonym pid_i, and the index of the data inde x in the hyper elliptic curve-based signcryption algorithm to the smart contract through uploadRequest in Algorithm 3. As for how consumers can choose sellers efficiently, they can make decisions based on the reputation value of the sellers, which will be described in detail in Section 4.2.

```
Require: a user's attribute set $\gamma_u$ and real identity $r_{\text{id}}$.
Ensure: the pseudonym of users $p_{\text{idu}}$.
if ABS.verify($b = 1$) then
    register successful;
    uploadReginfo ($\gamma_u, \text{pid}_u$);
else
    return false;
end if
```

Algorithm 1: Register and uploadReginfo.

```
Require: service provider has received the sensor data.
Ensure: publish sales information successfully.
if RS (receive status) = true; then
    Sales.sid = sid;
    Sales.pidu = pidu;
    Sales.info = info;
    Sales.price = $p$;
else
    return false;
end if
```

Algorithm 2: publishSales (sid, pidu, info, p).

```
Require: Consumer's public key, pseudonyms of both parties, and data index
Ensure: upload request successfully.
if SS (selected status) = true; then
    Req.cpk = $P_b$;
    Req.consumer = $\text{pid}_j$;
    Req.owner = $\text{pid}_i$;
    Req.data = inde x;
end if
```

Algorithm 3: uploadRequest (P_b, pid_j, pid_i, inde x).

4.1.5. Response. The sensor owner can obtain the consumer's request information through getRequest in the smart contract. If the owner agrees with the quotation and other matters in the request information, it encrypts its own symmetric key through signcryption (r, d_a, m_k, P_b, and P_a) and obtains the transmission text (c_k, R, s). Here, c_k refers to the ciphertext of the sensor owner in the signcryption algorithm, while R and s are the generated signature; d_a refers to the private key of the sensor owner, P_a and P_b are the public keys of the sensor owner and the data consumer. Then, it sends a tip information tip that agrees to the request to the service provider and calls uploadRes as in Algorithm 4 to upload the transmitted text to the smart contract.

4.1.6. Retrieval. The data consumer gets the corresponding file from getRes in the smart contract, and decrypts it through unsigncryption ($P_b, P_a, d_b, h, c_k, R, s$) to obtain the data key k. Note that the check() algorithm in unsigncryption can verify whether the signcryption calculation is performed using the public key provided by the consumer, which provides verifiability. After that, the consumer requests the encrypted data from the service provider. Of course, for the security of the transaction, the service provider will verify that the sensor owner has agreed to the request before transmitting the data to the consumer. Finally, when the consumer receives the data transmitted by the provider, he decrypts the original sensor data m_d using the AES.dec (k, c_d). Note that when sensor data is obtained, the system will automatically debit the consumer's account and credit the remaining fee to the sensor owner's account.

4.1.7. Guarantee. If the consumer finds that the key is invalid, i.e., the sensor owner has provided a fake data key, he can submit an appeal to the service provider via submitAppeal. The service provider reverifies the situation and orders the sensor owner to provide the consumer with a valid key. If the sensor owner continues to provide invalid keys, the service provider will reveal the real identity rid

```
Require: send a tip to the service provider
Ensure: upload response successfully.
if ST(status of tip) = true; then//the tip has been sent
    Res.text[] = $c_k, R, s$;
    Res.owner = pid$_i$;
    Res.consumer = pid$_j$;
else
    return "please send a tip agreeing to the request";
end if
```

Algorithm 4: uploadRes $(c_k, R, s, \mathrm{pid}_i, \mathrm{pid}_j)$.

behind the pseudonym and block all pseudonyms pidu, and also the data consumer's funds will be returned.

4.1.8. Evaluation. After a transaction cycle is completed, the data consumer can evaluate the transaction, that is, score and evaluate the sensor owner. The range of evaluation points is set from 1 to 10 points, with 6 points or more being positive evaluations and the following being negative evaluations. The evaluation within 1 month is the recent evaluation, otherwise it is the past evaluation, and the time window is 6 months. The calReputation in the smart contract automatically calculates the reputation of the sensor owner SR based on the above factors.

4.2. Reputation Calculation Model. In the proposed data sharing system, the reputation value of a sensor owner (seller) can be computed in real time by using the reputation calculation model, where the seller with a high reputation means that their data quality and transaction reputation are relatively good. Therefore, data consumers (buyers) can selectively choose sellers with high reputation for data trading. The reputation of the sensor owner is mainly affected by two key factors, transaction frequency, and after-sales evaluation. We combine these two factors to build a reputation calculation model to help consumers choose the right sellers efficiently.

(i) Transaction Frequency: The transaction frequency refers to the ratio of the number of transactions between sensor owner i and data consumer j to the average number of transactions between sensor owner i and other data consumers within the time window T, namely,

$$TF_{i\longrightarrow j} = \frac{N_{i\longrightarrow j}}{\overline{N_i}}, \tag{1}$$

where $N_{i\longrightarrow j} = (\alpha_i + \beta_i)$ and $\overline{N_i} = 1/|M|\sum_{m\in M} N_{i\longrightarrow m}$ (M is the total number of data consumers m transacting with sensor owner i within a time window). In conclusion, higher transaction frequency indirectly indicates a higher reputation of the sensor owner.

(ii) Evaluation Timeliness: Data consumers can rate sellers within one month after the transaction. In order to calculate reputation more accurately, the system assumes that recent reviews have a greater impact on the seller's reputation, while past reviews have less impact. Also, negative reviews have a greater impact on sellers than positive reviews. Therefore, we set the weight of recent evaluations to be ζ, the weight of past evaluations to be σ ($\zeta + \sigma = 1$, $\zeta > \sigma$), and the recent and past time periods to be one month. Positive reviews are weighted θ and negative reviews are weighted τ ($\theta + \tau = 1$ and $\theta < \tau$). Taking into account two sets of factors, the update transaction frequency formula is as follows:

$$\begin{cases} \alpha_i &= \zeta\theta\alpha_1^i + \sigma\theta\alpha_2^i, \\ \beta_i &= \zeta\tau\beta_1^i + \sigma\tau\beta_2^i. \end{cases} \tag{2}$$

Among them, when the current time t satisfies $t \leq 1$ (month), the number of recent positive evaluations is α_1^i, and the number of recent negative evaluations is β_1^i. For $t\ > 1$, the number of positive and negative past events are α_2^i and β_2^i, respectively. Therefore, the reputation calculation function of the data seller (SR) is as follows:

$$\mathrm{SR} = \frac{N_{i\longrightarrow j}}{\overline{N_i}} = \frac{\theta\left(\zeta\alpha_1^i + \sigma\alpha_2^i\right) + \tau\left(\zeta\beta_1^i + \sigma\beta_2^i\right)}{1/|M|\sum_{m\in M} N_{i\longrightarrow m}}. \tag{3}$$

In summary, the calReputation in the smart contract will automatically calculate and present the reputation of the sensor owner in real time according to the function. Data consumers can choose data sellers with high reputation for transactions. Of course, the price of data from sellers with high reputation will be higher.

5. Security Analysis

In this section, we present security analysis of our proposed system.

5.1. Privacy Preserving. The system adopts the ABS signature algorithm in the entity registration stage, and ABS has anonymity. Second, after the user is registered with the service provider, a certain number of pseudonyms pidus are returned for them to use when transacting. These hide the user's real identity and protect the user's privacy well.

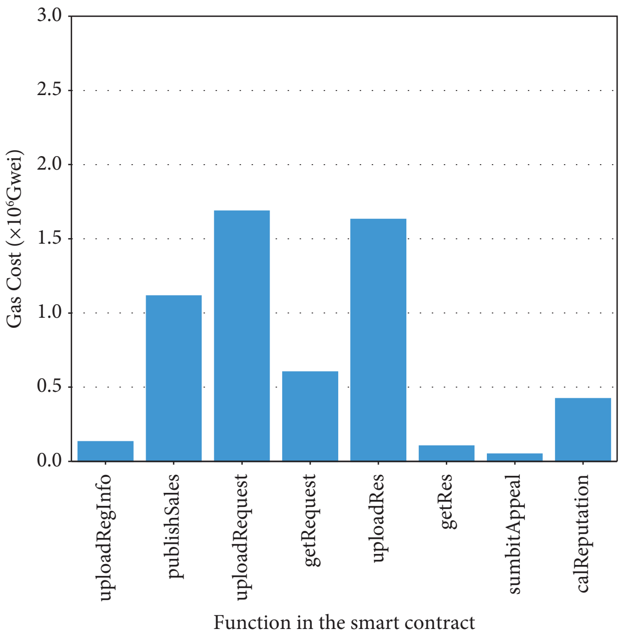

Figure 4: Gas cost of the function in smart contract.

5.2. Unlinkability and Revocability. The pseudonyms given by the service provider to the registered entity are only related to the real identity behind it, and there is no link between the pseudonyms. Since the service provider stores the real identity of the user locally, when the user acts dishonestly, the service provider will revoke the right to use the service under a pseudonym.

5.3. Data Integrity and Reliability. The sensor owner encrypts the data in the sensor with the AES algorithm and uploads it to the service provider, and the service provider stores it on their behalf. In the process of data transmission and storage, if there is no corresponding data key k, no one can modify and read the data.

5.4. Fairness. There is no third-party intervention in our system during the data transaction process. The service provider only provides the functions of registration, data storage and transmission, and does not enter into the process of data transaction. Additionally, data consumers can submit appeals when sensor owners provide invalid keys. These protect the rights and interests of consumers and ensure the fairness of the system.

6. Experimental Study

In this section, we evaluate the performance of the system, including testing out the gas cost of smart contracts and calculating the computational and communication cost of the cryptographic algorithms used. In particular, to facilitate compiling and testing smart contracts, we implement preops on Remix, a browser-based integrated development environment (IDE) for Ethereum. Specifically, the specific configuration in Remix includes the following: programming language (Solidity), compiler version (>=0.4.22 <0.7.0), and EVM version (default setting). In addition, we also evaluated the communication overhead and the computational cost of specific algorithms at each stage in the system running process.

Table 1: Computation cost of ECPM and HECDM.

Notation	Computation cost (ms)
ECPM	4.24
HECDM	2.2

6.1. Performance of Smart Contracts. The smart contract in the system consists of eight main functions, namely uploadRegInfo, publishSales, uploadRequest, getRequest, uploadRes, getRes, submitAppeal, and calReputation. The total gas cost of deploying smart contracts in the system is 1.0186×10^7Gwei, and the gas cost of each part of the function is 0.133, 1.114, 1.686, 0.602, 1.631, 0.103, 0.049, and 0.422 ($\times 10^6$Gwei), as shown in Figure 4. Among them, the reputation calculation for the sensor owner consumes a lot of gas, but it achieves our expected effect.

6.2. Communication and Computational Cost. We evaluated the communication and time cost of our system based on the benchmark given by [11], where the hardware is configured as a computer running jdk1.6, with 2 Intel CPU cores, a processing speed of 2.00 GHz, and a main memory capacity of 4 GB. As measured in [11], Table 1 shows time cost for elliptic curve point multiplication and hyperelliptic curve divisor-scalar multiplication, where a single scalar multiplication operation is respective 4.24 ms and 2.2 ms, and we use [12]'s ABS scheme to instantiate our system. In particular, we list some basic symbols in system cryptographic algorithms in Table 2 along with their cost. Therefore, we used these notations to calculate theoretical communication cost for different stages of the system's operational flow. As shown in Table 3, we only consider dominant operations for calculation, and the communication cost corresponding to initialization, publishing, request, response, and retrieval are 3040 bytes, 40 bytes, 65 bytes, 26 bytes, 66 bytes, and 72 bytes, respectively. In addition, the computational cost of the substeps of the ABS where the number of attributes is 50 and HECCS algorithms in the system are given in Table 4, which are 216.24 ms, 216.24 ms, 220.48 ms, 6.6 ms, and 4.4 ms, respectively.

6.3. Reputation Calculation Analysis. Since the reputation of the sensor owner is affected by the real-time evaluation and the positive and negative effects, as shown in Figure 5, we test the changes of the reputation value in the two time periods of $0 \sim 1$ month and $1 \sim 6$ months, respectively. Specifically, we preset $\theta = 0.3$, $\tau = 0.7$, $\zeta = 0.6$, and $\sigma = 0.4$ in the program, and take half a year as a time window. It can be clearly seen from Figure 5 that the greater the proportion of negative reviews within a month, the faster the decline in reputation value. On the other hand, the number of negative reviews

Table 2: Notation, definition, and size.

Notation	Definition	Size (byte)
$\lvert\mathbb{G}\rvert$	Size of an element in $\mathbb{G}$	20
$\lvert Z_p^*\rvert$	Size of an element of a group Z_p^*	20
$\lvert\sigma_u\rvert$	Size of a ABS signature	40
$\lvert K_h\rvert$	Size of a HECCS session key	16
$\lvert\sigma_h\rvert$	Size of a HECCS signature	56
$\lvert\mathrm{sid}\rvert$	Size of a sensor identity	4
$\lvert \mathrm{pid}_u\rvert$	Size of a pseudonym	5
$\lvert\mathrm{info}\rvert$	Size of the data information	40
$\lvert c_{\mathrm{AES}}\rvert$	Size of a AES ciphertext	16

Table 3: Communication cost of each phase.

Phase	Communication cost (byte)
Initialization	3040
Registration	40
Publication	65
Request	26
Response	66
Retrieval	72

Table 4: Computation cost of each algorithm step.

Algorithm	Computation cost (ms)
ABS.Setup	216.24
ABS.KeyGen	—
ABS.Sign	216.24
ABS.Verify	220.48
Signcryption	6.6
Unsigncryption	4.4

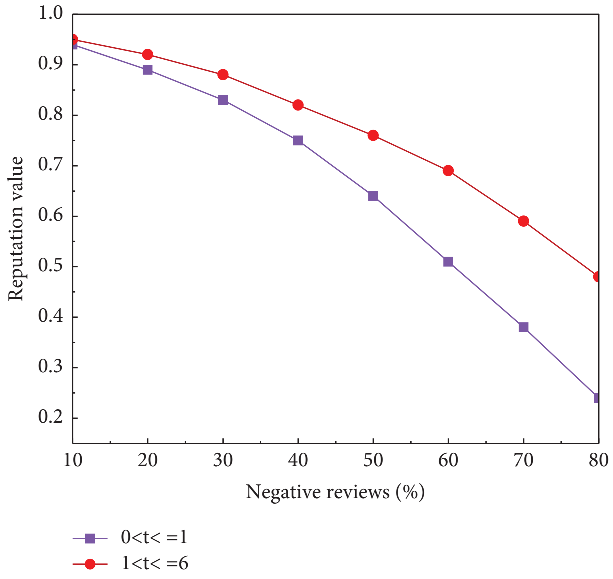

Figure 5: Reputation changes with different proportions of negative reviews.

between one month and six months has a lower impact on reputation value. This fully reflects the influence of the number of negative reviews and recent reviews on reputation value.

7. Related Work

Access control techniques are widely applied to share data from IoT sensors. Traditional access control techniques include discretionary access control (DAC) [13], role-based access control (RBAC) [14, 15], and capability-based access control (CapBAC) [16]. However, for these traditional models, a centralized authority is usually necessary to configure access control policies, resulting in centralized decision-making. Moreover, access control policies or records stored by a central third-party may be maliciously tampered with, leading to unreliable auditing. Facing this challenge, many attribute-based access controls [17] and attribute-based proxy re-encryption schemes [18, 19] have been proposed, but the issue of unreliable audits still exists in almost all of them. To settle the above issues, researchers combine blockchain technology with access control, which has the benefits of verifiability and decentralization.

Blockchain-based data sharing schemes have been presented in previous researches. Regarding data sharing between individuals and others, Chowdhury et al. [20] proposed a data sharing architecture of personal data with a notarization service offered by blockchain, and applied a blockchain-based mechanism to protect the privacy and integrity of transaction data. For data collected by IoT sensors, Manzoor et al. [21] combined the blockchain technology with the proxy re-encryption scheme to address the third-party trust issues of traditional IoT data sharing and improve scalability while guaranteeing data security. Since there are significant security issues in sharing data among users in multiple organizations, amounts of research has been conducted recently. Chen et al. [6] presented a blockchain-based privacy protection scheme based on k-anonymity and searchable, which achieves security and privacy protection of data in data sharing systems. However, the scheme requires further optimization and improvement for multiple groups data. Based on the Ethereum blockchain technology, Song et al. [22] accomplished the decentralization of the big data sharing system. However, these schemes mainly address data security and privacy issues and fail to focus on improving fairness in data sharing. To achieve anonymity and traceability of users, Huang et al. [7] utilized group signature technology in the proposed data sharing scheme without a trusted auditor by virtue of blockchain technology. Blockchain-based data sharing solutions are not only proposed in theory, but also play a significant role in solving difficulties in the life. To address the security and privacy concerns posed by electronic medical records, Chen et al. [23] proposed a signature based on antiquantum properties to share data securely with the blockchain. Tan et al. [24] proposed a blockchain-empowered solution that allows for direct tracking and revocation of medical records. To protect data privacy in building information model data sharing, Wang et al. [25]

proposed a blockchain-based approach, which can used to secure information in the next generation of smart building industrial IoT. These schemes motivated the achieved property of user traceability and revocability in our proposed data sharing scheme.

To further enhance fairness in the data sharing process, a number of blockchain-based solutions and architectures [26–28] have been proposed to ensure the security and fairness while implementing outsourcing services. Furthermore, Samuel et al. [8] presented a reputation system, fairly compensating through blockchain and differential privacy. In order to enhance the verifiability and fairness of cloud data management, Ge et al. [29] introduced a novel attribute-based proxy re-encryption scheme, according to which a concept called VA-ABPRE is defined and a concrete scheme is conducted. However, these schemes are constructed in the field of data outsourcing services while they cannot be directly deployed in microgrid. Wang et al. [9] applied blockchain technology to a supply chain to address issues such as distrust and asymmetric valuation of data that can arise from data sharing between upstream and downstream entities in the supply chain. But this study proposal uses an idealized model; actual supply chains cannot be completely adapted to it. Zhang et al. [30] introduced a data sharing scheme based on blockchain and ciphertext policy attribute-based encryption, where fair retrieval of ciphertexts is achieved through smart contracts. The editable blockchain in the authentication scheme of Zhai et al. [31] provided fine-grained and fair checksum functionality. Damisa et al. [32] proposed an Ethereum smart contract using a double auction mechanism to drive fairness and transparency in selection and compensation. The implementation of these smart contracts has effectively reduced the cost of manual intervention, where the property of accountability is not well studied [33].

8. Conclusions

In this work, we proposed a lightweight and privacy-preserving sensor data sharing system with attribute-based authorization in microgrid. In the system, we combined blockchain, smart contracts, and cryptographic algorithms (e.g., ABS, AES, and a lightweight signcryption scheme) to construct such sensor data sharing platform. Finally, we conducted a couple of experimental to evaluate the gas cost of functions in the smart contracts and general computational cost of cryptographic algorithms. To further improve the fairness of data sharing and running performance of the system, we continued to investigate the data pricing and claims mechanism, and moreover design a more lightweight cryptographic algorithm to replace the currently employed ABS algorithm.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was sponsored by National Natural Science Foundation of China (U1936213), Shanghai Rising-Star Program (no. 22QA1403800), Shanghai Sailing Program (no. 21YF1415000), and Program of Shanghai Academic Research Leader (no. 21XD1421500).

References

[1] A. Muhtadi, D. Pandit, N. Nguyen, and J. Mitra, “Distributed energy resources based microgrid: review of architecture, control, and reliability,” *IEEE Transactions on Industry Applications*, vol. 57, no. 3, pp. 2223–2235, 2021.

[2] Y. E. Oktian, E. N. Witanto, and S. G. Lee, “A conceptual architecture in decentralizing computing, storage, and networking aspect of iot infrastructure,” *IoT*, vol. 2, no. 2, pp. 205–221, 2021.

[3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Sensing as a service model for smart cities supported by internet of things,” *Transactions on emerging telecommunications technologies*, vol. 25, no. 1, pp. 81–93, 2014.

[4] C. Lin, D. He, S. Zeadally, X. Huang, and Z. Liu, “Blockchain-based data sharing system for sensing-as-a-service in smart cities,” *ACM Transactions on Internet Technology*, vol. 21, no. 2, pp. 1–21, 2021.

[5] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” *Decentralized Business Review*, vol. 15, p. 21260, 2008.

[6] Y. Chen, L. Meng, H. Zhou, and G. Xue, “A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6685762, 12 pages, 2021.

[7] H. Huang, X. Chen, and J. Wang, “Blockchain-based multiple groups data sharing with anonymity and traceability,” *Science China Information Sciences*, vol. 63, no. 3, pp. 130101–130113, 2020.

[8] O. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani, “A blockchain model for fair data sharing in deregulated smart grids,” in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, IEEE, Waikoloa, HI, USA, December 2019.

[9] Z. Wang, Z. E. Zheng, W. Jiang, and S. Tang, “Blockchain-enabled data sharing in supply chains: model, operationalization, and tutorial,” *Production and Operations Management*, vol. 30, no. 7, pp. 1965–1985, 2021.

[10] L. Jin, M. H. Au, W. Susilo, D. Xie, and K. Ren, “Attribute-based signature and its applications,” in *Proceedings of the 5th ACM symposium on information, computer and communications security*, pp. 60–69, Kyoto, Japan, June 2010.

[11] S. A. Ch, N. uddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, “An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography,” *Multimedia Tools and Applications*, vol. 74, no. 5, pp. 1711–1723, 2015.

[12] R. Ma and L. Du, “Attribute-based blind signature scheme based on elliptic curve cryptography,” *IEEE Access*, vol. 10, pp. 34221–34227, 2022.

[13] J. Zamite, D. Domingos, M. J. Silva, and C. Santos, “Group-based discretionary access control in health related repositories,” *Journal of Information Technology Research*, vol. 7, no. 1, pp. 78–94, 2014.

[14] A. Alshehri and R. Sandhu, “Access control models for virtual object communication in cloud-enabled iot,” in *Proceedings of*

the 2017 IEEE international conference on information reuse and integration (IRI), pp. 16–25, IEEE, San Diego, CA, USA, August 2017.

[15] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca, "Georbac: a spatially aware rbac," *ACM Transactions on Information and System Security*, vol. 10, no. 1, p. 2, 2007.

[16] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," *Mathematical and Computer Modelling*, vol. 58, no. 5-6, pp. 1189–1205, 2013.

[17] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pp. 523–528, Hangzhou, China, May 2013.

[18] K. Liang, L. Fang, W. Susilo, and S. Duncan, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 552–559, IEEE, Sanda-Shi, Japan, Dcember 2013.

[19] Y. Zhang, J. Li, X. Chen, and H. Li, "Anonymous attribute-based proxy re-encryption for access control in cloud computing," *Security and Communication Networks*, vol. 9, no. 14, pp. 2397–2411, 2016.

[20] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and S. Paul, "Blockchain as a notarization service for data sharing with personal data store," in *Proceedings of the 2018 17th ieee international conference on trust, security and privacy in computing and communications/12th ieee international conference on big data science and engineering (TrustCom/BigDataSE)*, pp. 1330–1335, IEEE, New York, NY, USA, August 2018.

[21] A. Manzoor, M. Liyanage, B. An, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure iot data sharing," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 99–103, IEEE, Seoul, Korea (South), May 2019.

[22] S. Song, "An effective big data sharing prototype based on ethereum blockchain," *Scientific Programming*, vol. 202214 pages, 2022.

[23] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, and W. Kong, "Aq–abs: anti-quantum attribute-based signature for emrs sharing with blockchain," in *Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1176–1181, IEEE, Austin, TX, USA, April 2022.

[24] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards secure and privacy-preserving data sharing for covid-19 medical records: a blockchain-empowered approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 271–281, 2022.

[25] H. Wang, X. Hao, L. Yin, P. Gong, F. Xiong, and W. Ren, "A blockchain-based and privacy-protected method for sharing of bim big data," in *Proceedings of the 2022 7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, pp. 185–191, IEEE, Chengdu, China, April 2022.

[26] Y. Guan, H. Zheng, J. Shao, R. Lu, and G. Wei, "Fair outsourcing polynomial computation based on the blockchain," *IEEE Transactions on Services Computing*, vol. 15, no. 5, pp. 2795–2808, 2022.

[27] H. Zhang, P. Gao, Y. Jia, J. Lin, and N. N. Xiong, "Machine learning on cloud with blockchain: a secure, verifiable and fair approach to outsource the linear regression," *IEEE Transactions on Network Science and Engineering*, vol. 9, 2021.

[28] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," *IEEE Transactions on Services Computing*, vol. 14, no. 4, pp. 1152–1166, 2021.

[29] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 2907–2919, 2022.

[30] L. Zhang, T. Zhang, Q. Wu, Y. Mu, and F. Rezaeibagha, "Secure decentralized attribute-based sharing of personal health records with blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12482–12496, 2022.

[31] M. Zhai, Y. Ren, G. Feng, and X. Zhang, "Fine-grained and fair identity authentication scheme for mobile networks based on blockchain," *China Communications*, vol. 19, no. 6, pp. 35–49, 2022.

[32] U. Damisa and N. I. Nwulu, "Blockchain-based auctioning for energy storage sharing in a smart community," *Energies*, vol. 15, no. 6, p. 1954, 2022.

[33] REMIX, "remix ide for smart contract deployment provided by ethereum," 2023, https://remix.ethereum.org/.