Blockchain Privacy Data Access Control Method Based on Cloud Platform Data

Biying Sun, Qian Dang, Yu Qiu, Lei Yan, Chunhui Du, Xiaoqin Liu
State Grid Gansu Electric Power Company Internet Division, Lanzhou, China

***Abstract*—With the improvement of digital informatization and openness of the smart grid, the security of all kinds of sensitive and private data in the power grid is inevitably facing severe threats and challenges. In this paper, we propose a privacy protection scheme for multidimensional data aggregation and access control in the cloud Internet of Things for smart grid. The scalable access control based on attribute encryption is used to determine the data security of power user data in the process of data information sharing in the blockchain under the large data traffic of the cloud platform, which is to achieve privacy protection and fine-grained access control for demand-side multidimensional data. By using the EBGN homomorphic encryption algorithm, the multidimensional data is encrypted, and each dimension can be decrypted separately using the corresponding private key. The multidimensional data aggregation at the gateway can aggregate the multidimensional data into cipher-text, and the control center does not need to decrypt the cipher-text data of each dimension, thereby simplifying the operation of the gateway and the control center and improving the security and privacy of the data. By encrypting the EBGN private key of each dimension through the cipher-text policy attribute encryption algorithm, the fine-grained access control at the dimension level is realized. The experimental results show that the proposed method can effectively improve the security of private data in the aspect of multidimensional data privacy protection, thus reducing the security risk of multidimensional data being illegally accessed. The research in this paper can effectively reduce the communication overhead and computational complexity, reduce the computational cost, and is suitable for data security and privacy protection of smart grid cloud Internet of Things.**

***Keywords*—Cloud platform; blockchain; private data; data encryption; access control**

I. Introduction

The combination of smart grid and the Internet of Things promote the wide application of various network information sharing technologies in the power system, which greatly changes the way of life and work, but also brings a series of hidden dangers, among which the hidden danger of information security is the core. Due to the bidirectionality of smart grid information flow, and in order to reduce communication bandwidth and achieve flexible fine-grained analysis, multi-dimensional aggregation and access of smart grid data are needed [1]. Each data dimension contains sensitive and private information, which may be analyzed and utilized by different research organizations. For example, in data transmission, the leakage and tampering of data information such as power information and privacy information may cause security and privacy threats to power supply companies and customers and even serious economic losses. Therefore, the privacy protection and access control of blockchain is particularly important [2].

So far, many scholars have conducted extensive research on smart grid privacy protection based on data aggregation and access control. The schematic diagram of smart grid data aggregation and access architecture is shown in Fig. 1.

Terminal devices distributed in multiple links such as power generation, transmission, distribution, and power consumption are used for blockchain collection. The gateway aggregates the blockchain into data cipher-text for data transmission and instruction transmission with the control center [3]. The control center stores the collected data in the cloud server and can decrypt the data cipher-text of the corresponding dimension to determine the power supply strategy according to the total demand. The access authority can access the data information of the authorized dimension [4].

Due to the advantages of homomorphic encryption in data confidentiality and privacy protection, the cipher-text can be directly operated without decrypting the cipher-text. J. W. et al. [5] proposed a track protection method based on privacy clustering, which is used to resist continuous query attacks by adding Laplace noise to the track position count in the cluster. The radius-limited Laplacian noise is added to the trajectory data in the cluster to avoid affecting the clustering effect, and the noise cluster center is obtained according to the noise position data and the noise position count. J. Zhang et al. [6] proposed an algorithm to protect access to sensitive sites in privacy-preserving trajectory data release, which generalizes sensitive sites with sensitive regions and distorts sub-trajectories within sensitive regions based on privacy. K. Xue et al. [7] proposed a method to protect the release of road network trajectory traffic by using privacy technology. After counting the traffic value of the trajectory data of each road section, the method adds random noise satisfying differential privacy to the traffic value and then proposes a post-adjustment algorithm to solve the consistency characteristics of the traffic map. The complexity of smart grid architecture based on cloud Internet of Things not only makes the whole power system more intelligent but also brings a large amount of information data, which may contain a large number of sensitive information (such as security risks of nodes, voltage data of a certain place, etc.) and very important privacy information (such as user identity information, location information, etc.) [8]. The research on data access control is helpful to improve the user's access speed to the encrypted data, reduce the waiting time for users to access the encrypted data. At the same time, it is also of great significance to the network data security.

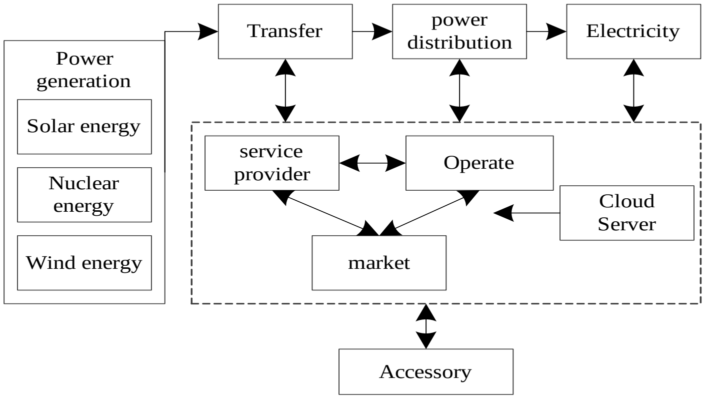

Fig. 1. System Architecture.

In the face of the large-scale and complex system of smart grid cloud Internet of Things, the above scheme is difficult to meet the security requirements of the system for data. In the smart grid cloud Internet of Things system, it also faces the problem of visitor access rights, which need to be revoked or updated in time.

In this paper, based on the attribute access control method and the data privacy protection requirements of the cloud Internet of Things on the demand side of the smart grid, a demand-side cloud Internet of Things blockchain aggregation and access control scheme is proposed, which completes the aggregation work of the blockchain and the fine-grained access control of privacy data. In the aggregation phase, Boneh-Goh-Nissim (EBGN) homomorphic encryption extended by wireless sensor networks is used to aggregate the blockchain into cipher-text, and CP-ABE encryption is used to perform fine-grained access control at the dimension level. Then, the implementation of the algorithm is introduced and the security of the scheme is proved, and a detailed comparison with other existing schemes is made in terms of functionality computation and communication overhead.

II. Related Work

A. Data Aggregation

The establishment of secure information communication is the task of building the information security of smart grid cloud Internet of Things, and it is also the basis of achieving efficient communication and reducing communication overhead. Smart grid privacy protection schemes using data aggregation techniques during communication have been proposed in many studies [9]. The basic idea of these techniques is based on the use of an aggregator and a trusted authority connected to the user, as shown in Fig. 2.

In the smart grid, the analysis of all kinds of power data can not only be applied to the formulation of real-time pricing and power dispatching strategies but also may produce other commercial values. In order to carry out fine-grained analysis, it is necessary to collect the blockchain of each link of the smart grid. Taking the user side as an example, by analyzing the power consumption of air conditioning equipment at the user side in hot weather in summer, the power station can prepare enough power in similar hot weather later [10].

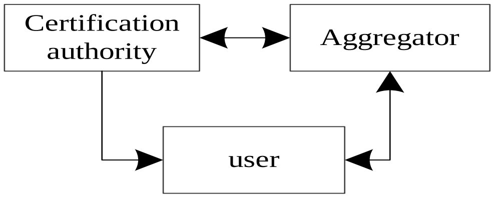

Fig. 2. Data Aggregation System Model.

B. EBGN Homomorphic Encryption Algorithm

EBGN homomorphic encryption is an extension of the BGN homomorphic encryption scheme proposed by Boneh, Goh, and Nissim. It makes up for the limitation that BGN encryption cannot support blockchain encryption. Both BGN and EBGN support addition and multiplication homomorphisms, that is, the results of addition and multiplication operations performed on cipher-text match the results of the corresponding operations performed on plaintext [11]. Because multiplication homomorphisms are computationally expensive, only additive homomorphisms are considered in this paper. EBGN consists of the following computational structure.

Let G be a group of prime order p. Let the generator of G be g, and let $e: G \times G \rightarrow G_T$ be the bilinear pairing operation. DBDH assumes that a security parameter κ is set if a quadruple $(g^a, g^b, g^c, e(g,g)^{abc})$ and a quadruple $(g^a, g^b, g^c, e(g,g)^z)$ cannot be distinguished by a non-negligible advantage by an attacker A in polynomial time, where $g^a, g^b, g^c \in G$, $a,b,c,z \in Z_P$. Then the advantage $ADV_A^{DBDH}(\kappa)$ of the attacker A is defined as:

$$ADV_A^{DBDH}(\kappa) = \left| \Pr\left[A(g^a, g^b, g^c, e(g,g)^{abc}) = 1 \right] - \Pr\left[A(g^a, g^b, g^c, e(g,g)^z = 1 \right] \right| \quad (1)$$

1) EBGN.KeyGen(l,k): Generate $k+1$ primes $Q_1, Q_2, \cdots, Q_{k+1}$, where $|Q_i| = l, i \in \{1,2,\cdots,k+1\}$. Then, generate an elliptic curve e of order $N = \prod_{i=1}^{k+1} Q_i$ and a group g of points on its elliptic curve and have $ord(g) = N$, where $ord(g)$ denotes the order of *g*. Next, randomly choose $k+1$ generators of *g*, namely: $g_1, g_2, \cdots, g_{k+1}$, such that $ord(g_i)=N, i\in\{1,2,\cdots,k+1\}$. Finally, calculate $P_i=(N/Q_i)\cdot g_i, i\in\{1,2,\cdots,k+1\}$ and $R=(N/Q_{k+1})\cdot g_{k+1}$ through $ord(P_i)=Q_i$ and $ord(R)=Q_{k+1}$. The public key $PK_{EBGN}=\left(N,e,\{P_1,P_2,\cdots,P_k\},R\right)$ and the secret key $SK_{EBGN}=\left(Q_1,Q_2,\cdots,Q_k\right)$ can be obtained.

2) EGBN.Enc(M_{S_i}, PK_{EBGN}): For the *k*-dimensional data $M_{S_i}=\{M_{i,1},M_{i,2},\cdots,M_{i,k}\}$ collected from the intelligent terminal S_i, $0\le\Re_i\le N$ is randomly selected. The following calculations are made:

$$C_i=\sum_{j=1}^{k}(M_{i,j}\cdot P_j)+\Re_i\cdot R \tag{2}$$

3) EBGN.Add($C_1,C_2,\cdots,C_n$): Cipher-text aggregation is calculated as follows:

$$\begin{aligned} C &= C_1+C_2+\cdots+C_n \\ &=\sum_{j=1}^{k}(\sum_{i=1}^{n}M_{i,j}\cdot P_j)+\sum_{i=1}^{n}\Re_i\cdot R \end{aligned} \tag{3}$$

4) EBGN.Dec(Q_j,P_j,C): In the decryption process, in order to understand the *jth* dimension data in the dense aggregate data, the method λ and Baby-step and Giant-step algorithms are required to calculate the discrete logarithm in the decryption algorithm, as shown below:

$$\begin{aligned} M_{d_j} &= \sum_{i=1}^{n}M_{i,j} \\ &=\log_{g_j'}((N/Q_j)\cdot C) \end{aligned} \tag{4}$$

Where, $g_j' = \prod_{i=1,i\neq j}^{k+1} Q_i\cdot P_j = N/Q_j\cdot P_j$.

III. Demand Side Blockchain Aggregation and Access Control Architecture

This paper first presents a demand-side data aggregation and access control framework, as shown in Fig. 3.

The smart meter installed on the user side can collect various privacy information, such as the user's basic identity information and the user's electricity consumption data, as shown in Table I.

Secondly, smart meters or smart terminals can collect information data such as power information and power environment. A collector, a concentrator, and gateways at all levels are adopted through a Home Area Network, BAN (Building Area Network), and NAN (Neighborhood Area Network), which is uploaded to the control center and cloud server [12]. The collected blockchain is encrypted using EBGN homomorphic encryption in the in-home network HAN, and the blockchain is aggregated at the building area network BAN gateway. The control center can decrypt and access the fine-grained data of the corresponding dimension, that is, the total power consumption data in the region, and share the data with the access authority [13]. At the same time, the access organization can access the fine-grained data of its authorized dimension to analyze the related work.

Based on the above framework, Fig. 4 shows the demand-side blockchain aggregation and access control model in this paper, which includes five parts, namely, trust authority, smart meter, gateway, control center, and access authority.

TABLE I. Data Information may be Provided on the Demand Side

Data element	Description
Name	Account responsible party
Address	Place of service
Account	A representation unique to the account
Electricity information	Kilowatt-hour consumption recorded for the current billing period
Other information	Environmental monitoring, equipment load, fault, power quality, distribution transformer status, etc.

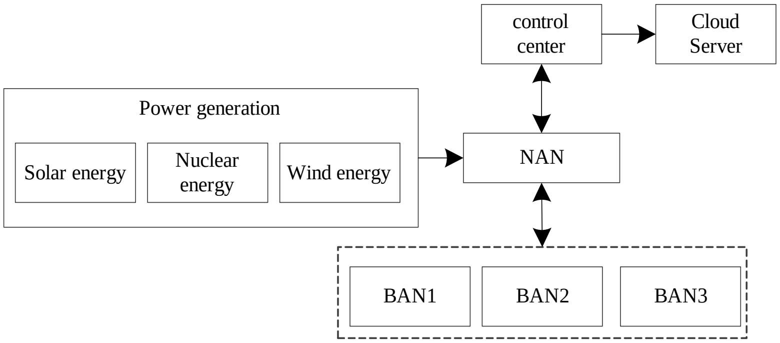

Fig. 3. Data Aggregation and Access Control Structure Block Diagram of Demand Side.

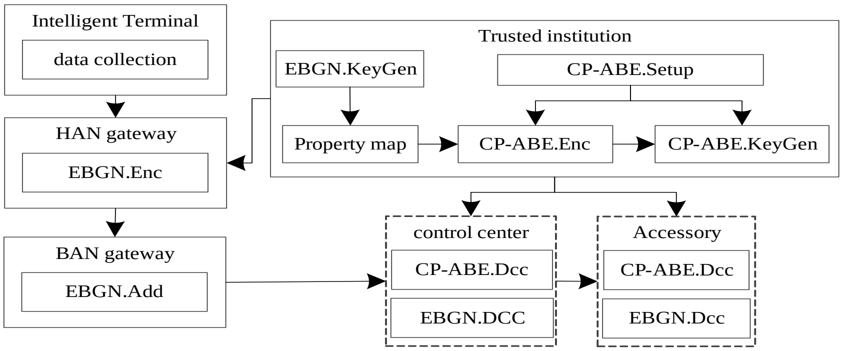

Fig. 4. Demand Side Blockchain Aggregation and Access Control Model.

The system model includes the following four operations: system initialization, blockchain encryption and aggregation, data access, and access permission update.

System initialization: The trusted authority performs the system initialization operation. First, the trusted authority generates the system parameters for EBGN and CP-ABE [14]. According to the access control policy of the control center and the access authority, the trusted authority generates the key of the CP-ABE and sends it to them. Next, it generates a mapping table indicating the mapping relationship between the public keys of the attribute set EBGN of the data. Finally, the trusted authority encrypts the EBGN key using the CP-ABE with the corresponding attribute set.

Blockchain encryption and aggregation: perform blockchain aggregation and encryption at the gateway. First, the data is categorized into multiple dimensions based on its attributes. Next, the gateway selects the corresponding EBGN public key from the mapping table and encrypts the blockchain. Finally, the cipher-text is sent to the superior gateway, and each gateway is responsible for aggregating all blockchains into one cipher-text [15].

Data access: In the data sharing process of blockchain, by using the CP-ABE key obtained from the trusted authority, the control center and each visitor can obtain the authorized data information of the corresponding dimension [16].

Access renewal: For key renewal of EBGN and CP-ABE, to revoke an accessor's access, the trusted authority first regenerates the EBGN's public and secret keys for the affected dimension. The trusted authority then re-encrypts the EBGN key and revokes the visitor's access to the corresponding attribute [17].

IV. Implementation of Blockchain Data Control Scheme in cloud Platform Area

A. Initial System Establishment

Given public parameters *l* and *k.* A security parameter k is set if, in any probabilistic polynomial time, it cannot be successfully computed by attacker A with a non-negligible advantage. The security parameter l is sent to the attribute authority, and the attribute authority calculates its own master key. The trusted authority runs EBGN.KeyGen(l,k) and ABE.Setup () functions to generate system public parameters:

$$\begin{cases} PK_{EBGN} = \left(N, e, \left\{P_1, P_2, \cdots, P_k\right\}, R\right) \\ SK_{EBGN} = \left(Q_1, Q_2, \cdots, Q_k\right) \\ PK_{CP-ABE} = \left(G, g^{\sum GID}, U_{GID}\right) \\ MK_{CP-ABE} = \left(\alpha, \chi\right) \end{cases} \quad (5)$$

The first dimension is set as the total power consumption of the user. The corresponding EBGN public key is P_1, and the control center is granted access rights. If the key *Q* of EBGN is used as the plaintext data encrypted by CP-ABE, the cipher-text encrypted by CP-ABE and the CP-ABE key generated for the control center and the visitor are as follows.

$$CT_i = CP - ABE.Enc\left(Q_i, \tau_i, PK_{CP-ABE}\right), i \in \left\{1, 2, \cdots, k\right\} \quad (6)$$

$$SK_{uj} = CP - ABE.KeyGen\left(S_{uj}, MK_{CP-ABE}, GID\right), j \in \left\{1, 2, \cdots, m\right\} \quad (7)$$

Where S_{uj} represents the attribute set. MK_{CP-ABE} represents the master key, and *GID* represents the visitor identity. Let SK_{u1} denote the key of the control center and *m* denote the total number of visitors. The EBGN key Q_i is encrypted according to the access structure τ_i . Finally, the private data and the visitor are encrypted and accessed according to the attribute mapping table, and the key SK_{uj} is sent to the visitor *uj* (such as a control center) through secure communication [18].

B. Blockchain Encryption and Aggregation

A terminal S_i in an area collects *k* types of data information according to different attribute sets, which is represented as $M_{S_i} = (M_{i,1}, M_{i,2}, \cdots, M_{i,k})$. The cipher-text after the value of $M_{i,j}$ of each dimension does not exceed the constant *B* and the data information C_i is encrypted by EBGN, which is shown below.

$$C_i = EBGN.Enc(M_{S_i}, PK_{EBGN}) \quad (8)$$

After receiving all the cipher-text information C_i , the gateway performs data aggregation on the cipher-text information is in the following manner.

$$C = EBGN.Add(C_1, C_2, \cdots, C_n) \tag{9}$$

The gateway then sends the encrypted and aggregated data to the control center.

Taking the *jth* dimensional data $M_{i,j}$ in the data collected by the terminal S_i as an example, the following calculation can be performed.

$$M_{i,j} = \sum_{l=0}^{|M_{i,j}|} 2^l \cdot M_{i,j,l} \tag{10}$$

$$P_{j,l} = 2^l \cdot P_j, \ \ 1 \le l \le |B| \tag{11}$$

$$R_l = 2^l \cdot R, \ \ 1 \le l \le |R| \tag{12}$$

The encrypted cipher-text is shown in the following calculation.

$$\begin{aligned} C_i &= (\sum_{j=1}^{k} \sum_{l=0}^{|M_{i,j}|} M_{i,j,l} \cdot P_{j,l}) + \sum_{l=0}^{|\Re_i|} \Re_{i,l} \cdot R_l \\ &= (\sum_{j=1}^{k} \sum_{M_{i,j,l}}^{|M_{i,j}|} P_{j,l}) + \sum_{l=0,\Re_{i,l}}^{|\Re_i|} R_l \end{aligned} \tag{13}$$

Where $M_{i,j,l}$ denotes the *lth* bit of $M_{i,j}$ and $\Re_{i,l}$ denotes the *lth* bit of $\Re_i$.

C. Data Access

For example, the first dimension is the total power consumption data. If the control center needs the total power consumption data C_1 in the access area, the control center first needs to download the cipher-text data of the EBGN key Q_1 from the trusted institution and perform CP-ABE decryption to obtain the EBGN key as shown below.

$$Q_1 = CP - ABE.Dec\left(CT_1, SK_{u1}, \tau, GID\right) \tag{14}$$

According to the key Q_1 and the aggregate cipher-text *C*, the control center may obtain the data information of the first dimension through the following calculation.

$$M_{d_1} = EBGN.Dec(Q_1, P_1, C) \tag{15}$$

Therefore, the control center can obtain the data information of the first dimension, that is, the total power consumption demand in the region. The control center sends the aggregate cipher-text *C* to the visitor in order to share the power data to the access mechanism. Similar to the control center, each visitor DA_{u_i} first needs to download the data cipher-text C_j satisfying his access policy [19]. Then, the EBGN key Q_j of the *jth* dimension is obtained by decrypting C_j as follows.

$$Q_j = CP - ABE.Dec(C_j, SK_{u_i}, \tau, GID) \tag{16}$$

Next, the visitor can obtain the specific data information of the *jth* dimension through the EBGN decryption algorithm, as shown below.

$$M_{d_j} = EBGN.Dec(Q_j, P_j, C) \tag{17}$$

In this process, in addition to updating access rights, only the control center and each visitor need to perform CP-ABE decryption. In addition, the control center cannot obtain the data information of all dimensions, so there is no need to decrypt and re-encrypt the data information of all dimensions.

V. Experimental Analysis

In this paper, the performance of the proposed scheme is analyzed in terms of computational cost and communication overhead. Although system initialization also incurs computational costs, it only needs to be deployed once, which has a negligible impact on smart grid performance. Therefore, only the efficiency of encryption, aggregation, and decryption is tested here in experiments.

In the experiment, we first compare the encryption efficiency of the proposed scheme with that of scheme 2 in [20] and scheme 3 in [21]. Scheme 2 uses super-increasing sequence and Paillier homomorphic encryption to achieve the privacy protection of blockchain aggregation. Reference [21] constructs a Scheme 3 scheme based on Paillier and ABE, which integrates data aggregation and access control.

Experiments were conducted using the LiDIA library and the MIRALC environment by running on a PC with a 4.6 GHz processor and 16 GB of memory. The length of the key is chosen to be $l = 256$ bits, and the length of the random number is chosen to be $|R| = 70$ bits so that the present security can be ensured. For Scenario 2, the blockchain is merged into one plain text before encryption, which is the simplest and most efficient super-incremental sequence. Scenario 2 and Scenario 3 are set the same, using the Paillier public key with a length of 1024 bits.

A. Cost Calculation

For data aggregation, the experiment takes 10 milliseconds to perform 100 aggregations in the scheme in this paper. In that data access phase, only the CP-ABE is executed to decrypt the EBGN key of the authorized single dimension, and the key of all dimensions does not need to be decrypted, so the influence on the efficiency of data share is small. Since Scenario 2 and Scenario 3 need to perform more operations on the gateway and the control center, such as decrypting and re-encrypting the aggregated data on the control center.

The experimental results are shown in Fig. 5.

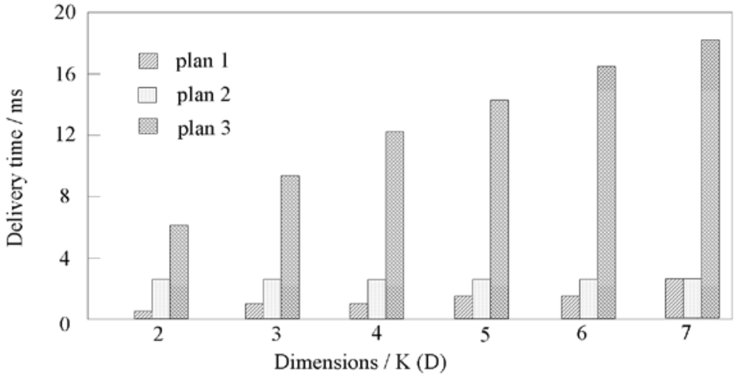

Fig. 5. Encryption Overhead in different Dimensions.

Since Scheme 2 always requires random numbers to be subjected to modular exponentiation, the encryption time of the blockchain does not increase with the number of dimensions. Moreover, Scheme 3 needs to generate multiple cipher-texts for the blockchain, and its encryption time increases linearly with the dimension. It can be concluded that the encryption time of the scheme in this paper is less than that of the scheme 2 when the dimension is $k < 7$. When $k = 7$, the efficiency of the scheme in this paper is similar to that of scheme 2.

B. Communication Overhead

The communication overhead of the data information, i.e., the cipher-text of the EBGN in the scheme in this paper, is considered. According to the encryption algorithm, the length of the power data cipher-text is $2 \cdot (k+1) \cdot l$ bits. When we choose the length of the key to be $l = 256$ bits and set $k = 7$, the length of the power data cipher-text is 4096 bits.

For Scheme 2, the cipher-text length of the blockchain is 2048 bits, which is the same as the cipher-text of one dimension in Scheme 3. The communication comparison between the scheme in this paper and the schemes 2 and 3 is shown in Fig. 6.

When $k = 7$ and $l = 256$ bits, the length of the power data cipher-text is 4096 bits in the scheme of this paper, which is twice of the cipher-text in the scheme 2. However, it is much smaller than the cipher-text 14336 bits in Scheme 3. The transmission of the cipher-text can be done immediately according to a common communication standard between the user and the building gateway. Compared with the encryption time, the impact of communication on the timeliness of smart grid is basically negligible.

Compared with other schemes in terms of computation cost and communication overhead, the scheme proposed in this paper is more effective in the case of low dimensionality, which is suitable for the encryption efficiency requirements of smart grid, and can achieve flexible and fine-grained access control and permission update at the dimensionality level, so the scheme proposed in this paper is more flexible and practical.

C. Privacy Protection Strength

The algorithm, PTM mechanism and GIPL mechanism are tested with different data sets. Firstly, the trajectory data is processed and then different random noises are added to the data. Then, the DTW value is calculated to represent the trajectory distortion, and the privacy protection performance of the trajectory data is analyzed. According to different distance thresholds, the experiment was divided into five groups, and the distance thresholds of each group were 100m, 300m and 500m, respectively. Each group of experiments was performed 100 times, and the final result was the average of the results of 100 times.

In a stationary user scenario, simulated data is used for experimental validation. In this scenario, because the user is in a static state, a trajectory sequence with all the same position points are simulated. There are 1000 identical position points in the trajectory sequence, so there is no need to set different distance thresholds, as shown in Fig. 7.

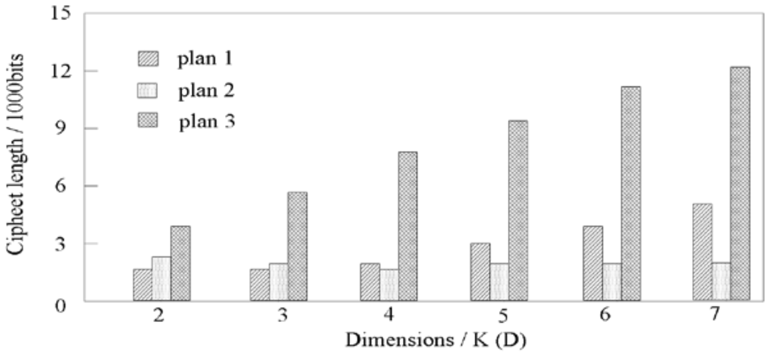

Fig. 6. Cipher-text Length in different Dimensions.

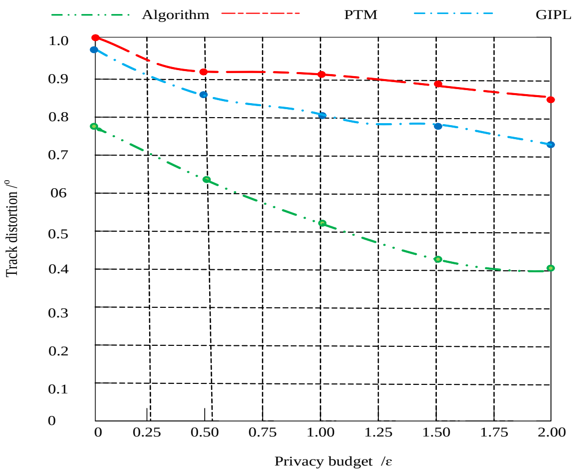

Fig. 7. Trajectory Distortion under different Privacy Budgets.

In Fig. 7, with the increase of privacy budget, the trajectory distortion of the algorithm, PTM mechanism and GIPL mechanism in this paper are decreasing, and the degree of privacy protection is also decreasing. However, no matter how the privacy budget changes, the trajectory distortion of the proposed algorithm is always smaller than that of PTM and GIPL.

The Geolife dataset is used for experimental validation in the low-speed running user scenario as shown in Fig. 8.

In Fig. 8, in the case of the same distance threshold, the trajectory distortion of the method proposed in this paper decreases with the increase of privacy budget, that is to say, in the case of the same distance threshold, as the privacy budget continues to increase, the closer the protected trajectory is to the original trajectory, the lower the degree of privacy protection is. Moreover, under the same privacy budget, the trajectory distortion of the proposed algorithm is always lower than that of PTM and GIPL.

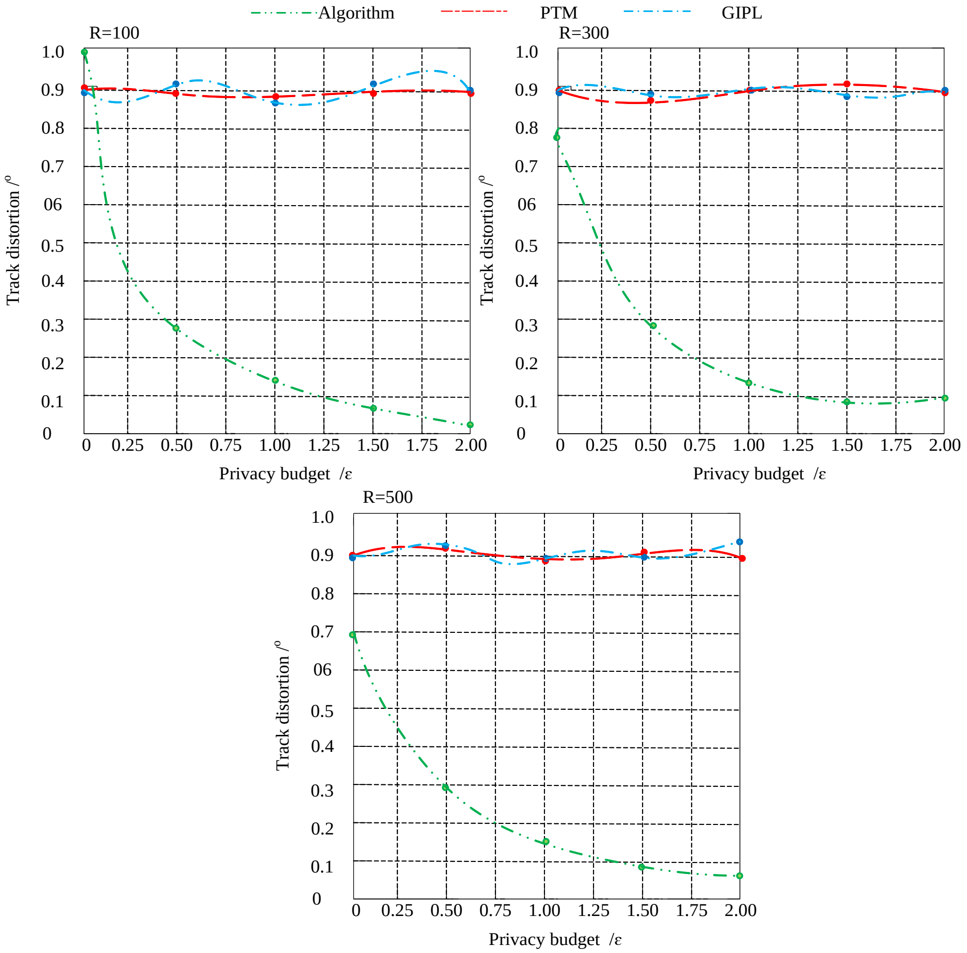

Fig. 8. Trajectory Distortion of Geolife Data Set under different Privacy Budgets.

VI. Conclusion

This paper explores the aggregation and access control of cloud Internet of Things blockchain on the demand side of the smart grid.

1) The related knowledge of smart grid data aggregation is studied, and the cloud Internet of Things data aggregation and access control privacy protection architecture on the demand side is proposed.

2) Based on this architecture, a blockchain aggregation and access control model is established. Encryption via EBGN preserves the priority of the blockchain and can decrypt each dimension separately using the corresponding key. By encrypting the EBGN key with a cipher-text policy attribute encryption algorithm, the scheme can achieve fine-grained access control.

3) The access rights can be updated flexibly and safely by regenerating the relevant parameters of EBGN and CP-ABE. Secondly, the security of privacy protection, access control, and access permission update of blockchain in this paper are analyzed and proved.

4) Through the performance analysis and comparison of the proposed scheme and similar schemes in terms of computing cost and communication overhead, it is shown that the proposed scheme has significant advantages in terms of computing cost and flexible fine-grained access control of blockchain in the face of a large number of smart grid demand-side terminals, large amount and variety of data, and the need for classification.

The research method in this paper realizes the encryption and aggregation of multi-dimensional data in the cloud Internet of Things. Each dimension can be encrypted with different public keys, and the multi-dimensional data is fused into a cipher-text. The EBGN private key of each dimension is encrypted by the cipher-text policy attribute encryption algorithm. The visitor is authorized to access the fine-grained data of the corresponding dimension, thus realizing the fine-grained access control of the multi-dimensional data.

In the privacy protection of the smart grid, this paper considers the privacy protection scheme on the demand side under the data aggregation model. It does not consider the smart grid marketing architecture, the home gateway smart community, and the privacy protection scheme under the vehicle networking model. In the future, the research on privacy protection schemes can be carried out under the multi-model of smart grid.

References

[1] A. Abdallah, X. S. Shen. Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections. IEEE Transactions on Vehicular Technology, 2017, 66(3):2615-2629.

[2] E. Mengelkamp, J. Gärttner, and K. Rock. Designing microgrid energy markets A case study: The Brooklyn Microgrid. Applied Energy, 2018, 210:870–880.

[3] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, X. Shen. Fine-grained data access control with attribute-hiding policy for cloud-based IoT. Computer Networks, 2019, 153:1-10.

[4] J. Huang, C. Lin, H. Zhou, Z. Xu, and C. Lin. Research on key technologies of deduction of multinational power trading in the context of Global Energy Interconnection. Global Energy Interconnection, 2019, 2(6):560-566.

[5] J. W. Bos, W. Castryck, I. Iliashenko, F. Vercauteren. Privacy-Friendly Forecasting for the Smart Grid Using Homomorphic Encryption and the Group Method of Data Handling. International Conference on Cryptology in Africa, 2017, 18201.

[6] J. Zhang, et al. Design scheme for fast charging station for electric vehicles with distributed photovoltaic power generation. Global Energy Interconnection, 2019, 2(2):150-159.

[7] K. Xue, W. Chen, W. Li, J. Hong, P. Hong. Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage. IEEE Transactions on Information Forensics and Security, 2018, 13(8):2062-2074.

[8] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. L. Wei, P. Hong. RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage. IEEE Transactions on Information Forensics and Security, 2017, 12(4):953-967.

[9] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. L. Wei, P. Hong. RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage. IEEE Transactions on Information Forensics and Security, 2017, 12(4):953-967.

[10] M. A. Ferrag, L. Maglaras, A. Ahmim. Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey. IEEE Communications Surveys & Tutorials, 2017, 19(4):3015-3045.

[11] M. Kim, et al. A secure charging system for electric vehicles based on blockchain. Sensors (Switzerland), 2019, 19(13):1-22.

[12] M. S. Rahman, A. Basu, S. Kiyomoto, M. Z. A. Bhuiyan. Privacy-friendly secure bidding for smart grid demand-response. Information Sciences, 2017, 379:229-240.

[13] N. Saxena, B. J. Choi. Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks. IEEE Transactions on Information Forensics & Security, 2017, 11(7):1438-1452.

[14] P. Liu, W. Jiang, X. Wang, H. Li, and H. Sun. Research and application of artificial intelligence service platform for the power field. Global Energy Interconnection, 2020, 3(2):175-185.

[15] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov. blockchain in smart grids: A review on different use cases. Sensors (Switzerland), 2019, 19(22):1-25.

[16] Xu Zhuxia, Zhang Chunyan, Xu Juan. Design of Storage and Service System of Meteorological Big Data Cloud Platform in Gansu Province. Information Technology and Informatization, 2022(02):53-57.

[17] Y. Jiang, W. Susilo, Y. Mu, F. Guo. cipher-text-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems, 2018, 78:720-729.

[18] Y. Xia, W. Chen, X. Liu, L. Zhang, X. Li, Y. Xiang. Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(10):2629-2641.

[19] Y. Jiang, C. Wang, Y. Wang, and L. Gao. A cross-chain solution to integrating multiple blockchains for IoT data management. Sensors (Switzerland), 2019, 19(9):1-18.

[20] Z. Ji, X. Wang, C. Cai, and H. Sun. Power entity recognition based on bidirectional long short-term memory and conditional random fields. Global Energy Interconnection, 2020, 3(2):186-192.

[21] Zhang Lu. Based on Research on data security of network service cloud platform based on OSI model. Modern electronic technology, 2020, 43(05):74-77+81.