Sensors and Materials, Vol. 37, No. 1 (2025) 207–216
MYU Tokyo

S & M 3901

Dynamic Sharing Algorithm for Power Grid Survey Data Based on Blockchain and Proxy Re-encryption

BangZheng He,[1] JingGuo Lv,[1*] JiYong Zhang,[2] ChunHui Zhao,[2]
DongHui Liu,[2] Hui Xu,[3] Bing Wu,[4] and Xiaohu Sun[2]

[1]College of Surveying and Urban Spatial Information, Beijing University of Civil Engineering and Architecture,
Beijing 102616, China
[2]State Grid Economic and Technical Research Institute Co.,
Beijing 102200, China
[3]Central Southern China Electric Power Design Institute Co., Ltd. of China Power Engineering Consulting Group,
Wuhan 430071, China
[4]Economic Research Institute of State Grid ZheJiang Electric Power Company,
Hangzhou 310020, China

(Received July 26, 2024; accepted January 21, 2025)

Keywords: multi-source survey data, dynamic sharing, blockchain, proxy re-encryption

Realizing the dynamic sharing of multi-source survey data in power grids helps to promote data flow and professional collaboration in the field of power grid surveying. Traditional attribute encryption methods suffer from inefficiency and poor security when coping with dynamic access in the data sharing process. To address the above problems, we propose a dynamic sharing algorithm for grid multi-source survey data based on blockchain and proxy re-encryption. A proxy re-encryption algorithm is designed to ensure the security of data sharing. Next, the user rights dynamic adjustment algorithm is designed to make the blockchain authorized nodes dynamically adjust the data access rights according to the business progress, so as to improve the efficiency of dynamic data sharing. Experiments showed that the method described in this paper is better than existing data sharing schemes in terms of computational overhead and dynamic sharing efficiency, and has certain advantages in the dynamic sharing of multi-source survey data in power grids.

1. Introduction

Dynamic data sharing is a crucial step in enhancing data value, preventing data silos, and ensuring the full utilization of data. By sharing data, different organizations and individuals can access and collaborate in real time, which facilitates faster data-driven decision-making and improves the accuracy and efficiency of decisions.

Currently, scholars worldwide are researching and practicing how to achieve dynamic data sharing. References 1 to 4 focus on using blockchain technology to address data sharing issues in specific industries, leveraging blockchain advantages in ensuring data dynamism and security through encryption and access control. References 5 to 7 concentrate on enhancing the

[*]Corresponding author: e-mail: lvjingguo@bucea.edu.cn
https://doi.org/10.18494/SAM5258

ISSN 0914-4935 © MYU K.K.
https://myukk.org/

dynamism and security of data sharing with blockchain, partially resolving issues related to system performance and computational overhead. Reference 8 introduces a security access control model with fine-grained access control based on attribute-based encryption under a blockchain model, whereas Ref. 9 proposes a blockchain data traceability algorithm based on attribute encryption. Although the above methods achieve dynamic data sharing to a certain extent, they suffer from poor data dynamics and low security owing to the adoption of a single-point-of-failure and centralized control approach.

Current research on data sharing in power grid engineering is largely focused on sharing data related to power equipment,(10–13) electricity consumption,(14) power line losses,(15) power trading,(16) and the supply chain of power materials.(17) There is essentially no targeted research on sharing multi-source survey data for power grids. The sharing of multi-source survey data in power grids still relies on simply applying existing sharing algorithms without tailored improvements based on survey operations, often failing to meet the needs of cross-disciplinary data sharing.

In power grid projects, especially ultrahigh voltage ones, numerous units and specialties are involved in surveying. The current decentralized storage and independent management of on-site collected multi-source survey data prevent real-time access and dynamic updates, posing significant risks to the project's layout and site selection. Delays in adjusting the overall engineering design plans lead to increased workload, extended schedules, and higher costs.

In this paper, by integrating the content of multi-source survey data in power grids, we propose solutions to the specific problems existing in the dynamic sharing of multi-source survey data in power grids. The contributions of this paper are summarized as follows.

(1) We constructed a proxy re-encryption algorithm for the dynamic sharing of multi-source survey data in power grids based on blockchain. We designed a proxy re-encryption algorithm based on the SM2 encryption algorithm to achieve the dynamic sharing of multi-source survey data in power grids while ensuring data security.

(2) We proposed a method for dynamically adjusting user permissions for the dynamic sharing of multi-source survey data in power grids. By leveraging blockchain nodes to divide the work and manage proxy re-encryption keys, the authorization management node verifies user data access permissions, achieving deterministic updates of user access permissions. It allows the dynamic adjustment of the visibility of multi-source survey data in power grids, eliminating the need to re-encrypt data when authorization changes.

2. Multi-source Survey Data for Power Grids

Power grid surveying is one of the preparatory steps for the design and construction of power grids. The survey data for power grids is sourced from various units and specialties, including geology, surveying, hydrology, meteorology, and other fields, characterized by a wide range of sources, diverse types, and large volume. Currently, there is no dynamic sharing of foundational data between surveying and design professions, leading to issues such as redundant data collection and modeling, and low data integration efficiency, which is not conducive to the comprehensive utilization of data resources. Table 1 shows the specifics of the multi-source survey data for the design phase of the survey operation.

3. Scheme Design

3.1 System models and entity

We provide a new solution for the dynamic sharing of power grid engineering survey data. As shown in Fig. 1, the scheme of this paper mainly contains four entities: data sharer, data user, authorized manager, and blockchain node.

Data sharer: member of either the meteorological, hydrological, geotechnical, surveying, or other professional working groups under the power grid engineering survey department. Data

Table 1
Design phase content of multi-source survey data for power grids.

Name	Content	Format	Real-time vs non-real-time
Image data	Remote sensing data, aerial data, laser point cloud data, etc.	TIFF, PNG, JPG, GeoTiff, IMG, GIF, BMP	real-time
Video data	Live video, surveillance video data	MP4, AVI, JPEG, PNG	non-real-time
Tower base measurement data	Tower base section, topographic data element attribute information	XML, HTML, JSON, YAML, CSV	real-time
Hydrological data	Attribute information of basic data elements of flow velocity, flow, and dam, etc.		
Meteorological data	Wind speed and ice cover data element attribute information, etc.	XML, HTML, JSON, YAML, CSV	real-time
Geotechnical data	Attribute information of exploration data elements of exploration points, etc.		

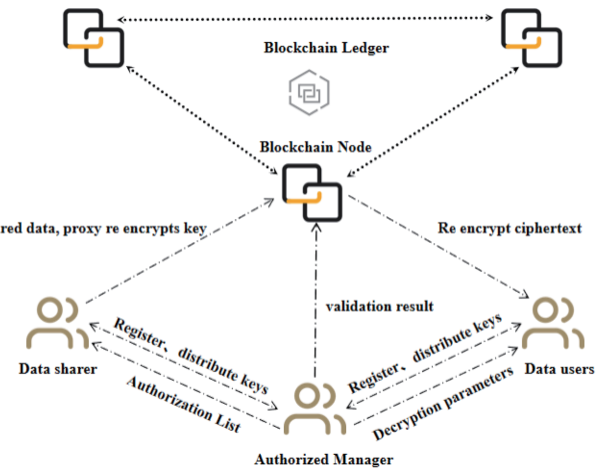


Fig. 1. (Color online) Dynamic sharing system model of multi-source survey data for power grid based on blockchain and proxy re-encryption.

sharers are responsible for encrypting the shared data to generate the initial ciphertext, specifying the data access rights, deciding on the revocation and reconstruction of user rights, and constructing the proxy re-encryption key.

Data user: member of either the working groups in grid engineering design or other departments. Data users request access to grid multi-source survey data on the blockchain and decrypt re-encrypted data using private keys and decryption parameters to obtain shared data.

Authorized manager: authorized member of the power grid engineering survey business management department. The authorized manager achieves decentralized system management, elects management nodes through blockchain consensus mechanism, completes node registration, manages key distribution, verifies data user rights, sends decryption parameters to legitimate users, and collaborates with data sharers to update shared data access rights.

Blockchain node: re-encrypts shared data using a proxy re-encryption key provided by a data sharer and decrypts and transmits the re-encrypted shared data to the data user. The blockchain node broadcasts the shared data record over a period of time and other nodes verify the record and add it to the blockchain ledger.

3.2 Specific program processes

The scheme proposed in this paper is divided into four main phases, as shown in Fig. 2.

3.2.1 System establishment phase

There are two steps in this phase, namely, system activation and key generation, which mainly include the initialization of system parameters, the generation of blockchain public and private keys, and the establishment of the data encryption base.

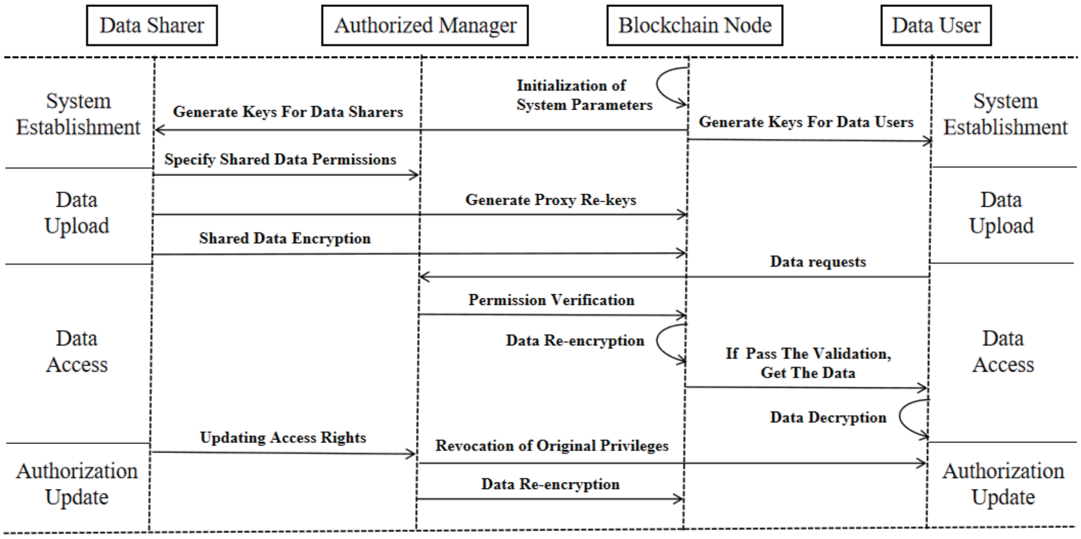


Fig. 2. Program flow.

(1) System Initialization. Determine the security parameter α, based on which select primes p and q, and define an elliptic curve θ over the finite field F_p. Choose a point G on the elliptic curve as the generator of the group G, which is a cyclic group of order q. Define the following hash functions: H_1:$\{0, 1\}^* \rightarrow \{0, 1\}^3$, H_2:$G \rightarrow Z_q^*$, H_3:$\{0, 1\}^* \rightarrow G$, H_4:$\{0, 1\}^* \rightarrow G$. The set of public parameters is $\pi = \{H_1, H_2, H_3, H_4, P, \theta, G\}$.

(2) Key Generation. Input the public parameter π and choose a random number $\beta \in Z_q^*$, the private key $S = \beta$, and the public key $Q = \beta p$.

3.2.2 Data upload phase

There are three steps in this phase: the initial encryption of shared data, the generation of proxy re-encryption key parameters, and the generation of the proxy re-encryption key. This phase mainly includes the following: the data sharer encodes the shared data using the public key, generates the initial data ciphertext, specifies the access rights to the shared data according to the survey business requirements, and generates the corresponding agent re-encryption key. The key and the initial data ciphertext are subsequently broadcast to the blockchain network, while the data authorization list is sent to the authorized manager.

(1) Initial Encryption. The data sharer uses the public key PK_A to encrypt the message M, where the length of M is 2, and selects $i \in G$. The process is as follows.

$$r = H_2(i) \tag{1}$$

$$C_1 = rP = (x_0, y_0) \tag{2}$$

$$rPK_A = (x_A, y_A) \tag{3}$$

$$t = H_1(x_A \parallel y_A) \tag{4}$$

$$C_2 = M \oplus t \tag{5}$$

$$C_3 = H_3(x_A \parallel M \parallel y_A) \tag{6}$$

$$C_4 = H_4(M \parallel C_1 \parallel C_3) \tag{7}$$

$$C = (C_1, C_2, C_3, C_4) \tag{8}$$

The shared data is initially encrypted and published to the blockchain for broadcasting, then verified by the blockchain node. The data sharer can access the uploaded shared data and decrypt it using a private key. The decryption process is as follows.

$$S = SK_A C_1 = (x_A \parallel y_A) \tag{9}$$

$$t = H_1(x_A \parallel y_A) \tag{10}$$

$$M = C_2 \oplus t \tag{11}$$

$$C_3' = H_3(x_A \parallel M \parallel y_A) \tag{12}$$

(2) Proxy Re-encryption Key Parameter Generation. The data sharer constructs proxy re-encryption key parameters for data user B. $DL = \{rPK_A,\ rPK_B\}$ is a random number chosen by the data sharer.

(3) Proxy Re-encryption Key Generation. The data sharer calculates the proxy re-encryption key for data user B using the proxy re-encryption key parameter β and the authorization parameter α. The key $RK_{A\to B}$ is uploaded to the blockchain network, that is,

$$RK_{A\to B} = H_1(rPK_A) \oplus (rPK_B \parallel \alpha). \tag{13}$$

3.2.3 Data access phase

There are two steps in this phase: proxy re-encryption and data decryption. It mainly includes the following: the data user submits data access request to the blockchain. The authorization management verifies the user rights from the authorization list provided by the data sharer. After verification, the blockchain node re-encrypts the data using the proxy re-encryption key to ensure that only authorized users decrypt and access the data.

(1) Proxy Re-encryption. Data users send requests to the blockchain node, seeking to access specified shared data. If a data user is authorized, the blockchain node uses the proxy re-encryption key RK_A uploaded by the data sharer to perform proxy re-encryption on the initial data ciphertext, generating a new ciphertext C'. The calculation formula is as follows.

$$C_1' = C_1 \tag{14}$$

$$C_2' = RK_{A\to B} \oplus C_2 \tag{15}$$

$$C_3' = C_3 \tag{16}$$

$$C_4' = C_4 \tag{17}$$

$$C' = (C_1', C_2', C_3', C_4') \tag{18}$$

(2) Decryption. Data users, after obtaining the re-encrypted data from the blockchain node, can use their private key and the decryption parameter J sent by the authorized manager to decrypt the encrypted data. The decryption process for the data users is as follows.

$$M' = C_2 \oplus H_1(SK_B C_1' \parallel J) \tag{19}$$

$$k = H_4(M' \parallel C_1' \parallel C_3') \tag{20}$$

3.2.4 User authorization update phase

There are three steps in this phase: user A authorizes user B, user A authorizes user C, and authorization revocation. This phase mainly includes the following: the data sharer interacts with the blockchain authorization management, updates the authorization list to complete the update of shared data access rights, and dynamically adjusts the blockchain data visibility.

(1) User A authorizes user B. Subsequently, data sharer A interacts with the authorized manager to update the authorization list L, adds authorization parameters for user B, and constructs the corresponding proxy, while broadcasting the re-encryption key $RK_{A\to B}$ to the blockchain network.

(2) User A authorizes user C. Data sharer A interacts with the authorization manager to update the authorization list L, adds authorization parameters for data user C, and constructs the corresponding proxy re-encryption key $RK_{A\to C}$, which is then broadcast to the blockchain network.

(3) Authorization revocation. Data sharer A revokes the access rights of data user C. Data sharer A interacts with the authorized manager to remove the corresponding authorization list parameters.

During the authorization update, after the data sharer has initially encrypted the data, the permission update does not need to re-encrypt the data, but simply sends the authorization list to the authorized manager and generates a proxy re-encryption, and then broadcasts the key to the blockchain node.

4. Experiment

4.1 Functional comparison

Reference 8 proposes an algorithm that combines attribute encryption with proxy re-encryption for hidden access policy, Ref. 18 proposes a ciphertext policy attribute encryption algorithm with a partially hidden access structure, Ref. 19 proposes an attribute-encryption-based blockchain data traceability algorithm, and Ref. 20 proposes an attribute revocation ciphertext policy attribute-based encryption-based blockchain data access control algorithm. Next, we compare this paper's algorithm with the existing algorithms in terms of whether it supports shared data access control, whether it is able to share large-scale datasets, whether permission updates are deterministic, whether it is proxy re-encryption, and whether multi-source heterogeneous survey data are applicable. The results are shown in Table 2.

4.2 Performance analysis

The configuration of the experimental host in this paper is a 3.40 GHz, AMD Ryzen 7 PRO 5845 CPU and NVIDIA T1000 graphics card, with Python 3.9.6 as the programming tool. The experiment adopts the 256-bit elliptic curve recommended in the SM2 elliptic curve public key encryption algorithm standard, which is $y^2 = x^3 + ax + b$; curve parameters are shown in Table 3.

Table 2
Data content of electrical network engineering surveys.

Algorithm	Shared data access control	Large-scale dataset	Permission update	Proxy re-encryption	Survey data applicability
Ref. 8	✓	×	✓	✓	×
Ref. 18	✓	✓	×	×	×
Ref. 19	×	×	✓	×	×
Ref. 20	✓	✓	×	×	×
Ours	✓	✓	✓	✓	✓

Note: ✓ indicates that the algorithm uses this technology or has this function, while × indicates that the technology is not used or the function is not available.

Table 3
Parameters of the elliptic curve for SM2 public key encryption algorithm.

Curve parameters	Value
P	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFF
A	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFC
b	28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
n	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFF7203DF6B21C6052B53BBF40939D54123
xG	32C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7
yG	BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

Since Refs. 8 and 17 describe data sharing algorithms based on proxy re-encryption, they are closely related to the algorithm proposed in this paper. Therefore, a comparative analysis of computational costs was conducted between the algorithm in this paper and those described in Refs. 8 and 17, with the results shown in Fig. 3.

As can be seen from Fig. 3, during the system establishment phase, the time cost of the algorithm in this paper is less than that in the algorithm described in Ref. 8 and similar to that in the algorithm described in Ref. 17. However, the algorithm in this paper is built on a large-scale dataset of multi-source survey data for power grids, with parameter settings that consider the nonlinear relationship with the data scale, thus offering stronger scalability than the algorithms described in Refs. 8 and 17. In the data upload phase, which is performed by the data sharer, the algorithm in this paper takes the least amount of time compared with those described in Refs. 8 and 17. This is because the algorithm in this paper assigns access rights on the basis of survey business needs, reducing the computational cost for data sharers to encrypt data with their public key. During the data access phase, the algorithm in this paper takes less time to access data than the data sharing algorithms described in Refs. 8 and 17. In the user authorization update phase, the time spent by the algorithm in this paper is less than those in the algorithms described in Refs. 8 and 17 owing to the interaction between the data sharer and the authorized manager to update the authorization list without the need to re-encrypt the data.

From the user's perspective, as shown in Fig. 4(a), as the data volume increases, the re-encryption key generation time for the algorithms described in Refs. 8 and 17 gradually increases. However, the re-encryption key generation time for the algorithm in this paper is a relatively small fixed constant value, independent of the data volume. As shown in Fig. 4(b), the re-ciphertext decryption time for the algorithm in Ref. 17 increases linearly with the data

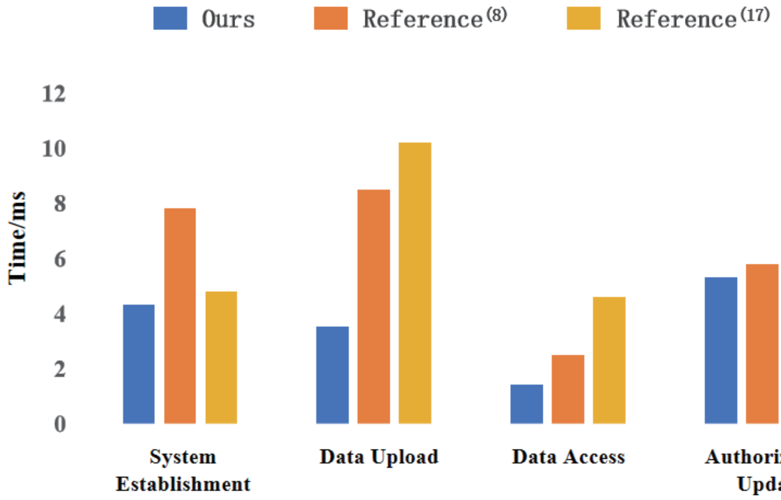
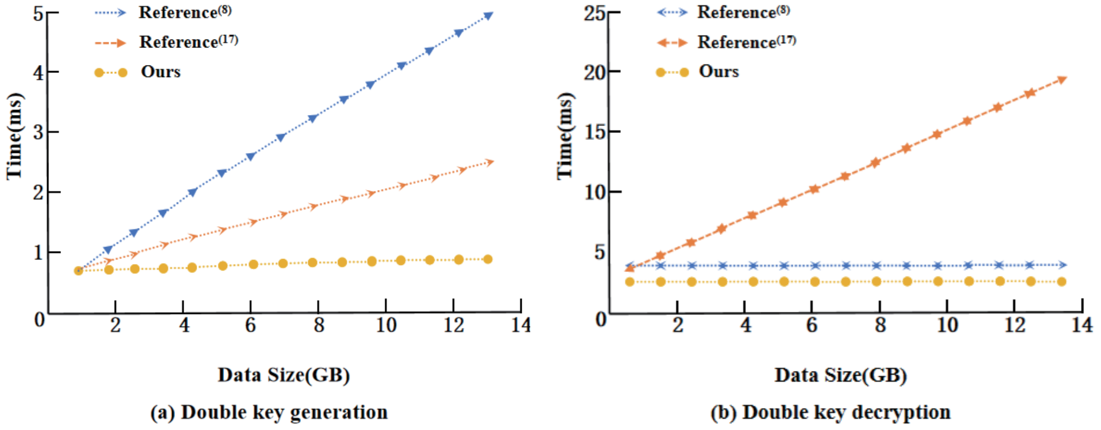


Fig. 3. (Color online) Computational cost comparison.



(a) Double key generation

(b) Double key decryption

Fig. 4. (Color online) Impact of data volume on the re-encryption key generation and re-ciphertext decryption phases. (a) Re-encryption key generation. (b) Re-encryption key decryption.

volume, whereas the decryption times for the algorithms in Ref. 8 and in this paper are both fixed constant values, but the algorithm in this paper requires less time for re-decryption than that in Ref. 8.

5. Conclusion

In this paper, we proposed a dynamic sharing algorithm for multi-source survey data in power grids based on blockchain and proxy re-encryption, which addresses issues in the dynamic sharing process of multi-source survey data for power grids. The algorithm optimizes access permission updates through proxy re-encryption and dynamic permission adjustment, reducing the need for re-encryption and achieving a balance between dynamic data sharing and privacy protection. Experiments showed that while the algorithm implements features such as dynamic sharing and privacy protection during the sharing process, it has lower computational overhead than existing data sharing schemes and meets the needs for dynamic data sharing in power grid surveying operations.

Acknowledgments

This study was supported by the Science and Technology Project of the State Grid Corporation of China: Research and Application of Multi-source Collaborative and Dynamic Data Sharing Technology for Power Grid Engineering Survey Data (5700-202356317A- 1-1-ZN).

References

1 X. Chen, M. Huang, Y. Tian, Y. Wang, S. Cao, and X. Zhang: J. Comput. Res. Develop. **61** (2024) 2246. https://doi.org/10.7544/issn1000-1239.202330899

2 Y. Zheng, H. Liu, and Y. Dong: J. Railw. Sci. Eng. **21** (2024) 2488. https://doi.org/10.19713/j.cnki.43-1423/u.T20231394

3 Y. Zhou, J. Zhu, and W. Zhang: Chin. J. Cancer Prev. Treat. **31** (2024) 325. https://doi.org/10.16073/j.cnki.cjcpt.2024.06.03

4 J. Zhu, C. Yan, Y. Ouyang, Y. Chen, and X. Wang: Intell. Autom. Soft Comput. **33** (2022) 1747. https://doi.org/10.32604/iasc.2022.026934

5 R. Siyal, J. Long, M. Asim, N. Ahmad, H. Fathi, and M. Alshinwan: Mathematics **12** (2024) 1596. https://doi.org/10.3390/math12131956

6 V. Jaiman and V. Urovi: IEEE Access **8** (2020) 143734. https://doi.org/10.1109/ACCESS.2020.3014565

7 F. Al-Zahrani: IEEE Access **8** (2020) 115966. https://doi.org/10.1109/ACCESS.2020.3002823

8 X. Li, X. Zhang, J. Gao, and D. Xiang: J. Xidian University **49** (2022) 1. https://doi.org/10.19665/j.issn1001-2400.2022.01.001

9 Y. Tian, K. Yang, Z. Wang, and T. Feng: J. Commun. **40** (2019) 101. https://doi.org/10.11959/j.issn.1000-436x.2019222

10 C. Liu, Q. Zhang, Y. Li, and H. Zhang: J. Shenyang University Technol. **46** (2024) 1. https://doi.org/10.7688/j.issn.1000-1646.2024.01.01

11 F. Guo, S. Liu, X. Wu, B. Chen, W. Zhang, and Q. Ge: Autom. Electr. Power. Syst. **47** (2023) 52. https://doi.org/10.7500/AEPS20220112003

12 S. Qin, W. Dai, H. Zeng, and X. Gu: Netinfo Secur. **23** (2023) 52. https://doi.org/10.3969/j.issn.1671-1122.2023.08.005

13 S. Deng, Q. Hu, D. Wu, and Y. He: Comput. Electr. Eng. **108** (2023) 108666. https://doi.org/10.1016/j.compeleceng.2023.108666

14 X. Wang, J. Du, L. Zhong, W. Xu, B. Liu, and W. Yu: J. Comput. Appl. **11** (2024) 1. https://doi.org/10.11772/j.issn.1001-9081.2024020173

15 Y. Xiang, L. Yang, B. Chen, and G. Li: Comput. Appl. Software **40** (2023) 333. https://doi.org/10.3969/j.issn.1000-386x.2023.07.051

16 B. Wang, Q. Guo, and Y. Yu: Appl. Energy **314** (2022) 118871. https://doi.org/10.1016/j.apenergy.2022.118871

17 J. Song, Y. Yang, J. Mei, G. Zhou, W. Qiu, Y, Wang. L. Xu, Y. Liu, J. Jiang, Z. Chu, W. Tan, and Z. Lin: Energy **15** (2022) 2570. https://doi.org/10.3390/en15072570

18 H. Cui, R. Deng, J. Lai, Y. Xun, and N. Surya: Comput. Networks **133** (2018) 157. https://doi.org/10.1016/j.comnet.2018.01.034

19 X. Yang, T. Li, X. Pei, L. Wen, and C. Wang: IEEE Access **8** (2020) 45468. https://doi.org/10.1109/ACCESS.2020.2976894

20 J. Li and Y. Qi: Comput. Eng. Des. **45** (2024) 348. https://doi.org/10.16208/j.issn1000-7024.2024.02.004