Multi Authority Attributes Based Keyword Searchable Scheme In Medical Cloud Data

Abisha P.K[1], M.Manchu[2]
[1, 2] Dept of CSE
[1, 2] Ponjesly College of Engineering

Abstract- *In cloud-based electronic medical record (EMR) systems, attribute-based encryption (ABE) has been utilized to protect the confidentiality of EMRs and provide keyword search over the encrypted EMRs. However, existing schemes are designed for a single attribute authority, and lack sufficient user privacy protection. In this article, we introduce TABKS, a privacy-preserving traceable attributebased keyword search scheme in multi-authority medical cloud. First, we propose an anonymous EMR access control framework with multiple authorities, which provides user anonymity against the untrusted authorities. Second, we achieve traceable attribute-based Boolean keyword search, which enables the authorized user who satisfies the policy to conduct Boolean keyword search over the encrypted EMRs. In this process, TABKS improves the efficiency of legitimate users by partially decrypting the matched results, and also achieves efficient traitor trace by revealing the user identity from the trapdoor. Finally, we prove the security of TABKS against chosen plaintext attack and chosen keyword attack, and conduct extensive experiments with two real-world datasets to show the feasibility of TABKS.*

Keywords- Medical cloud, attribute-based encryption, keyword search, privacy preservation, traitor trace

I. INTRODUCTION

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud.

Data sharing is the important service in the cloud. In data sharing service user share the data with group of user. User does not have physical control when the data is in cloud. Any mistake can cause loss of data. To check integrity of data some scheme is used, when user cheat or leaves the group, the user should be revoked from group. Therefore user revocation is important in cloud storage. The cloud data owner uses his private key to generate signature for file blocks. When user is removed the user private key should also be removed .In previous scheme all signatures generated should get transfer to non-revoked user. In such case the nonrevoked user download all revoked user block resign and upload new one. This cause lots of computation of resources. Once user is removed from group, there is lots of burden of user revocation for large cloud. The situation will be more difficult when membership changes frequently.

With the development of Internet technology, the traditional paper medical record has been superseded by electronic medical record (EMR). The United States National Institutes of Health (NIH) first proposed the definition of EMR, which is an electronic document that details all the relevant clinical reports of a person over a period. Nowadays, EMRs play as a bridge between patients and healthcare providers, including doctors, medical researchers, and health insurances, etc. The layout speed of cloud computing in the medical industry has obviously accelerated, and the medical cloud has entered a stage of rapid development.

The emergence of cloud-based EMR systems has not only brought a large convenience to patients and healthcare providers, but also has promoted the development of health careers. Similarly, the popularity of mobile devices has also driven the wide application of the EMR system. For example, the doctors in the hospital can access the EMRs through mobile devices, and the researcher can develop more effective drugs and treatments with the help of the patients' EMRs.

The EMR contains not only the user's physical data, but also personal privacy information, such as phone number, home address, certificate of medical insurance and medication history. Once these EMRs are revealed by hackers, the patients' privacy will be threatened. Due to the centralized storage of EMRs in cloud computing, the confidentiality of data has been greatly threatened. Specifically, the cloud service providers, which will respond the user's request correctly, but also will collect the information of EMRs, and even sell them for profit. Currently, many countries have raised the security protection of EMRs to the legal level. For example, General Data Protection Regulations (GDPR) enacted by the European Union has addressed the privacy and security concerns associated with the health information.

Throughout the development of EMR systems in cloud computing, secure EMRs sharing is the key to the sustainable development of the entire system.

The EMR should be encrypted and uploaded to the cloud, and then shared with specific users. Fortunately, attribute-based encryption (ABE) is introduced as a fine-grained access control technique for EMR systems in cloud computing. Specially, in ciphertext-policy ABE (CP-ABE), the user is described with a set of attributes, and if the user's attributes match the access policy structured by the access tree, AND gate or linear secret sharing scheme (LSSS), the ciphertext can be decrypted correctly. Although CP-ABE can protect EMR confidentiality and guarantee fine-grained access control, there are still many privacy and availability challenges for practical medical cloud.

In a traditional EMR system in cloud computing, the EMR cloud can assist the system to realize data sharing between different entities, as shown in Fig. 1.3. In fact, each EMR in the cloud will be accessed by multiple healthcare provider. These healthcare providers can apply EMRs to manage the health of patients. For example, the doctor can access the patient diagnostic information and illness descriptions through these EMRs, the researcher can find better solutions to a specific patient's stubborn disease based on EMRs, and the insurance company mainly checks the authenticity of the patient's condition. Thus, the secret keys of these users should be issued by these authorities accordingly.

In a multi-authority ABE, each attribute authority (AA) will honestly issue the secret keys according to the users' attributes and will not collude with malicious parties, which is more suitable for EMR systems. Moreover, an AA may assign multiple values to the same attribute in EMR systems. For example, some doctors may have multiple specialties, such as internal medicine and dermatology, internal medicine and psychiatry. Then, these doctors can have multiple values from the AA for the professional attribute "specialty". However, the untrusted AA can impersonate the user or leak the user's identity if it knows her/his attributes. In addition, the EMRs can also be threatened by the leakage of user's credential. For example, the hospital may suffer phishing attacks, and the hacker may steal the account of employees and use them to search and download the EMRs of patients. Therefore, it is urgent to locate the attacked users.

The security problems caused by the untrusted authorities in cloud computing and the malicious users in EMR sharing into account, and introduce TABKS, a privacy-preserving traceable attribute-based keyword search scheme over the encrypted medical records in multi-authority medical cloud.

II. LITERATURE SURVEY

Cloud storage and edge computing are utilized to address the storage and computational challenges arising from the exponential data growth in IoT. However, data privacy is potentially risky when data is outsourced to cloud servers or edge services. While data encryption ensures data confidentiality, it can impede data sharing and retrieval. Attribute-based searchable encryption (ABSE) is proposed as an effective technique for enhancing data security and privacy. Nevertheless, ABSE has its limitations, such as single attribute authorization failure, privacy leakage during the search process, and high decryption overhead. This paper presents a novel approach called the blockchain-assisted efficient multi-authority attribute-based searchable encryption scheme (BEM-ABSE) for cloudedge collaboration scenarios to address these issues. BEM-ABSE leverages a consortium blockchain to replace the central authentication center for global public parameter management. It incorporates smart contracts to facilitate reliable and fair ciphertext keyword search and decryption result verification. To minimize the computing burden on resource-constrained devices, BEM-ABSE adopts an online/offline hybrid mechanism during the encryption process and a verifiable edge-assisted decryption mechanism. This ensures both low computation cost and reliable ciphertext. Security analysis conducted under the random oracle model demonstrates that BEM-ABSE is resistant to indistinguishable chosen keyword attacks (IND-CKA) and indistinguishable chosen plaintext attacks (INDCPA). Theoretical analysis and simulation results confirm that BEM-ABSE significantly improves computational efficiency compared to existing solutions.

Ciphertext attribute-based encryption is a proven mechanism for providing the privacy and security for the shared resources in the cloud. However, the issues that are concerned with the sharing mechanisms such as master key and access policies were exploited by the malicious users. Moreover, the access control mechanisms are developed by using the large universe of attributes of the shared resource in the cloud. More number of attributes results into increase in computation time while computing the master and secret keys as well as for encryption and decryption processes. The observations over the participating attributes play vital role to prepare a machine learning model in terms of better accountability. In this paper we have proposed specifc attribute-based encryption to provide the better security and better cloud access control mechanism. Inclusion of dynamic attributes while performing the encryption at data owner, cloud server would serve a better performance to avoid key

exposure. This performance is elevated while generating the secret key at the proxy server. The performance has been found to be satisfactorily encouraging by reducing the computation time to almost half of the existing schemes and the observations are in accordance to the required accountability.

Cloud storage has been deployed in various real-world applications. But how to enable Internet users to search over encrypted data and to enable data owners to perform finegrained search authorization are of huge challenge. Attributebased keyword search (ABKS) is a well-studied solution to the challenge, but there are some drawbacks that prevent its practical adoption in cloud storage context. First, the access policy in the index and the attribute set in the trapdoor are both in plaintext, they are likely to reveal the privacy of data owners and users. Second, the current ABKS schemes cannot provide multi-keyword search under the premise of ensuring security and efficiency. We explore an efficient way to connect the inner product encryption with the access control mechanism and search process in ABKS, and propose a privacy-protecting attributebased conjunctive keyword search scheme. The proposed scheme provides conjunctive keyword search and ensures that the access policy and attribute set are both fully hidden. Formal security models are defined and the scheme is proved IND-CKA, IND-OKGA, access policy hiding and attribute set hiding. Finally, empirical simulations are carried out on real-world dataset, and the results demonstrate that our design outperforms other existing schemes in security and efficiency.

Public key searchable encryption (PKSE) scheme allows data users to search over encrypted data. To identify illegal users, many traceable PKSE schemes have been proposed. However, existing schemes cannot trace the keywords which illegal users searched and protect users' privacy simultaneously. In some practical applications, tracing both illegal users' identities and the keywords which they searched is quite important to against the abuse of data. It is a challenge to bind users' identities and keywords while protecting their privacy. Moreover, existing traceable PKSE schemes do not consider the unforgeability and immutability of trapdoor query records, which can lead to the occurrence of frame-up and denying. In this paper, to solve these problems, we propose a blockchain-based privacypreserving PKSE with strong traceability (BP3KSEST) scheme. Our scheme provides the following features: (1) authorized users can authenticate to trapdoor generation center and obtain trapdoors without releasing their identities and keywords; (2) when data users misbehave in the system, the trusted third party (TTP) can trace both their identities and the keywords which they searched; (3) trapdoor query records are unforgeable; (4) trapdoor query records are immutable because records are stored in blockchain. Notably, this scheme is suitable to the scenarios where privacy must be considered, e.g., electronic health record (EHR). We formalize both the definition and security model of our BP3KSEST scheme, and present a concrete construction. Furthermore, the security of the proposed scheme is formally proven. Finally, the implementation and evaluation are conducted to analyze its efficiency.

Attribute-based encryption enables users to flexibly exchange and share files with others. In these schemes, users utilize their own attributes to acquire public-private key pairs from the key generation center. However, achieving this for users who wish to keep their attributes private poses a challenge. To address this contradiction, we propose an original scheme that combines ciphertext policy attribute-based encryption with a k-out-of-n oblivious transfer protocol. This scheme allows the distribution of corresponding public-private key pairs to users without the key generation center needing to obtain specific user attributes. Furthermore, it ensures the privacy of the key generation center. Security analysis demonstrates that the scheme is secure in the random oracle model. Our performance comparison and experimental results indicate that the scheme is both flexible and efficient.

III. PROPOSED SYSTEM

In a typical EMR system, users from different healthcare providers are authorized to access the EMR. In order to protect EMR privacy in cloud computing. In this model, the key generation center (KGC) is in charge of initializing the system and maintaining the AAs. Meanwhile, each AA manages a group of attributes from the universe. The KGC and AAs generate the secret keys of users collaboratively, in which the AAs grant access privileges by distributing the secret keys related to the users' attribute values using the k-out-of n obvious transfer protocol, while the KGC only knows their identities. The EMR cloud has abundant storage capacity and stores encrypted EMRs with access policies from data owners.

The data owner such as the information management department of the hospital which manages the specified patients' EMRs and outsources them to the EMR cloud by enforcing access policies and defining keywords.

The user such as a doctor or a medical researcher possessing a set of attribute values and the corresponding secret key from the AAs can search the encrypted EMRs in the cloud. If an encrypted EMR's keywords match the user's search condition and the user's attributes satisfy the access

policy of this EMR, the user can successfully get the search result and decrypt this EMR efficiently.

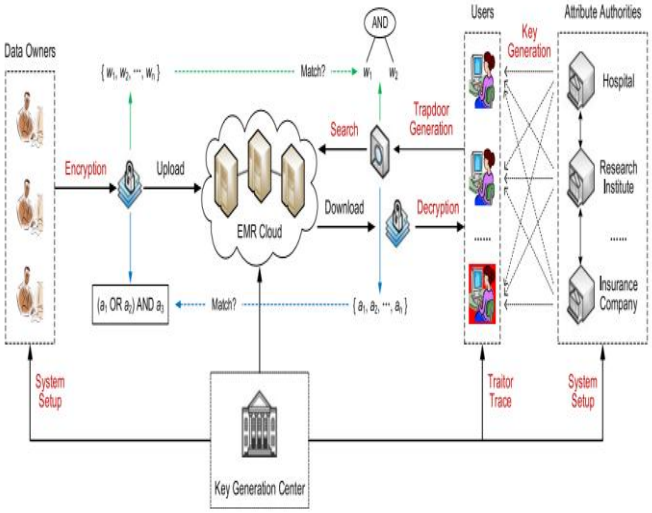

Fig 1: System Architecture

In a typical EMR system, users from different healthcare providers are authorized to access the EMR. In order to protect EMR privacy in cloud computing, introduce the system model of TABKS in Fig 4.1 . In this model, the key generation center (KGC) is in charge of initializing the system and maintaining the AAs. Meanwhile, each AA manages a group of attributes from the universe. The KGC and AAs generate the secret keys of users collaboratively, in which the AAs grant access privileges by distributing the secret keys related to the users' attribute values using the k-out-ofn obvious transfer protocol, while the KGC only knows their identities. The EMR cloud has abundant storage capacity and stores encrypted EMRs with access policies from data owners.

The data owner such as the information management department of the hospital which manages the specified patients' EMRs and outsources them to the EMR cloud by enforcing access policies and defining keywords. The user such as a doctor or a medical researcher possessing a set of attribute values and the corresponding secret key from the AAs can search the encrypted EMRs in the cloud. If an encrypted EMR's keywords match the user's search condition and the user's attributes satisfy the access policy of this EMR, the user can successfully get the search result and decrypt this EMR efficiently.

MODULES

- Key Generation and Trapdoor Generation
- Data Encryption and Decryption
- Search and Decryption Delegation
- Traitor Trace

Description

Key Generation and Trapdoor Generation

The KGC and AAs run KeyGen algorithm to generate the secret key for a user with identity uid and a set of attributes $S = (L, \varepsilon)$, where L denotes the attribute names, ε denotes the attribute values.

The user defines the keyword expression as a LSSS structure $Q = (K, \pi)$, in which K is an $l \times \tau$ matrix, and generates the trapdoor with the secret key by the TrapGen algorithm.

Data Encryption and Decryption

The data owner selects a random DK to encrypt the EMR M symmetrically, and runs Encrypt algorithm to encrypt DK.

Finally, using the Decrypt algorithm, the user first calculates $F = \frac{e[C_1^D C_2 D_0)}{(F_1)^{\frac{1}{\tau}}} = e(g,g) \sum f_k s_1$ with the retrieve key, and then outputs $DK = C_0/F$. Then, he can further get the searched EMR M with DK.

Search and Decryption Delegation

The EMR cloud will conduct search over the encrypted EMRs with the keyword expression. For an encrypted EMR ct, the cloud tries to evaluate whether its keywords match the expression Q and whether the user's attributes satisfy the access policy T. Then, the EMR cloud searches the result by the Search algorithm.

Traitor Trace

If a sold secret key is used to search the ciphertext, the traitor can be traced by Trace algorithm. In TABKS, the keywords information and attributes information must be matched before the final decryption. Therefore, different from existing schemes which trace the traitor directly from the secret key sk, use the trapdoor tk.

ALGORITHM DESCRIPTION

AES Encryption

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other

operations, on an array of data that holds exactly one block of data the data to be encrypted. This array call the state array.

- Take the following AES steps of encryption for a 128-bit block:
- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- SubBytes
- ShiftRows
- MixColumns
- XorRoundKey

The details of these operations are described shortly, but first need to look in more detail at the generation of the Round Keys, so called because there is a different one for each round in the process.

The order of operation in decryption is:

Perform initial decryption round:

- XorRoundKey
- InvShiftRows
- InvSubBytes
- Perform nine full decryption rounds:
- XorRoundKey
- InvMixColumns
- InvShiftRows
- InvSubBytes
- Perform final XorRoundKey

The same round keys are used in the same order.

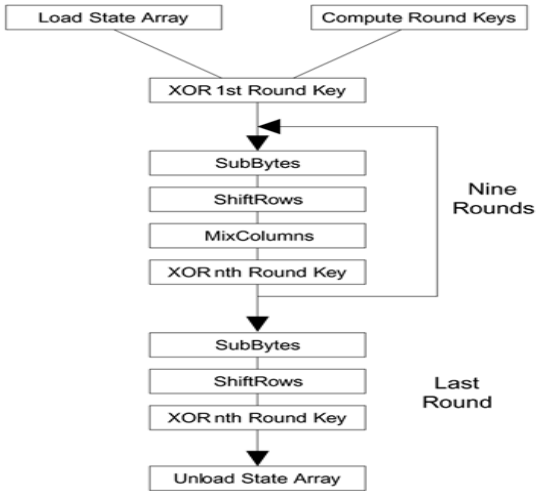

Fig 2: AES Encryption

SHA-256

An n-bit hash is a map from arbitrary length messages to n-bit hash values. An n- bit cryptographic hash is an n-bit hash which is one-way1 and collision-resistant.2 such functions is important cryptographic primitives used for such things as digital signatures and password protection. Current popular hashes produce hash values of length n = 128 (MD4 and MD5) and n = 160 (SHA-1), and therefore can provide no more than 64 or 80 bits of security, respectively, against collision attacks. Since the goal of the new Advanced Encryption Standard (AES) is to offer, at its three crypto variable sizes, 128, 192, and 256 bits of security, there is a need for companion hash algorithms which provide similar levels of enhanced security. SHA-256 operates in the manner of MD4, MD5, and SHA-1: The message to be hashed is first. The SHA-256 compression function operates on a 512-bit message block and a 256- bit intermediate hash value. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key.

IV. SCREEN SHOTS

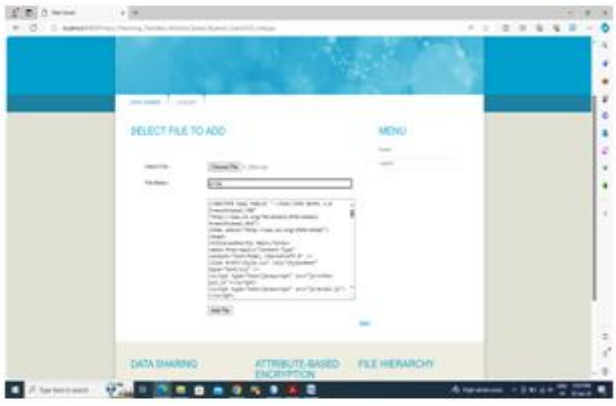

Fig 3. Upload File

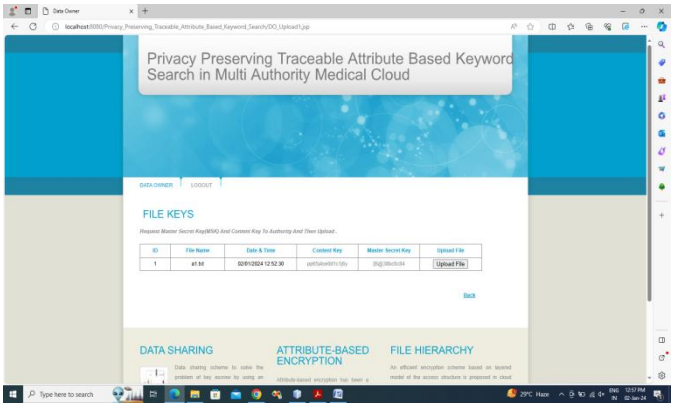

Fig 4.File Keys

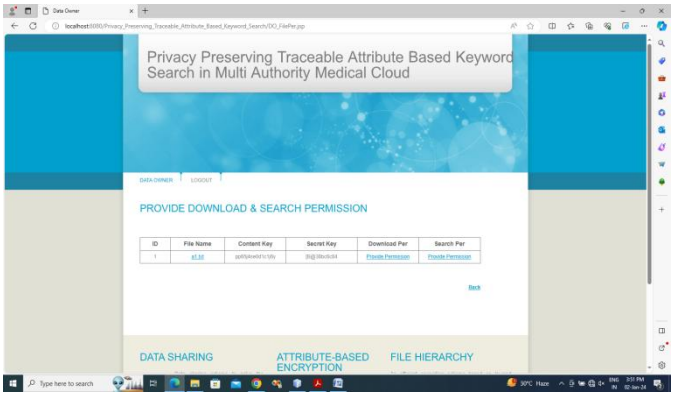

Fig 5. Provide Permission

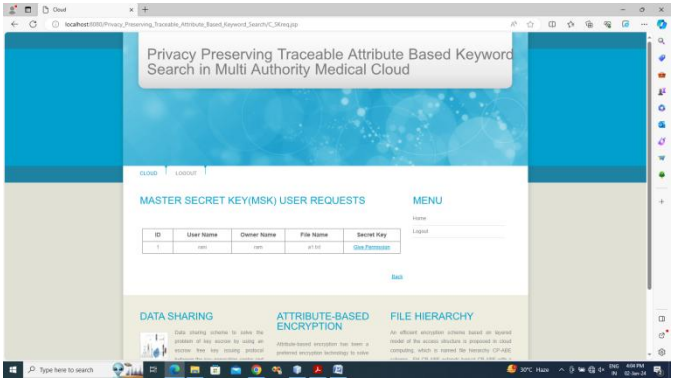

Fig 6. Master Key User Response

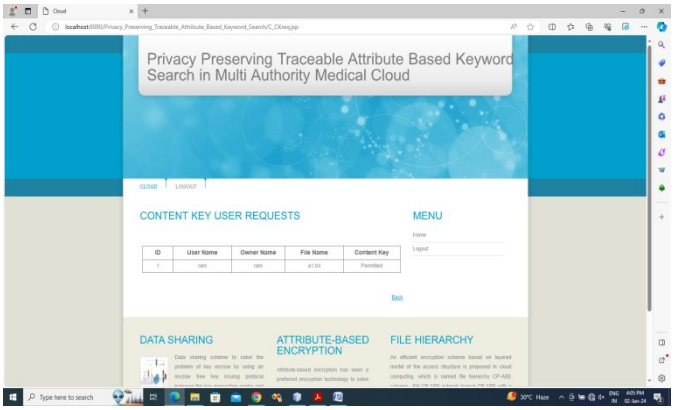

Fig 6. Content Key User Response

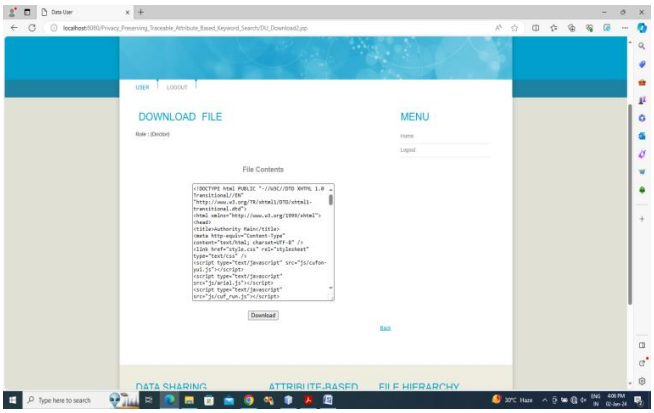

Fig 7. Download File

V. CONCLUSION

In this work introduce TABKS, a privacy-preserving traceable attribute-based keyword search scheme over encrypted EMRs in cloud computing. First, propose an anonymous and fine-grained EMR access control framework with multiple authorities, which protects the EMR confidentiality, and also provides user anonymity against the untrusted authorities. Then allow the users to define Boolean search conditions over the encrypted EMRs in the cloud. Hence, a certain EMR can be searched by an authorized user only if she/he satisfies the access policy and the keyword expression is matched. Further present that TABKS can also trace the traitor by revealing the user identity from the trapdoor. Finally, prove the CPA and CKA security of TABKS and conduct extensive experiments to show that TABKS is efficient and practical for privacy-preserving EMR sharing scenarios.

REFERENCES

[1] Peng Liu, Qian He1, Baokang Zhao, Biao Guo, "Efficient Multi-Authority Attribute-Based Searchable Encryption Scheme with Blockchain Assistance for Cloud-Edge Coordination," CMC, 2023, vol.76, no.3.

[2] P. Prathap Nayudu, Krovi Raja Sekhar, "Accountable specifc attribute-based encryption scheme for cloud access control," Spring 9 july 2022.

[3] Yang Chen, Yang Liu, Jin Pan, Fei Gao, "Privacy-Protecting Attribute-Based Conjunctive Keyword Search Scheme in Cloud Storage," Journal of Internet Technology Vol. 24 No. 1, January 2023.

[4] Yue Hana, Jinguang Hana, Weizhi Meng, "Blockchain-based Privacy-Preserving Public Key Searchable Encryption with Strong Traceability," in arXiv:2312.16954v1 [cs.CR] 28 Dec 2023.

[5] Hao Zhang, Yue Zhao, Jintao Meng, Attribute-Based Encryption Scheme with k-Out-of-n Oblivious Transfer Electronics 2023, 12, 4502.
[6] Han, D.; Pan, N.; Li, K.C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection. IEEE Trans. Dependable Secur. Comput. 2020, 19, 316–327.
[7] Cui, H.; Deng, R.H.; Qin, B.; Weng, J. Key regeneration-free ciphertext-policy attribute-based encryption and its application. Inf. Sci. 2020, 517, 217–229.
[8] Sowjanya, K.; Dasgupta, M. A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC. J. Inf. Secur. Appl. 2020, 54, 102559.
[9] Zhang, Z.; Zhang, J.; Yuan, Y.; Li, Z. An expressive fully policy-hidden ciphertext policy attribute-based encryption scheme with credible verification based on blockchain. IEEE Internet Things J. 2021, 9, 8681–8692.
[10] Hu, G.; Zhang, L.; Mu, Y.; Gao, X. An expressive "test-decrypt-verify" attribute-based encryption scheme with hidden policy for smart medical cloud. IEEE Syst. J. 2020, 15, 365–376.
[11] Zeng, P.; Zhang, Z.; Lu, R.; Choo, K.-K.R. Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. IEEE Internet Things J. 2021, 8, 10963–10972.
[12] Xie, M.; Ruan, Y.; Hong, H.; Shao, J. A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. Future Gener. Comput. Syst. 2021, 121, 114–122.
[13] Miao, Y.; Deng, R.; Liu, X.; Choo, K.-K.R.; Wu, H.; Li, H. Multi-authority attribute-based keyword search over encrypted cloud data. IEEE Trans. Dependable Secur. Comput. 2019, 18, 1667–1680.
[14] Zhang, W.; Zhang, Z.; Xiong, H.; Qin, Z. PHAS-HEKR-CP-ABE: Partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system. J. Ambient. Intell. Humaniz. Comput. 2022, 13, 613–627.
[15] Zhao, C.; Xu, L.; Li, J.; Fang, H.; Zhang, Y. Toward secure and privacy-preserving cloud data sharing: Online/offline multiauthority CP-ABE with hidden policy. IEEE Syst. J. 2022, 16, 4804–4815.