Research Article

A Privacy Protection Scheme for Facial Recognition and Resolution Based on Edge Computing

Junhua Wu,1 Wenzhen Feng,1 Guopeng Liang,1 Tiantian Wang,1 Guangshun Li,1 and Yuanwang Zheng2

1School of Computer Science, Qufu Normal University, Rizhao 276826, China
2Shandong Huatong Used Car Information Technology Limited Company, Jining 272600, China

Correspondence should be addressed to Guangshun Li; guangshunli@qfnu.edu.cn

Received 25 November 2021; Accepted 25 January 2022; Published 10 March 2022

Academic Editor: Yuling Chen

Copyright © 2022 Junhua Wu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Facial recognition and resolution technology have extensive application scenarios in the era of big data. It ensures the consistency of personal identity in physical space and cyberspace by establishing correspondence between physical objects and network entities. However, massive data brings huge processing pressure to cloud service, and there are data leakage risks about personal information. To address this problem, we propose a privacy security protection scheme for facial recognition and resolution based on edge computing. Firstly, a facial recognition and resolution framework based on edge computing is established, which improves the communication and storage efficiency through task partition and relieves the pressure of cloud computing. Then, a verifiable deletion scheme based on Hidden CP-ABE is proposed to provide fine-grained access control and ensure the safe deletion of target data in the cloud. Moreover, after applying the verifiable deletion method, the safe deletion of the target data in the cloud can be achieved. Finally, the simulation results show the effectiveness and security of the proposed scheme.

1. Introduction

Internet of Things (IoT) devices are very common in our daily life, and more and more physical entities are connected to cyberspace. A series of intelligent applications derived from IoT such as smart home, smart medical, and smart grid are profoundly changing social public services and people's daily life [1]. As a key biometric technology to authenticate personal identity, facial recognition and resolution technology can collect any object that needs monitoring and interaction through information sensors. It has been widely used in security fields such as smart card user authentication, criminal investigation, and access control management [2]. Because facial image involves a large amount of private information including identity identifiers, and its recognition and resolution process requires high computing, high storage, and high communication capabilities. This information is usually uploaded to the cloud server in an unencrypted state. Once the cloud server is attacked, privacy leakage is likely to occur [3].

Some researchers have adopted cloud computing to improve computing, storage, and communication capabilities. But limited network bandwidth has become the bottleneck of this centralized processing architecture. As a distributed computing paradigm, edge computing can provide an intermediate layer between the cloud and terminal devices and use the computing power of edge devices to provide efficient services [4]. Compared with the traditional cloud server model, we introduce edge computing technology into the facial recognition and resolution framework, forming a three-tier distributed architecture composed of cloud, edge, and terminal devices. The cloud server offloads some computing tasks to the edge server and performs some operations on it, in order to reduce the interaction with the cloud server. Therefore, we propose a face recognition and resolution framework based on edge computing, which can not only ease the tension between computing-intensive applications and resource-constrained mobile devices, but also reduce the long delay caused by the
interaction between devices and the cloud to improve data processing efficiency [5].

The cloud server provides finite privacy protection under the complex network environment, and the data stored in them is vulnerable to malicious attacks [6]. At present, the shared files on most data storage servers are generally expressed in plain text or simply encrypted. This traditional security mechanism consumes more resources and bandwidth. In CP-ABE encryption, the ciphertext is associated with the access structure, and the key is associated with the attribute set. Only when the decryptor attribute meets the ciphertext-related access policy can the ciphertext be decrypted. However, any user who can obtain the ciphertext can see the content of the access structure, so it may cause information leakage of the decryption party or the encryption party. When data in the cloud is no longer available, the lack of effective deletion will lead to serious problems such as abuse and theft [7]. Physical destruction is obviously the most effective way to delete stored data, but we need to delete it at the file level, and other data can still remain. Therefore, the privacy and security issue of data transmission and data storage in facial recognition and resolution needs to be resolved urgently.

This paper aims to optimize the security and privacy protection scheme of facial recognition and resolution framework and further ensure data security during transmission and storage. We introduce the edge nodes to relieve the bandwidth pressure of transmission and improve the efficiency of calculation. And we apply the Hidden CP-ABE scheme to the data before it is transmitted to the cloud. Furthermore, we adopt a verifiable deletion scheme to ensure the “true deletion” of cloud data.

The main contributions can be summarized as follows:

1. We establish a face recognition and resolution framework based on edge computing, and it can reduce the network bandwidth pressure of the cloud server through completing the recognition and resolution of facial images on the edge server.

2. We propose a verifiable deletion scheme based on the Hidden CP-ABE, which encrypts the data before uploading it to the cloud. According to the requirements of the data owner, a verifiable deletion method is adopted to confirm the deletion of the target data in the cloud, to prevent attackers from accessing the relevant data after “false deletion.” Consequently, the data storage security is ensured in the cloud.

3. Experimental results show that the transmission bits are effectively reduced under this scheme, and the facial recognition and resolution framework can provide more secure and efficient services.

The rest of the paper is organized as follows. Section 2 briefly introduces the relevant work. Section 3 introduces the system model. Section 4 introduces the verifiable deletion scheme of cloud data in facial recognition and resolution. Section 5 carries on the simulation experiment to test the validity of our scheme. Section 6 draws the conclusion.

2. Related Work

The privacy security of facial recognition and resolution is of great significance to ensure the security of the IoT. Researchers at home and abroad have conducted some studies on the architecture and security of the IoT.

Compared with the traditional cloud computing network, the layered distributed computing architecture based on edge computing and cloud computing can solve the problems of data transmission efficiency and network bandwidth more effectively [8]. In order to meet the requirements of high computing power and reduce the corresponding costs, most operators outsource huge amounts of data and computing tasks to cloud servers [9]. However, the cloud server is generally located far away from the position of the service request, which may lead to a longer delay and lower user satisfaction, especially, applications of face recognition that require swift feedback [10]. Therefore, in order to provide highly responsive cloud services. In [11], Shi et al. proposed to sink the computing and storage center to the edge of the Internet near the image acquisition equipment to reduce the communication delay. In [12], Ning et al. proposed a new information retrieval scheme that better reduces the computing burden and network transmission load of the cloud by introducing edge computing technology. In [13], Yu et al. improved the Label Distribution Protocol (LDP) algorithm and the centralized algorithm for global interference location. And they designed a distributed Centralized and Localized Traversal (CLT) algorithm on this basis, which only lost a constant part of the optimal scheduling and significantly reduced the time complexity of the algorithm and transmission delay. In [14], Barbieri et al. proposed an independent health management architecture, which executes efficient and fast algorithms on edge servers and combines them with other algorithms on cloud servers, showing a certain degree of robustness.

All of the above schemes have optimized the delay problem, but the edge computing architecture determines that it faces new security and privacy challenges [15]. Especially in the field of biological information recognition, the problem of information transmission security between edge server and cloud server has not been effectively solved. After many sensors collect our facial data, if the data is sent to the cloud server without encryption, there will be the risk of privacy leakage of eavesdropping or tampering, reducing the reliability of network transmission [16, 17]. Regarding the problems above, researchers put forward many privacy protection methods for biometric recognition.

In [18], Ma et al. proposed a lightweight adaptive enhanced facial recognition framework based on additive secret sharing and edge computing, and designed a series of interactive protocols for privacy protection integrated classification. It not only improves the fault tolerance rate of the system, but also makes it possible to calculate encrypted facial features between the two deployed edge servers. To further ensure security and prevent malicious client attacks, in [19], Im et al. proposed a smart phone face authentication system. The face feature vector is stored on the cloud server in encrypted form, and the Euclidean distance matching.
Facial recognition and resolution framework based on edge computing

3. Network Model and definitions

In this section, we first introduce the facial recognition and resolution framework based on edge computing. Then, we analyze the functions of each module and the specific process of facial recognition and resolution. In addition, we analyze the potential risks in the transmission and stored process based on this framework.

3.1. Facial Recognition and Resolution Framework Based on Edge Computing

Compared with the traditional cloud computing model, in order to reduce the throughput of the transmission channel and the computing load of the cloud, a facial recognition and resolution framework based on edge computing is proposed.

The framework consists of three main parts: client, edge server, and cloud server. The client usually consists of terminal devices such as mobile phones and computers with cameras. The edge server includes two kinds of resolution servers: one is an image parsing server, and the other is an information parsing server. The cloud servers usually consist of a management server and a data center in the cloud. Figure 1 shows the facial recognition and resolution framework. The functions of each functional module are as follows.

**Client:** It is responsible for temporarily storing the original facial images collected by the visual detection equipment, and initiating facial recognition and resolution services to the edge server. After the identity is successfully matched, it returns the resolved identity information to the client.

**Edge Server:** It mainly includes an image resolution server and information resolution server. Resolution is performed closer to the user side without delivering the information to the cloud. The image resolution server is used to resolve the original facial image into the corresponding facial identifier. The information resolution server is used to resolve each piece of personal information registered by the client into a corresponding serial number, bind the facial identifier to each serial number, and then send it to the cloud for identity matching.
Data Center (DC): It is responsible for storing the information from the edge server and performing preliminary matching operations in the existing database.

Management Server (MS): It is responsible for receiving the information from the edge server, and properly scheduling and distributing it to the data center for matching operations during facial resolution.

3.2. Facial Recognition

(1) The client device collects the original facial image and uploads it to the client.

(2) The client receives the original facial image and registers the necessary personal information. It initiates a facial recognition service to the edge server and sends the obtained original facial image and personal information to the edge server after establishing a network connection.

(3) The edge server receives the original facial image and personal information. The image resolution server resolves the original facial image and generates the facial identifier. Generate facial identifiers by performing algorithms such as face detection and preprocessing, feature extraction, and facial identifier generation. At the same time, the personal information is parsed into the corresponding serial number by the information resolution server. The facial identifier and serial number are bound and uploaded to the cloud together.

(4) The management server in the cloud receives the facial identifier and serial number and then stores them in the data center. Finally, the successful registration flag is returned to the edge server, and then, returned to the client.

At this point, the whole facial recognition process is completed. It successfully realized the identity information registration and transform individual faces in physical space into identity identifiers in information space.

Table 1: Symbol definition list of key negotiation process.

| Term       | Description             | Page |
|------------|-------------------------|------|
| $q$        | A prime number          | 6    |
| $g$        | Generator               | 6    |
| $ID_{RS}$, $ID_{MS}$ | The identifier of RS, the identifier of MS | 6 |
| $x_{RS}$, $x_{MS}$ | The private key of RS, The private key of MS | 6 |
| $y_{RS}$, $y_{MS}$ | The public key of RS, The public key of MS | 6 |
| $K_{RS}$, $K_{MS}$ | The secret key of RS, the secret key of MS | 7 |
| $K_{RS,MS}$ | The shared secret key of RS and MS | 7 |
3.3. Facial Resolution

(1) The client device obtains the original facial image of the person being tested, sends a facial resolution request to the edge server, and then sends the original facial image to the edge server.

(2) Similar to the facial recognition process, the image resolution server in edge server generates facial identifier from the received original facial image by performing algorithms such as face detection, preprocessing, feature extraction, and facial identifier generation. Edge server initiates a facial resolution service to the cloud and sends the facial identifier to the cloud after establishing network connection.

(3) The cloud receives the facial identifier. Firstly, the management server in the cloud initially matches the facial identifier with the existing facial identifier in the data center. After the match is successful, the corresponding serial number of the facial identifier is returned to the management server, which in turn is returned to the edge server. The information resolution server in the edge server reversely parses the returned serial number into the corresponding personal information. Finally, the edge server returns the obtained personal information to the client and displays it to the terminal user.

At this point, the whole facial resolution process is completed, realizing the matching of the facial image in the physical space and the personal identity in cyberspace, and ensuring the consistency of the corresponding relationship between them.

3.4. Security Issues. Due to the openness of channels and the sensitivity of data, with the maximization of business purposes, both edge and cloud computing sectors have a strong interest in user information. There are many potential security threats in practical application, so it should be guaranteed from the following three aspects.

(1) Security of data transmission process. The process of facial recognition and resolution involves the transmission from the edge server to the cloud server, which is extremely vulnerable to malicious attacks. Facial information is usually closely associated with sensitive personal information such as health care or financial records. Leakage of facial information will pose a serious threat to users’ privacy. Therefore, the data is authenticated before being uploaded to the cloud and encrypted to ensure security during transmission.

(2) The concealability of attributes in access policy. In the traditional CP-ABE scheme, the access policy is embedded in the ciphertext. It is required that the attributes in the set of attributes owned by the visitor can satisfy the attributes in the access structure, so as to decrypt the data. In fact, regardless of whether the decryption is successful or not, some important information can be deduced according to the existing plaintext access policy. Therefore, in order to eliminate the security risks caused by plaintext transmission of the access policy, the attribute values in the access policy can be encrypted and hidden.

(3) Confirmability of target data deletion in the cloud. Users usually store their data in the cloud. However, the cloud is honest but curious. It may be driven by interest to extract some useful information and leak it to the analysis organization. Users do not want their information to be permanently stored in the cloud. When they want to delete data in the cloud, the cloud may be reluctant to delete or fraudulently delete it for hidden business interests, but users cannot verify whether their data has actually been deleted. Therefore, it is particularly important to delete the target data with assurance and confirmability.

In the process of facial recognition and resolution, the framework offloads some tasks from the cloud to the edge server by applying the task partitioning strategy, rather than performing all the facial resolution processes in the cloud. It makes full use of the powerful computing and parsing capabilities of the edge server, which not only significantly reduces the amount of personal information transmission, but also reduces the computing pressure of cloud. However, how to ensure the data security of transmission, access, and stored procedures needs to be solved urgently. Thus, we propose a cloud data verifiable deletion scheme in response to the above security issues to ensure the security of the scheme.

4. Verifiable Deletion Scheme of Cloud Data in Facial Recognition and Resolution

In this section, we first optimize the MTI session key agreement scheme, which ensures the correctness of channel transmission by confirming the identity between the sender server and the receiver server. In addition, based on the analysis of the security and privacy issues of the framework, we introduce the verifiable deletion scheme of cloud data in detail.

4.1. Optimized MTI Session Key Agreement Scheme. To ensure the security of the channel during transmission, the identity between the resolution server and the management server needs to be verified. Firstly, we optimize the MTI session key agreement scheme, which has the ability to resist replay attacks and parallel sessions. The symbol is shown in Table 1.

The system first exposes $q$ and $g$ to RS and MS. RS has a unique $ID_{RS}$, $x_{RS}$, $y_{RS} = g^{x_{RS}} \mod q$, authorization $C_{RS} = (ID_{RS}, y_{RS}, y_{TA}, (ID_{RS}, y_{RS}))$ certificate

$$C_{RS} = (ID_{RS}, y_{RS}, y_{TA}, (ID_{RS}, y_{RS})),$$

which binds public key and identity.

Similarly, MS has a unique $ID_{MS}$, $x_{MS}$, $y_{MS} = g^{x_{MS}} \mod q$, authorization certificate

- $ID_{MS}$, $x_{MS}$, $y_{MS}$, $y_{TA}, (ID_{MS}, y_{RS})$
\[ C_{MS} = (ID_{MS}, y_{MS}, \text{Sig}_{TA}(ID_{MS}, y_{MS})) \]

which binds public key and identity. RS randomly selects \( r_{RS} \in [0, q - 1] \), then calculates
\[ s_{RS} = g^{r_{RS}} \mod q, \]
and sends \( \{S_{RS}, ID_{MS}, C_{RS}\} K_{MS} \) to MS. MS randomly selects \( r_{MS} \in [0, q - 1] \) and then calculates
\[ s_{MS} = g^{r_{MS}} \mod q, \]
\[ K_{RS,MS} = s_{MS}^{r_{RS}} \mod q, \]
The system gets \( K_{RS,MS} \) which is the session key for further communication between RS and MS. Then, it sends \( \{S_{MS}, ID_{RS}, C_{MS}\} K_{RS} \) to RS. RS gets
\[ K_{RS,MS} = s_{MS}^{r_{RS}} \mod q, \]
by calculation and sends \( \{S_{RS,MS}, ID_{MS}, C_{RS}\} K_{MS} \) to MS. MS judges whether \( K_{RS,MS} \) is consistent with \( K_{RS,MS} \) or not. If \( K_{RS,MS} \neq K_{RS,MS} \), it indicates that the negotiation is successful, and RS and MS have completed authentication between each other. If \( K_{RS,MS} \neq K_{RS,MS} \), the negotiation fails.

In this algorithm, the shared key can be derived from the \((q, s_{MS})\) or \((g, s_{RS})\), but not from \((s_{MS}, s_{RS})\). In other words, although the attacker can eavesdrop on \( q, g, s_{RS}, s_{MS} \) and even ciphertext, it cannot export the correct session key \( K_{RS,MS} \) due to the unknown values of \( r_{RS} \) and \( r_{MS} \). Therefore, it cannot crack the ciphertext.

The algorithm adds a fresh factor every time the message is sent and binds the source and destination of the message, which can effectively prevent replay attacks. Because the session keys \( (s_{RS}, s_{MS}) \) are randomly selected, attackers can only destroy the formation of the key but has no way to launch a parallel session attack against it. The optimized MTI session key agreement scheme defines the authorization certificate and increases the authentication process, which improves the security of the scheme.

4.2. Encryption Scheme in Facial Recognition. Firstly, there are two communication channels that are absolutely safe. One is the channel among the trusted authority (TA), RS, and MS, and the other is the channel between the client and RS. Secondly, MS uses read-only access to decrypt files and will not tamper with relevant data. Furthermore, the communication channel between RS and MS is not secure, and the cloud storage center is also semi-honest.

When the user collects the facial image, the edge server generates facial data through facial detection, facial image preprocessing, feature extraction, and facial identifier generation algorithms. MTI session key agreement scheme and SHA-1 hash algorithm are used to ensure the security and integrity of data transmission, and CP-ABE algorithm is used to encrypt personal data and fine control access as shown in Figure 2. The symbol definition and description list of facial recognition and resolution are in Table 2.

The encryption scheme in facial recognition is as follows:

4.3. Verifiable Deletion Scheme of Cloud Data in Face Resolution. In the process of facial resolution, the client first collects the facial image of the person being tested, and the edge server resolves it into a facial identifier and uploads it to the cloud. The cloud server first uses the decryption algorithm to decrypt the ciphertext file and then matches the decrypted facial identifier with the facial identifier uploaded in the data center. The serial number of personal information bound with the facial identifier is returned to the edge server to match with each other. The verifiable deletion scheme in face resolution is as follows:

When the user completes the facial resolution, some information in the cloud is no longer available. If user needs to delete it, the verifiable deletion scheme can be used to cancel the user’s access to facial data. Our scheme is to add a verifiable process after the user deletes the data to ensure the deletion succeeds completely, and also to avoid false deletion of the cloud. This enables users to better control their own data, and the security of data in the cloud is effectively ensured as shown in Figure 3.

5. 5. Experimental Simulation Results Analysis

5.1. Security Analysis. This part mainly analyzes the security of data transmission in the process of facial recognition and resolution, the concealability of access policy attributes, and the confirmability of cloud data deletion.

(1) In our security scheme, we adopt the MTI session key agreement scheme. In the process of session key agreement, the public keys of RS and MS are allocated to be shown in public. They perform bidirectional authentication to confirm each other’s identity and ensure antireplay attack by adding fresh factors and randomly selecting keys each time they send messages. At the same time, we use the SHA-1 algorithm. All the facial identifiers \((K_{RS,MS}, CT||\text{sig}_{sk,R}||\text{Hash}(CT)||\text{sig}_{sk,R})\) stored in the data center are extracted and decrypted; we calculate \(\text{Hash}(CT||\text{sig}_{sk,R})\) and \(\text{Hash}(CT||\text{sig}_{sk,R})\) to ensure the integrity of the data access process and effectively prevent malicious tampering by illegal users.

(2) The scheme first generates the symmetric key \(DK\) through AES symmetric key algorithm and construct the access policy by the CP-ABE algorithm. Then, it uses \(DK\) to encrypt the data, which is further encrypted to the ciphertext \(CT\) associated with the access policy \(A\). Based on this, the plaintext attribute values in the access policy are successfully partially hidden. Visitors must make their own attributes meet the access policy attributes in order to achieve the access and decryption of the data.

(3) In the cloud storage environment, when the data owner wants to delete the outsourced data, in order to avoid logical deletion, the attribute access control policy
corresponding to the ciphertext is changed by reen-crypting the ciphertext to achieve fine-grained operation and deterministic permanent deletion. In the proposed scheme, we use CP-ABE algorithm to generate the reencryption key and then use it to encrypt the ciphertext $CT$ to generate new ciphertext and MHT tree roots. RS compares the new and old tree root. And if the two are equal, it indicates that the target data has indeed been completely deleted in the cloud.

5.2. Setup of Experiment. In this part, we add the facial recognition and resolution security privacy protection scheme based on edge computing to the prototype system and then verify the security and effectiveness of the scheme through a large number of simulation experiments. Because

the facial recognition process is similar to the facial resolution process, we only test the effectiveness of verifiable deletion schemes in facial resolution.

This experiment uses one cloud server, two edge servers, and six mobile terminal devices to build the system as shown in Figure 1. All the algorithms are tested on a Win10-64-bit laptop using Intel®-6700HQ processor at 2.60 GHz. We use the following three face databases: Caltech face image database, GT face image database, and BioID face image database. These three databases are, respectively, composed of 450 color face images of 27 characters, 750 face avatars of 50 characters, and 1521 gray-scale face images of 23 characters. We firstly pre-process the original database and randomly select 50 sheets from them. Then, the preprocessed data is used as the database for our experiment.
In order to evaluate the impact of the communication overhead of the scheme in practical application, we mainly measure the network transmission from the edge server to the cloud server. Compared with the traditional scheme, this scheme can reduce the amount of data transmission. In this experiment, three face databases are tested. Figure 4 shows an increase of only 0.132 kb relative to the prototype framework system and a decrease of 0.044 kb relative to the original security framework system. The experimental results show that the experimental communication overhead is relatively small, which can meet the needs of practical applications and have good stability.

5.3.2. Response Time of Facial Database. We include the time of issuing the request, generating the facial identifier, network transmission, data encryption and decryption, identifier matching, and verifiable deletion of the target data in the cloud. Compared with security scheme, our scheme increases the computing time of data encryption and decryption and data verifiable deletion. Through comparing it with the experiment without face database, Figure 5 shows that the average consumption of this scheme increases by 84 ms milliseconds compared to the system without security framework and only increases by 14 ms compared to the system with security framework. But we can safely manage data in the cloud, which shows that our experiments can satisfy the practical application to a certain extent.
Figure 3: Verifiable deletion process of cloud data in face resolution.

Figure 4: Amount of network transmission for different face databases.
The framework with security scheme
The designed scheme in this paper
The framework without security scheme

**Figure 5:** Average response time for different face databases.

The framework with security scheme
The designed scheme in this paper
The framework without security scheme

**Figure 6:** Average response time for different size of face databases.
5.3.3. Response Time of Face Databases of Different Sizes. In order to better reflect the performance of the experiment, we use BioID face database to test the response time of the system. By selecting the face database test in the range of 400–1600, Figure 6 shows that the scheme grows steadily with the increase of face database size, without great instability. The time consumption of this scheme increases by 64 ms compared to the system without security framework and increases by 12 ms compared to the system with security framework. This shows that our scheme has good advantages in stability.

6. Conclusion

In this paper, we focused on the privacy security of facial recognition and resolution framework based on edge computing. In summary, we analyzed the security threats of facial recognition and resolution framework, including the security of data transmission, the concealability of access policy attributes, and the verifiability of cloud data deletion. To solve these problems, we improved the framework by combining the characteristics of cloud computing and edge computing. To further ensure the security of cloud data transmission and storage, we proposed a verifiable deletion scheme based on Hidden CP-ABE, which can effectively prevent attackers from stealing sensitive information and deleting data falsely. Then, we applied this scheme to the facial recognition and resolution framework based on edge computing and evaluated its performance by simulation experiments. The results indicated that the proposed scheme performs good stability and can effectively meet the requirements of facial recognition and resolution in practical application. In future work, we will further verify this scheme through experiments in more dimensions. Moreover, on the premise of ensuring the efficiency of facial recognition and resolution, the performance of low energy consumption and low latency performance will be optimized at a higher level.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Ramesh and M. Govindarasu, “An efficient framework for privacy-preserving computations on encrypted IoT data,” IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8700–8708, 2020.

[2] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, “Pspr: a source location privacy protection scheme based on sector phantom routing in wsns,” International Journal of Intelligent Systems, vol. 37, no. 2, pp. 1204–1221, 2022.

[3] T. Li, Y. Chen, Y. Wang et al., “Rational protocols and attacks in blockchain system,” Security and Communication Networks, vol. 2020, pp. 1–11, 2020.

[4] A. Naouri, H. Wu, N. A. Nouri, S. Dhelim, and H. Ning, “A novel framework for mobile-edge computing by optimizing task offloading,” IEEE Internet of Things Journal, vol. 8, no. 16, pp. 13065–13076, 2021.

[5] G. Li, J. Cao, J. Wu, X. Ren, and H. Yu, “Dimension reduction algorithm based on adaptive maximum linear neighborhood selection in edge computing,” IEEE Internet of Things Journal, vol. 11, no. 19, pp. 4237–4662, 2020.

[6] X. Xu, R. Mo, X. Yin et al., “P. D. M.: Privacy-aware deployment of machine-learning applications for industrial cyber-physical cloud systems,” IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5819–5828, 2020.

[7] Y. Shin, D. Koo, J. Yun, and J. Hur, “Decentralized server-aided encryption for secure deduplication in cloud storage,” IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1021–1033, 2020.

[8] K. Gai, K. Xu, Z. Lu, M. Qiu, and L. Zhu, “Fusion of cognitive wireless networks and edge computing,” IEEE Wireless Communications, vol. 26, no. 3, pp. 69–75, 2019.

[9] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, “Privacy-preserving outsourced classification in cloud computing,” Cluster Computing, vol. 21, no. 1, pp. 277–286, 2018.

[10] G. Li, Y. Liu, J. Wu, D. Lin, and S. Zhao, “Methods of resource scheduling based on optimized fuzzy clustering in fog computing,” Sensors, vol. 19, no. 9, pp. 21–22, 2019.

[11] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: vision and challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

[12] H. Ning, X. Liu, X. Ye, J. He, W. Zhang, and M. Daneshmand, “Edge computing-based ID and nID combined identification and resolution scheme in IoT,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 681–6821, 2019.

[13] K. Yu, J. Yu, X. Cheng, D. Yu, and A. Dong, “Efficient link scheduling solutions for the Internet of Things under Rayleigh fading,” IEEE/ACM Transactions on Networking, vol. 29, no. 6, pp. 2508–2521, 2021.

[14] M. Barbieri, K. T. P. Nguyen, R. Diversi, K. Medjaher, and A. Tili, “RUL prediction for automatic machines: a mixed edge-cloud solution based on model-of-signals and particle filtering techniques,” Journal of Intelligent Manufacturing, vol. 32, no. 5, pp. 1421–1440, 2021.

[15] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, “Semi-selfish mining based on hidden Markov decision process,” International Journal of Intelligent Systems, vol. 36, no. 7, pp. 3596–3612, 2021.

[16] X. Zhao, J. Wu, M. Wang, G. Li, H. Yu, and W. Feng, “Multi-sensor data fusion algorithm based on adaptive trust estimation and neural network,” in Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC), pp. 582–587, Chongqing, China, August 2020.

[17] K. Yu, B. Yan, J. Yu, H. Chen, and A. Dong, “Methods of improving secrecy transmission capacity in wireless random networks,” Ad Hoc Networks, vol. 117, Article ID 102492, 2021.

[18] Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, “Lightweight privacy-preserving ensemble classification for face recognition,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5778–5790, 2019.

[19] J.-H. Im, S.-Y. Jeon, and M.-K. Lee, “Practical privacy-preserving face authentication for smartphones secure against malicious clients,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2386–2401, 2020.
[20] Y. Chen, S. Dong, T. Li, Y. Wang, and H. Zhou, “Dynamic multi-key fhe in asymmetric key setting from lwe,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5239–5249, 2021.

[21] S. Qi, Y. Lu, W. Wei, and X. Chen, “Efficient data access control with fine-grained data protection in cloud-assisted IoT,” *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2886–2899, 2020.

[22] Y. Zhang, J. Li, and H. Yan, “Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure,” *IEEE Access*, vol. 7, pp. 47982–47990, 2019.

[23] H. Tian, X. Li, H. Quan, C.-C. Chang, and T. Baker, “A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection,” *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15793–15806, 2020.

[24] Y. Yu, L. Guo, S. Liu, J. Zheng, and H. Wang, “Privacy protection scheme based on CP-ABE in crowdsourcing-IoT for smart ocean,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10061–10071, 2020.

[25] C. Ge, Z. Liu, J. Xia, and L. Fang, “Revocable identity-based broadcast proxy re-encryption for data sharing in clouds,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1214–1226, 2021.

[26] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, “Is semi-selfish mining available without being detected?” *International Journal of Intelligent Systems*, 2021.

[27] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, “Cloud-based fine-grained health information access control framework with dynamic auditing and attribute revocation,” *IEEE transactions on cloud computing*, vol. 6, no. 2, pp. 532–544, 2015.

[28] M. Miao, J. Wang, J. Ma, and W. Susilo, “Willy. Publicly verifiable databases with efficient insertion/deletion operations,” *Journal of Computer and System Sciences*, vol. 86, pp. 49–58, 2017.

[29] H. Ma, R. Zhang, S. Sun, Z. Song, and G. Tan, “Server-aided fine-grained access control mechanism with robust revocation in cloud computing,” *IEEE Transactions on Services Computing*, p. 1, 2019.

[30] K. Edemacu, B. Jang, and J. W. Kim, “Collaborative eHealth privacy and security: an access control with attribute revocation based on OBDD access structure,” *IEEE journal of biomedical and health informatics*, vol. 24, no. 10, pp. 2960–2972, 2020.

[31] G. Yu, X. Zha, X. Wang et al., “Enabling attribute revocation for fine-grained access control in blockchain-IoT systems,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1213–1230, 2020.