Proxy Re-Encryption Scheme For Cloud Computing With Public Verifier

S. R. Ashmi[1], Mrs. M. Supriya, M.E, Ph.D[2]
[1, 2] Dept of CSE
[1, 2] Stella Mary's College of Engineering

Abstract- *With the rapid development of cloud computing technology, how to achieve secure access to cloud data has become a current research hotspot. Attribute-based encryption technology provides the feasibility to achieve the above goal. However, most of the existing solutions have high computational and trust costs. Furthermore, the fairness of access authorization and the security of data search can be difficult to guarantee. To address these issues, we propose a novel access control scheme based on block chain and attribute-based searchable encryption in cloud environment. The proposed scheme achieves fine-grained access control with low computation consumption by implementing proxy encryption and decryption, while supporting policy hiding and attribute revocation. The encrypted file is stored in the IPFS and the metadata ciphertext is stored on the block chain, which ensures data integrity and confidentiality. Simultaneously, the scheme enables the secure search of ciphertext keyword in an open and transparent block chain environment. Additionally, an audit contract is designed to constrain user access behaviour to dynamically manage access authorization. Security analysis proves that our scheme is resistant to chosen-plaintext attacks and keyword-guessing attacks. Theoretical analysis and experimental results show that our scheme has high computational and storage efficiency, which is more advantageous than other schemes.*

Keywords- Access control, Attribute-based encryption, Blockchain, Secure search, Attribute revocation.

I. INTRODUCTION

With the connection of the global mobile Internet and the rapid development of cloud computing, more and more communication academia and industry are committed to shaping a safe and effective resource sharing method in the cloud environment. Cloud storage technology has been widely used due to its high performance and low cost. To ensure the security of private data, data is usually stored in cloud services in encrypted form. However, the traditional public key encryption technology has been unable to meet the current needs of cloud data privacy protection. In this context, how to achieve access authorization and accurate retrieval of encrypted cloud data has become a new challenge.

Access control (AC) is a key technology to maintain data security and privacy. Te AC provides a solution to the above problem by constraining user access rights to ensure legitimate access to sensitive data. Attribute based searchable encryption based on ciphertext policy not only enables fine-grained access control of encrypted data, but also supports users to retrieve ciphertext based on keywords. Ciphertext Policy Attribute-Based Encryption Algorithm (CP-ABE) allows data owners to autonomously set data access policies according to a set of attributes, and associate data access policies with ciphertexts. When the user's attribute set satisfies the access policy, the ciphertext can be decrypted using the corresponding attribute private key, while the specific identity of the decrypt or remains unknown, which is suitable for "one-to-many" access scenarios. In recent years, a large number of studies have applied attribute based encryption technology to cloud data access control to improve the privacy and security of cloud data. However, the traditional CP-ABE algorithm consumes a lot of computational cost and the security of the access policy is often ignored because the access policy is embedded in the ciphertext. In addition, attribute access expiration and permission changes are also urgent issues to be addressed.

Attribute-based proxy re-encryption (ABPRE) scheme is one of the proxy cryptography, which can delegate the reencryption capability to the proxy and re-encrypt the encrypted data by using the re-encryption key. ABPRE extending the traditional proxy cryptography and attributes plays an important role. In ABPRE, users are identified by attributes, and the access policy is designed to control the user's access.

Using ABPRE can have these advantages: (i) The proxy can be delegated to execute the re-encryption operation, which reduces the computation overhead of the data owner; (ii) The authorized user just uses his own secret key to decrypt the encrypted data, and he doesn't need to store an additional decryption key for deciphering; (iii) The sensitive information cannot be revealed to the proxy in re-encryption, and the proxy only complies to the data owner's command. In this prospective recipient. Later, when a transplant surgeon accepts the donated organ, the donor's surgeon is notified to remove

the donated organ. Finally, the donated organ is transported to the patient's hospital and received by the transplant surgeon. However, suppose the situation is for a live donor and it has been planned to donate to a known person by name. In that case, the data will go directly to the transplant surgeon to start the surgery of removing and transplanting the donated organpaper, we survey two various access policy attribute-based proxy re-encryption schemes and analyze these schemes. Thereafter, we list the comparisons of them by some criteria.

II. LITERATURE SURVEY

Due to the mobility of users in an organization, inclusion of dynamic attributes such as time and location becomes the major challenge in Ciphertext-Policy Attribute-Based Encryption (CP-ABE). By considering this challenge; we focus to present dynamic time and location information in CP-ABE with multi-authorization. At first, along with the set of attributes of the users, their corresponding location is also embedded. Geo hash is used to encode the latitude and longitude of the user's position. Then, decrypt time period and access time period of users are defined using the new time tree (NTT) structure. The NTT sets the encrypted duration of the encrypted data and the valid access time of the private key on the data user's private key. Besides, single authorization of attribute authority (AA) is extended as multi authorization for enhancing the effectiveness of key generation. Simulation results depict that the proposed CP-ABE achieves better encryption time, decryption time and security level and memory usage.

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 specific 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.

Attribute-based Encryption (ABE) schemes have proven to be essential for providing privacy and security for the cloud-based data intensive applications. With the evolution of cloud computing data storage services understanding the vulnerabilities of the privacy and security systems is challenging. The task of incorporating various specific implementation needs adaptability which would further develop side effects. In this paper, an exhaustive study is conducted on various proposed works. Defining revocation policies, access policies, and attribute definition policy need special attention for a better security mechanism. Moreover, it has been observed that ML has its own role to provide the intelligent solutions. Adopting ML for implementing the ABE schemes would develop efficient solution, which would further enhance the cloud security performance. Various research challenges and opportunities are listed for the purpose of research that can be conducted in these directions. However, the challenge in implementing the security mechanisms through the unknown layer or untrusted layers or untrusted third party is verifying the authenticity of the decryption keys which are used to decrypt the sensitive data on a sharable platform.

Access control is an important security mechanism for the protection of sensitive information and critical system resources. While it has been well-known that traditional access control models (TACMs), such as DAC, MAC, RBAC, etc., are not well suited for open networks due to the lack of dynamism in the management of access privileges, pro-active or dynamic access control models (PACMs) developed in recent years generally suffer from performance problems due to complex evaluation performed prior to access authorization. In game theory based dynamic access control models, which are one type of dynamic models, each access is modeled as a game that is played between the accessing subject and the accessed or protected object and the result of the play serves as the basis for making the authorization decision. Thus, delay is unavoidably introduced into the authorization process due to such pre-access evaluation. To overcome the shortcomings of TACMs and PACMs simultaneously, in this paper, we propose a new access control model called ISAC that, unlike all present access control models, is used not as a mechanism for access authorization but one for dynamic management of access privileges upon the completion of each access with the result being an updated set of access privileges for the accessing subject and used for updating the corresponding access control list for the subject. Access authorization will

still be performed in the same way as that in the traditional access control models.

In IoT, a flexible and trustworthy access control framework is of significance to ensure the security of lightweight IoT devices. The conventional centralized access control framework is no longer fit for the open and large-scale IoT environments. In this paper, we propose an attribute-based distributed access control framework (ADAC) for IoT using blockchain technology. The attributes, such as manufacturer and object-specified attribute, are considered in the proposed ADAC for more fine-grained access control in the open and lightweight IoT devices. Particularly, we design a smart contract system, which includes a subject contract (SC), an object contract (OC), an access control contract (ACC) and multiple policy contracts (PCs), to manage and access attributes of IoT devices for distributed and trustworthy access control (DTAC). SC and OC are responsible for managing subject attribute and object attribute information, respectively. PCs are used to manage access control policies. ACC performs authorization judgment by accessing attributes and policies. Finally, a case study is performed to demonstrate the workflow and show that ADAC could achieve fine-grained and flexible access control for IoT.

III. PROPOSED SYSTEM

Currently, most access control schemes typically use a centralized management model, which makes them susceptible to system-wide failure in the event of a single malfunction. Furthermore, traditional solutions rely on trusted third parties for access decisions, which not only incur high trust overhead but also unfair service fee payments. Therefore, designing secure and fair search able access control schemes remains a pressing challenge. Block chain is a distributed ledger technology characterized by decentralization, openness, transparency, tam per resistance, and traceability. It supports the secure storage and transaction of data without the involvement of third parties, and users no longer have to worry about the high trust and security risks posed by third parties. This means that block chain technology can be used to replace traditional third parties for access authorization management, enabling a fair and trusted distributed access control framework.

Based on the analysis of the above problems, we combine block chain technology with attribute-based searchable encryption technology to propose a novel distributed data-sharing scheme. This scheme focuses on achieving fine-grained searchable access to encrypted cloud data while taking into account low computational cost, policy privacy, attribute revocation and dynamic authorization.

The main contributions of this study are as follows:

(1) A distributed fine-grained access control scheme is developed by combining block chain and attribute based searchable encryption. Te scheme stores the data cipher text in the distributed IPFS (Inter Planetary File System), and facilitates the secure distribution of metadata cipher text via block chain smart contract, thus avoiding the high trust cost and low security of storage caused by third-party intervention in traditional access systems.

(2) An improved attribute-based searchable encryption algorithm based on policy hiding is designed to prevent the leakage of user privacy attributes. Proxy encryption and decryption are introduced to reduce the user's computational consumption. Simultaneously, the algorithm supports attribute revocation and decryption verification.

(3) Te proposed scheme realizes the secure search of encrypted keywords on the block chain. At the same time, we design a smart contract with a search audit function to dynamically manage access rights based on user access behaviour and accessibility period to prevent illegal access.

(4) Security analysis, performance comparison, and simulation experiments indicate that the proposed scheme is both feasible and advantageous.

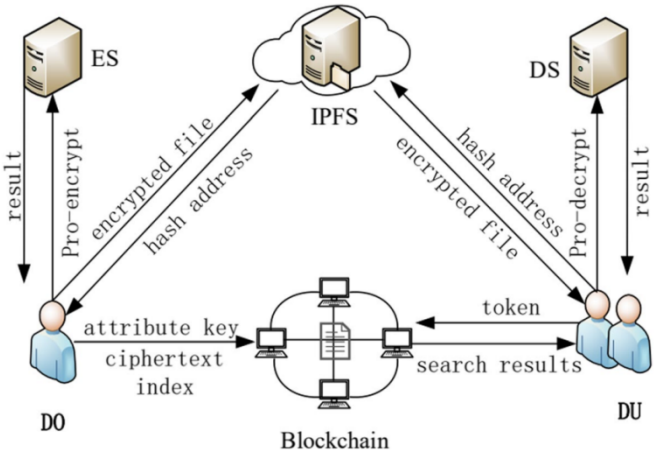

Fig.1. System Architecture

This scheme uses block chain technology, attributes based searchable encryption, and IPFS to propose a fine grained access control scheme with a hidden policy and distributed storage. IPFS is a distributed storage system with decentralized cloud computing capabilities. Compared with traditional centralized storage systems, IPFS does not have a single point of failure, and the nodes do not trust each other, which provide higher security and access efficiency. With the development of cloud computing, it has become a trend for

IPFS to replace traditional local storage technology. When a file is uploaded to the IPFS, it is split into multiple blocks for storage, and the system returns a unique hash value. Te user does not need to know the storage path, and the unique hash value can determine data tampering. To download a file from the IPFS, the user can retrieve it through a hash address.

SYSTEM MODULES

- Data Owner
- Data User
- IPFS
- Block chain
- Proxy encryption server
- Proxy decryption server

MODULE DESCRIPTION

Data Owner

Data Owner is the publisher of data. Its main responsibilities are to develop attribute sets, set private keys and access time periods for accessing users, and set access policies and keyword indexes for shared data. It also uploads the file cipher to IPFS and the metadata cipher to the smart contract.

Data User

Data User requests cryptographic metadata ciphertext and storage address from the smart contract according to the search token, and the address obtains the ciphertext file from IPFS. When the attribute set of DU satisfies the access policy, it can be accessed through the attribute private key to decrypt the ciphertext.

IPFS

IPFS is mainly responsible for the distributed storage of ciphertext data uploaded by DO and returning the ciphertext according to the hash storage address.

Block chain

The block chain is responsible for the distribution of the user's private key and ciphertext, and for making appropriate audit decisions based on user access behaviour. Simultaneously authenticate user attributes and perform keyword searches.

Proxy encryption server

Mainly responsible for proxy encryption calculation.

Proxy decryption server

Mainly responsible for proxy decryption calculation.

IV. RESULT AND DISCUSSION

4.1 SIMULATION OUTPUT

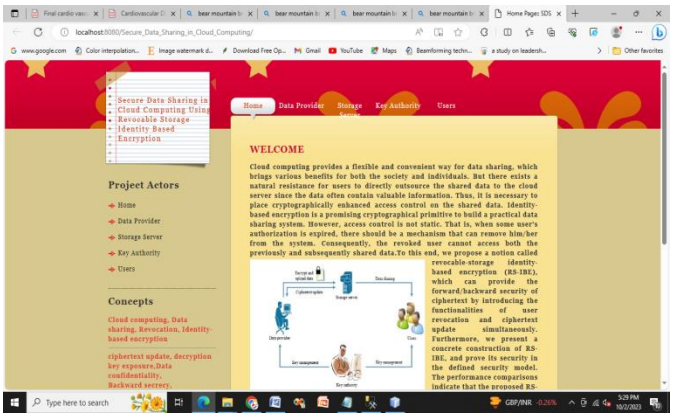

Fig.2. Home Page

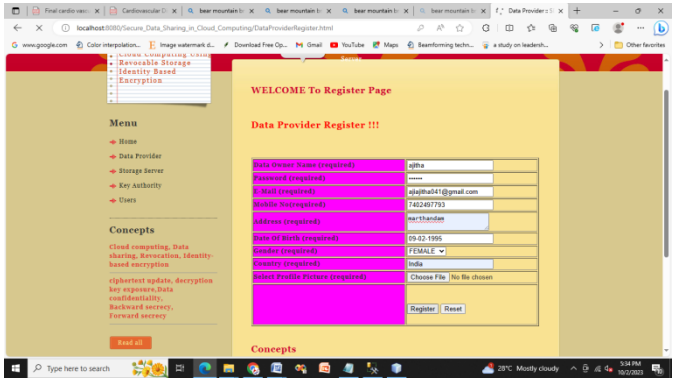

Fig.3. Data Provider Registration

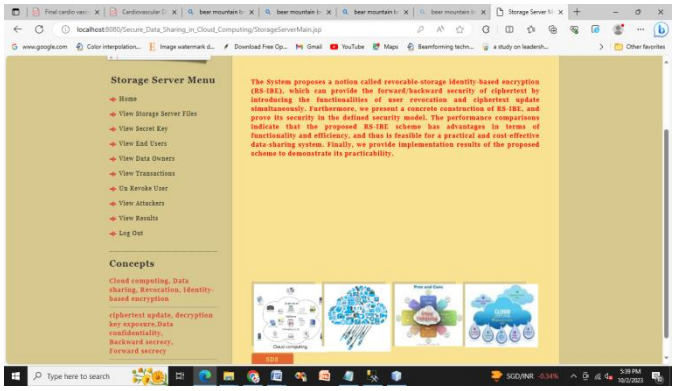

Fig.4. Storage Server Home Page

Fig.5. Storage File details

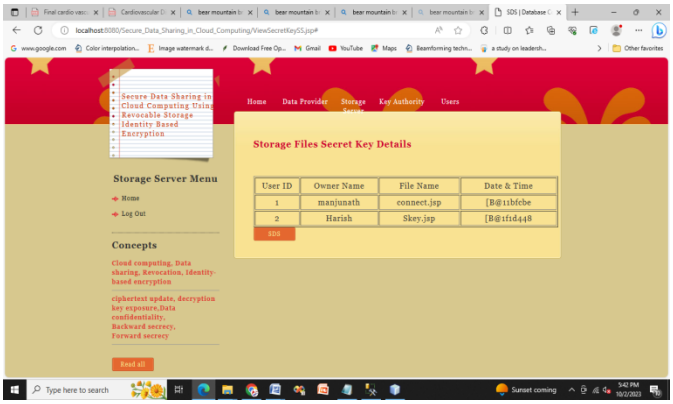

Fig.6. Storage File Secret Key

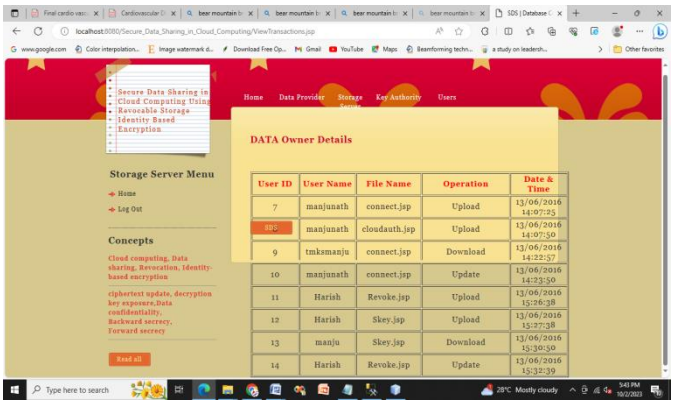

Fig.7. Data Owners

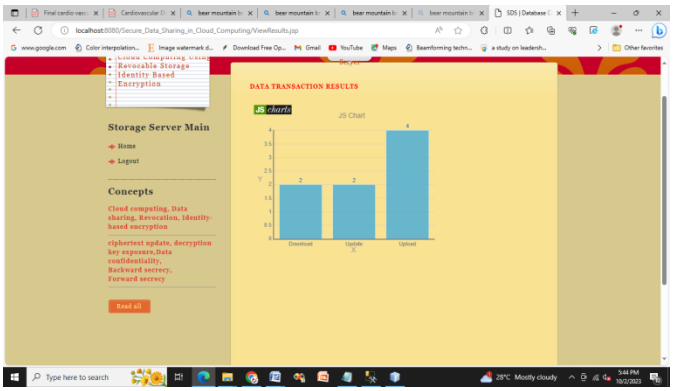

Fig.8. Data transaction result

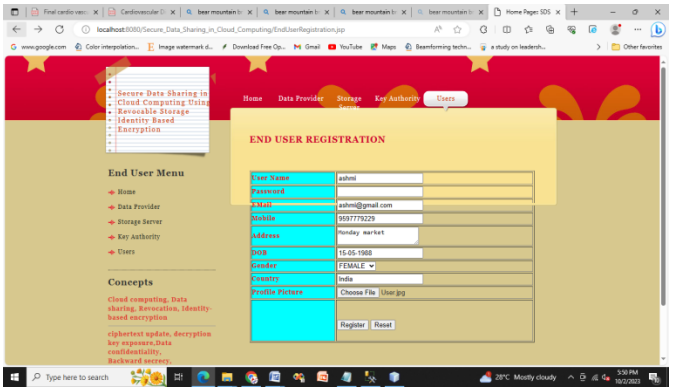

Fig.9. End User Registration

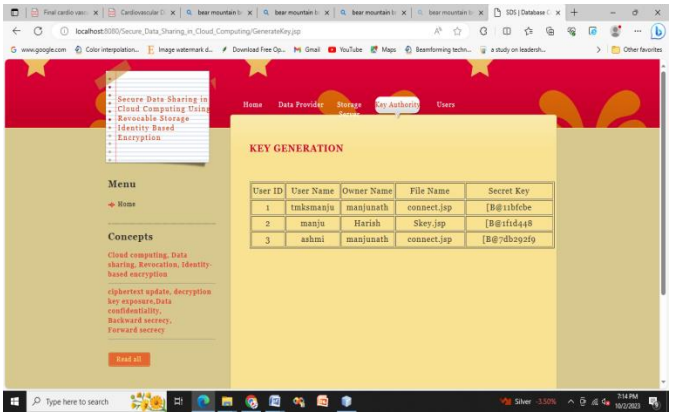

Fig.10. Key Generation

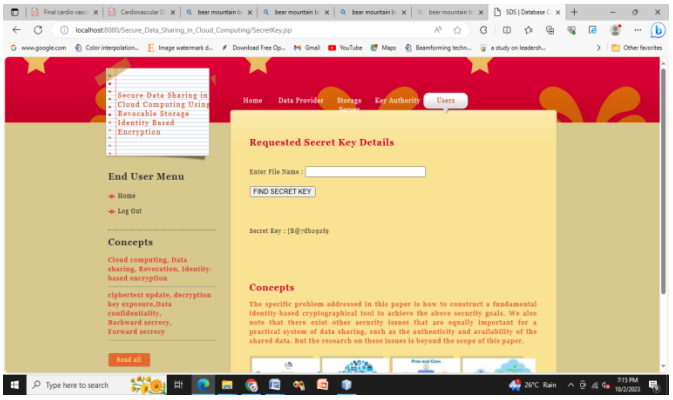

Fig.11. Request secret key

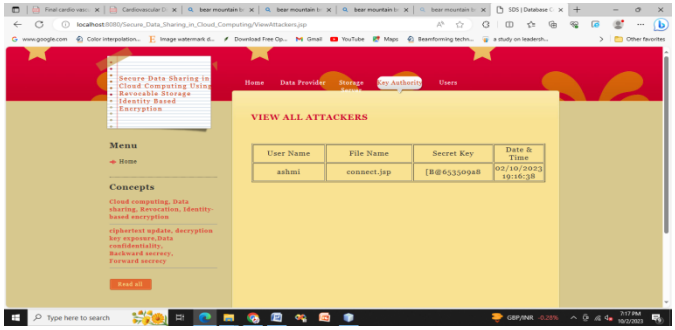

Fig.12. Attacker details

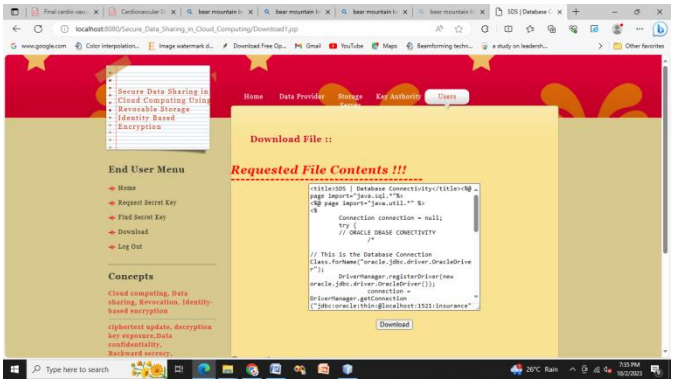

Fig.13. Request File contents

V. CONCLUSION

Thus a data security access control scheme based on block chain and attribute-based searchable encryption in the cloud computing environment. This solution realizes fine-grained access and secure search of cloud data on the premise of supporting policy hiding and attribute revocation. At the same time, proxy encryption and decryption are introduced to reduce the computing cost of users. Combined with block chain technology, it ensures the secure distribution of metadata ciphertext and keys, as well as a fair search for keywords. In addition, the smart contract is used to realize dynamic monitoring of user access behaviour. Security analysis, performance comparison, communication analysis and computing analysis show that this scheme provides higher storage and computing performance while ensuring data security and user access fairness. It can be better applied to practical application scenarios such as smart grid and smart healthcare.

In future research, we will mainly focus on how to improve the efficiency of user access and multi-keyword search on the block chain.

REFERENCES

[1] Al Breiki H, Al Qassem L, Salah K, Rehman MHU, Sevtinovic D (2019) Decentralized access control for iot data using blockchain and trusted oracles. In: 2019 IEEE International Conference on Industrial Internet (ICII). IEEE, Orlando, pp 248–257

[2] Cao L, Kang Y, Wu Q, Wu R, Guo X, Feng T (2020) Searchable encryption cloud storage with dynamic data update to support efcient policy hid ing. China Commun 17(6):153–163

[3] Chen N, Li J, Zhang Y, Guo Y (2020) Efcient cp-abe scheme with shared decryption in cloud storage. IEEE Trans Comput 71(1):175–184

[4] De SJ, Ruj S (2017) Efcient decentralized attribute based access control for mobile clouds. IEEE Trans Cloud Comput 8(1):124–137 21. Li H, Pei L, Liao D, Chen S, Zhang M, Xu D (2020) Fadb: A fne-grained access control scheme for vanet data based on blockchain. IEEE Access 8:85190–85203

[5] Fan K, Pan Q, Zhang K, Bai Y, Sun S, Li H, Yang Y (2020) A secure and verifable data sharing scheme based on blockchain in vehicular social networks. IEEE Trans Veh Technol 69(6):5826–5835

[6] Gao S, Piao G, Zhu J, Ma X, Ma J (2020) Trustaccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain. IEEE Trans Veh Technol 69(6):5784–5798

[7] Huang C, Wei S, Fu A (2019) An efcient privacy-preserving attribute based encryption with hidden policy for cloud storage. J Circ and Syst Comput 28(11):1950186

[8] Hur J (2013) Attribute-based secure data sharing with hidden policies in smart grid. IEEE Trans Parallel Distrib Syst 24(11):2171–2180

[9] Kang J, Yu R, Huang X, Wu M, Maharjan S, Xie S, Zhang Y (2018) Block chain for secure and effcient data sharing in vehicular edge computing and networks. IEEE Internet Things J 6(3):4660–4670

[10] Li R, Song T, Mei B, Li H, Cheng X, Sun L (2018) Blockchain for large-scale internet of things data storage and protection. IEEE Trans Serv Comput 12(5):762–771

[11] Liu B, Xiao L, Long J, Tang M, Hosam O (2020) Secure digital certif cate-based data access control scheme in blockchain. IEEE Access 8:91751–91760

[12] Maesa DDF, Mori P, Ricci L (2019) A blockchain based approach for the definition of auditable access control systems. Comput Secur 84:93–119

[13] Nayudu PP, Sekhar KR (2018) Cloud environment: A review on dynamic resource allocation schemes. Int J Appl Eng Res 13(6):4568–4575

[14] Nayudu PP, Sekhar KR (2021) Enhancement of attribute - based encryp tion schemes through machine learning techniques: research challenges and opportunities. J Jilin University 40:1–18

[15] Nayudu PP, Sekhar KR (2022) Accountable specifc attribute-based encryption scheme for cloud access control. IntJ Syst Assur Eng Manag 1–10

[16] Nayudu PP, Sekhar KR (2023) Dynamic time and location information in ciphertext-policy attribute-based encryption with multi-authorization. Intell Autom Soft Comput 35(3):3801-3813

[17] Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafq M (2019) A secure data sharing platform using blockchain and interplanetary file system. Sustainability 11(24):7054

[18] Qiu S, Liu J, Shi Y, Zhang R (2017) Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. Sci China Inf Sci 60(5):1–12
[19] Sandhu RS, Samarati P (1994) Access control: principle and practice. IEEE Commun Mag 32(9):40–48
[20] Sandor VKA, Lin Y, Li X, Lin F, Zhang S (2019) Effcient decentralized multi authority attribute based encryption for mobile cloud data storage. J Netw Comput Appl 129:25–36
[21] Wang P, Yue Y, Sun W, Liu J (2019) An attribute-based distributed access control for blockchain-enabled iot. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, Barcelona, pp 1–6
[22] Yang Y (2015) Attribute-based data retrieval with semantic keyword search for e-health cloud. J Cloud Comput Adv Syst Appl 4(1):1–6
[23] Yu J, Zhang H, Li S, Mao L, Ji P (2019) Data sharing model for internet of things based on blockchain. J Chin Mini-Micro Comput Syst 40(11):2324–2329
[24] Yuan Y, Wang FY et al (2016) Blockchain: the state of the art and future trends. Acta Autom Sin 42(4):481–494
[25] Zhu N, Cai F, He J, Zhang Y, Li W, Li Z (2019) Management of access privi leges for dynamic access control. Cluster Comput 22(4):8899–8917