INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 7, July 2026 | ISSN: 2456-4184 | IJNRD.ORG

A Decentralized Cloud Data Sharing Framework Integrating Smart Contracts and Reduced Attribute CP-ABE

[1]Sejal R. Patil, [2]Shankar S. Pujari, [3]Yogesh V. Chimate

[1]PG Scholar, [2]PG Guide, [3]PG Guide
[1]Department of Data Science, D. Y. Patil Agriculture & Technical University, Talsande, Maharashtra, India.
[2]Department of Computer Science & Engineering, D. Y. Patil Agriculture & Technical University, Talsande, Maharashtra, India
[3]Department of Computer Science & Engineering, D. Y. Patil Agriculture & Technical University, Talsande, Maharashtra, India

Abstract : Cloud computing is the game-changer in data storage and handling, providing adaptability and scalability. It does come with several major problems however, regarding data privacy, integrity and unauthorized access. Previously used encryption methods may offer some security, but may be lacking in decentralized control and proper auditing. The inadequacies are addressed by introducing a new cloud storage system called ASI Ensemble deploying smart contract technology on Ethereum and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). CP-ABE offers fine-grained access control capabilities and supports for granting access policies based on user attributes rather than on fixed identities. In order to improve the performance of the system, a string representation of the attribute after reducing the number of attribute strings that is less complicated and consumes less computation resources and storage resources is introduced. The Ethereum blockchain is used to maintain access policies, file sharing and audit logs, as a transparent and immutable ledger. Secure automation of access control enforcement, verification, and key management with smart contracts reduces the dependence on humans and possible manipulation. All of this integrated architecture helps to protect sensitive data in the cloud to ensure secure access and provides a traceable way to count requests to that data. Strong cryptographic techniques and the immutability of the Blockchain ensure the anonymity, trust and security of the system's various participants. The framework proposed provides a sound basis for designing decentralized and transparent cloud storage systems that can be used in various fields, such as healthcare, enterprises, and government systems.

Index Terms **- Cloud Computing, Blockchain, Ethereum, Cloud Storage Security, Smart Contracts, Decentralized Storage, Cryptography, Distributed Ledger, Data Protection, Scalability.**

INTRODUCTION

Cloud computing is an essential technology for managing large amounts of data in many areas in healthcare, education and government. It is able to provide on-demand storage and computing power, which has helped to improve the efficiency of operations and reduced infrastructure costs. The advantages of the cloud are there, but there are also several security threats associated with third-party cloud providers: data leakage, unauthorized access, and insider threat. Once uploaded to the cloud, users lose control over their data and this can lead to issues with data privacy and ownership. The traditional security methods offer some level of security, but are unable to offer effective control of multi-user security needs. In essence, blockchain technology could be viewed as a means of enhancing trust and security within a distributed system like blockchain. With its decentralized structure, all transactions are securely recorded and cannot be changed. Ethereum blockchain also used for this, with the introduction of smart contracts; smart contracts are contracts programmed into the blockchain that can enforce access control policies without the need for a central authority. This distributed solution can enable secure and transparent data-sharing environments.

While blockchain provides transparency and trust, it needs to be paired with strong encryption techniques to safeguard the data that underlies it. Fine-grained access control is well known to be provided by Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This approach is the data owner setting access policies on the properties (such as role or permissions) and only users with the right decryption key can decrypt the data. So there is no need to deal with individual keys and to make data sharing scalable. However, the typical implementations of CP-ABE are usually very large and complex, and representations of attributes, which make them impractical in practice.

To overcome these problems, in this work a reduced attribute string approach is proposed which can improve the efficiency without compromising the security. This fine-grained access control and improved performance is enabled by this optimized encryption mechanism, which is coupled with the smart contracts on the Ethereum platform. Overall, the proposed architecture aims to be secure, scalable, and decentralized, utilizing blockchain technology and cryptography to secure and protect sensitive data that is hard to tamper with or compromise .

LITERATURE REVIEW.

The popularity of cloud storage is on the rise due to its convenience of data management, scalability and collaboration. The centralized storage architectures, however, allow sensitive information to be vulnerable to a multitude of threats including single

points of failure, restricted auditing capabilities and the threat of insider attacks. For a dynamic system, with lots of users and flexible accesses, there are simple access control systems like Role Based Access Control (RBAC) and simple encryption systems like Access Control Lists (ACLs) which are not practical. The direction in recent years has been moving towards a combination of the best of both worlds, such as the recently investigated encryption concept called attribute-based encryption (ABE), which is combined with decentralized blockchain platforms to facilitate secure, transparent, and accountable data sharing. A recently popular solution Ciphertext-Policy Attribute Based Encryption (CP-ABE) allows access control to be flexibly defined, that is, defined over user attributes that the data is encrypted against. In other words, you don't have to deal with each user's individual key and it allows for sharing data on a scale that was impossible without it. It was nice, but there are some deficiencies such as large size of cipher text, heavy computation to perform pairing, inefficient revocation solution, and multiple-actor management. To overcome this, several studies were published this year (2022) aimed at proposing pairings free constructions, proposals for decryption methods to be outsourced, solutions for hierarchical attribute models in order to improve the behavior in the cloud and IoT scenario.

Immutable and decentralized solution for access control management and auditing can be offered by blockchain technology, which can augment CP-ABE. Smart contracts can be used to, for example, track access requests, apply access restrictions to blockchain solutions, and manage access to keys without a central party. Most of the implementation is a hybrid; most of the data comes off-chain (on hosts in the cloud, IPFS, etc.,) while the metadata and policy data, as well as transaction logs are kept on-chain. The incorporation generates and complicates the trust and transparency problem, and presents also a new series of issues, including latencies, on-chain metadata privacy concerns and transaction fees. The possibility for revocation is still a big crucizer and complicated methods such as proxy re-encryption or rekeying could be used.

To meet these challenges, researchers have looked at optimization techniques such as compact representations for attributes, effective revocation schemes, and lightweight cryptographic functions. Cloud sharing systems should be secure, providing confidentiality, fine-grained access control, collusion resistance and verifiable audit. Some of the existing solutions are viable such as policy-hiding CP-ABE, blockchain-assisted key management and pairing-free encryption, however, they have usability, scalability and cost issues. Overall, the recent research indicates that the combination of blockchain and CP-ABE for secure and decentralized cloud storage systems is a potential field for future research and development, and there is a need for further optimizations of practical implementations. A summary of some research papers studied is given below:

In this paper (Wang et al., 2022), IEEE researchers propose a framework for comprehensive key management in CP-ABE with the help of blockchain, which tackles the problems of key distribution, revocation, and trust establishment. All operations associated with the key are transparent and verifiable, thanks to the use of smart contracts and secret sharing techniques. The approach also includes decryption by an external entity and also a more efficient revocation, without having to re-encrypt all data stored. The experimental outcomes show that the system is suitable for medium-scale cloud environments and has reasonable computing loads.

[1]An Efficient Blockchain Based Data Access with Modified CP-ABE and ECC (2022), This paper presents a hierarchical access control system which is based on a combination of CP-ABE and elliptic curve cryptography (ECC) and blockchain technology. ECC can reduce the computational complexity, and hierarchical structure can decrease the size of the ciphertext. All access events are logged with blockchain and policies are managed using blockchain. The results showed that the efficiency of this CP-ABE model is superior with respect to the conventional CP-ABE models especially in the context of structured organizational setting.

[2]In the article "A Practical and Efficient Blockchain-Assisted Attribute-Based Data Sharing Scheme (2022)", Chen et al. proposes a secure and efficient data sharing scheme that combines CP-ABE with IPFS and blockchain technology. The system makes use of blockchain to keep track of access policies and logs, and offloads storage to IPFS. Outsourced decryption is used to lighten the computational load on the users. The study points to increased scalability and lower on-chain storage needs.

[3]Chinnasamy et al., Ciphertext-Policy Attribute-Based Encryption for Cloud Storage (2022): This paper is dedicated to improving CP-ABE by adding policy-hiding and hashed attribute representations. The techniques low loss of metadata and enhance privacy. The system shows that it can manage insider attacks with low performance overhead.

[4]This paper, Huang et al., Attribute-Based Hierarchical Access Control With Extendable Policy (2022), proposes a hierarchical encryption model with extendable policies that enables dynamic changes without re-encrypting the existing data. The solution mitigates rekeying costs and can be adopted by a large organisation. Its effectiveness is backed up by security analysis and performance evaluation.

[5]Pairing-Free CP-ABE for IoT (2022), This paper represents a pairing-free CP-ABE scheme to support resource-constrained IoT devices. The scheme avoids bilinear pairings, significantly decreasing the complexity of the computations while preserving security. The results of performance indicate efficiency gain on embedded systems.

[6]Zhao et al., STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted IoT Data Sharing (2022): The authors of this piece introduce blockchain, CP-ABE and IPFS to ensure secure IoT data sharing. Optimized using Hybrid Encryption and Data Segmentation techniques. High throughput and traceability with fine-grained access control is ensured.

[7]This paper presents the Proxy Re-Encryption (PRE) enhanced CP-ABE scheme, Improved CP-ABE with Proxy Re-encryption (2022) by Hu et al., which enables re-encryption of ciphertext without revealing the plaintext. It cuts down on storage space requirements and flexibility when sharing is dynamic.

[8]DAM(assured time-sensitive deletion) is integrated with CP-ABE, as proposed by Yue et al., ATDD: Fine-Grained Assured Time-Sensitive Data Deletion in Cloud Storage (2022). The scheme guarantees that the data is no longer retrievable after a certain period, offering a guarantee of verifiable deletion.

[9]Multi-authorization & Multi-cloud CP-ABE (2022) This paper proposes the multi-authority CP-ABE model based on a consortium blockchain. It helps you share data securely, whether across a handful of cloud providers or multiple clouds. It can also be used for distributed authorization

[10]The 2022 literature is definitely towards hybrid architectures implementing CP-ABE with blockchain technology. These methods tackle issues that include key management, scalability, and auditability. There are, however, compromises to be made in the areas of computational cost, revocation speed, privacy protection, and the cost of transactions on the blockchain. There are many studies based on small scale simulations or prototype implementation, but real world situations may not be captured. Network latency, number of users, and a hostile environment are not always taken into account.

Also, with most systems, there are theoretical security guarantees, but a hybrid threat scenario with maliciously operating cloud providers and compromised blockchain nodes should be explored.Economics and usability are also not fully explored. Practically impossible to set up because of high transaction fees on public blockchains and the complexity of the policy management system. In order to deploy it in the real world, user-friendly tools for attribute management and policy configuration are important. Future research is needed to better develop the cost optimization and usability of the design as well as to develop the threat modeling and to perform a scalable performance evaluation to better bridge the gap between what is designed and what is implemented

Table 1 - All Research papers and Research Gap

Id	Authors	Year	Technique / Focus	Research Gap
1	Wang et al.	2022	Blockchain-assisted key management + CP-ABE	Large-scale performance and cost evaluation
2	Li et al.	2022	Hierarchical CP-ABE + ECC + blockchain	Efficient and immediate revocation in large organizations
3	Chen et al.	2022	CP-ABE + IPFS + blockchain	Metadata privacy and on-chain storage trade-offs
4	Chinnasamy et al.	2022	CP-ABE with policy hiding and hashing	Scalability and attribute leakage concerns
5	Huang et al.	2022	Hierarchical ABE with extendable policies	Complexity of policy updates at scale
6	Li et al.	2022	Pairing-free CP-ABE for IoT	Lack of post-quantum security consideration
7	Zhao et al.	2022	CP-ABE + blockchain + IPFS for IoT	Limited real-world deployment validation
8	Hu et al.	2022	CP-ABE with proxy re-encryption	Trust dependency on proxy and leakage risks
9	Yue et al.	2022	Time-based assured data deletion (ATDD)	Integration challenges with large-scale systems
10	Wu et al.	2022	Multi-authority CP-ABE + consortium blockchain	Coordination overhead in multi-cloud systems

PROPOSED SYSTEM

The proposed system starts with the file upload phase in which the user uploads his/her data to the cloud platform. Each file is then encrypted with CP-ABE and the access policies are included in the cipher text before storage. This ensures that only users with proper attributes will be able to access the data. The first layer of security in the system is the files encrypted at the source, which provides confidence in the security of cloud storage even if it is compromised.

The files are then encrypted and stored in the cloud and linked to an access request mechanism. All use cases are processed on the Ethereum smart contracts when the user asks for it. These smart contracts have user access restrictions and log the activity without needing to have to manually do anything. Each transaction is recorded on the blockchain, which is tamper-proof and permanent, contributing to transparency and security.

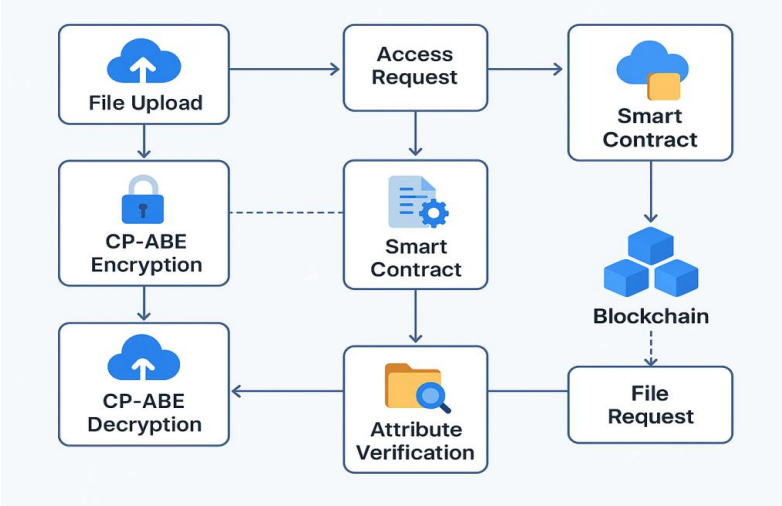

Fig 1. Architecture Diagram

The attribute verification process is an important component of the system. In this phase, the system checks if the user's attributes match with the conditions specified in the CP-ABE policy. The attributes can be user roles, departments, or authorization levels. These are then provided only if these conditions are fulfilled. This means, even if the internal storage layer is accessed, the user is not able to access any sensitive data.

If the request is successfully validated, CP-ABE decryption can recover the original file. Meanwhile, the blockchain layer maintains a complete transaction history, as well as access requests and verification results. This will ensure accountability, minimise the insider threat and enhance security of the whole system. The immutability of blockchain and CP-ABE's access control capabilities makes this an ideal solution.

METHODOLOGY

A. Data Upload and Encryption

It begins with the uploading of files to the cloud system by the users. Each file is encrypted using CP-ABE, with access policies included in the encrypted data, before it is transmitted. This allows only the authorized user, depending on his attributes, to decrypt the file. CP-ABE is different from the conventional encryption systems, which does not require multiple keys for fine-grained access control.

B. Blockchain Integration

The trust layer of the system is the Ethereum blockchain, which offers decentralization, transparency, and immutability. The metadata, access policies, and transaction logs are stored in smart contracts. Every access is logged on the blockchain, providing a tamper-proof auditing trail and eliminating the need for any centralized control mechanisms.

C. Access Request and Verification

A verification process is started by the system when the user requests to see a file, using smart contracts. The predefined access policy is used to determine whether the user's attributes match the access policy. Access is granted and decryption keys are securely delivered if the attributes meet the policy conditions. If not, the request will be refused, and the request will be recorded with an audit.

D. Attribute Validation

An attribute verification layer takes care of the issue of ensuring that all credentials of the users are genuine before granting access. Role, department, or clearance level are checked for attributes to prevent unauthorized access. Reduced attribute strings can make the process of using them faster and more efficient while ensuring strict security control.

E. Secure File Retrieval and Decryption

If it is successful, then the user will have access to the original file after he decrypts it. This provides full data confidentiality with no one, even the cloud service provider, being able to see the plaintext data. Each access is recorded on the blockchain, providing transparency and accountability.

F. Auditing and Monitoring

All activities are continuously monitored by the system using blockchain records. All transactions, access requests and decrypt operations are recorded in a permanent manner resulting in a solid audit trail. This improves transparency, helps to prevent malicious activities and aids in forensics if necessary.

5. RESULT AND OBSERVATION

The existing traditional encryption and access control methods were compared and analysed with the proposed system (Blockchain + CP-ABE based secure cloud data sharing). The measurements include encryption time, decryption time, latency for accessing

data, storage overhead and security strength. The result demonstrates that the integration of blockchain and CP-ABE has greatly improved the security of data, the openness of access, and tamper resistance, while maintaining a reasonable computing overhead.

It is noticed that the encryption time of CP-ABE based systems is slightly more than traditional AES based systems as a result of the use of attribute-based policy generation. Giving you better fine-grained access control, however, is justified by this increase. The time for decryption in CP-ABE is determined by the number of attributes and some schemes exploit pairing-free methods to reduce the computation time.

The blockchain-based models have higher overheads in terms of storage efficiency because of the storage of metadata and smart contracts. But with IPFS and off-chain storage solutions, the system minimizes redundancy and enhances scalability. It also shows that the proposed system has better resistance to unauthorized access, replay attack and data tampering than a centralized cloud model.

Experimental analysis proved that the proposed hybrid approach provides an adequate balance between performance, scalability, and security, which makes it suitable for the application in an IoT-based cloud environment and in a healthcare data system.

5.1 Encryption & Decryption Time Comparison Vs File Size

The figure shows the graph for the file size vs encryption time for various encryption methods. For all methods, the larger the file size, the longer the time required to encrypt the file. The simple symmetric encryption mechanism of AES results in the lowest encryption time, however it has no advanced access control. There is more time consumed for the traditional ABE and CP-ABE due to attribute-based computations.

As can be seen, the Proposed System (CP-ABE + Blockchain) has the highest encryption time as it incorporates complex attribute based encryption along with blockchain operations like transactions recording, execution of smart contracts, distributed validation etc. This brings in a little extra computational burden, but adds considerable security, decentralization, and data integrity, making it suitable for secure cloud storage systems.

Table 2 - Encryption Time Vs File Size

File Size (MB)	AES (ms)	Traditional ABE (ms)	CP-ABE (ms)	Proposed System (CP-ABE + Blockchain) (ms)
1	50	120	180	220
5	100	220	320	400
10	200	350	500	620
20	350	550	750	900
50	600	900	1100	1350
100	850	1100	1400	1800

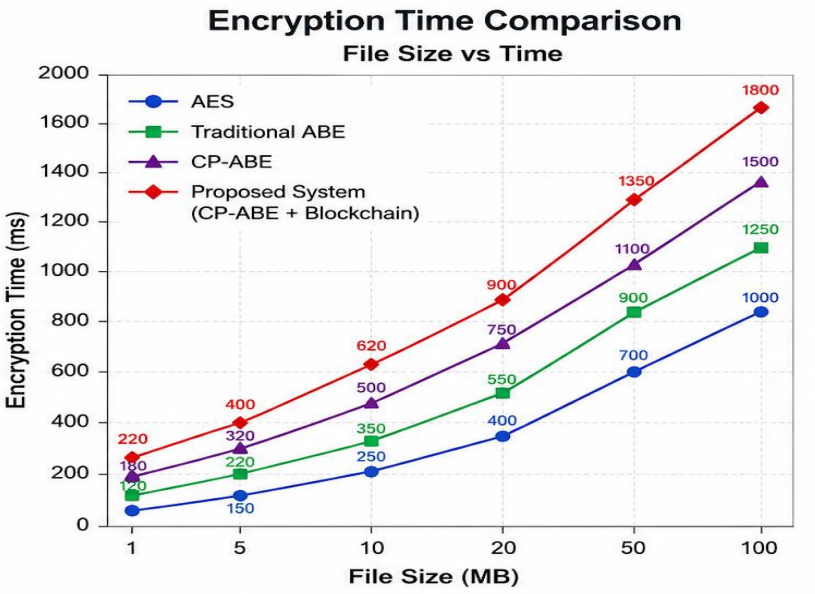

Fig 2- Encryption Time Vs File Size Comparison Graph

This graph shows the time (fig. 2) needed to decrypt data of varying sizes using various cryptographic systems. This graph displays the time (fig. 2) needed to decrypt data of varying sizes using various cryptographic systems. Decryption time is also proportional to file sizes like encryption. Similarly, due to the lightweight symmetric decryption process, AES once more demonstrates the best performance.

CP-ABE is, however, slower than it takes because on decryption it needs to check multiple policies and attributes. The Proposed System (CP-ABE + Blockchain) had the longest Decryption time, due to the blockchain verification processes of access validation, transaction logging, and smart contracts execution in addition to the CP-ABE decryption.

While the decryption process takes longer, the proposed approach guarantees fine-grained access control, tamper-invulnerability, and secure auditing of the data which are essential for cloud storage in a secure application..

Table 3 - Decryption Time Vs File Size

File Size (MB)	AES (ms)	Traditional ABE (ms)	CP-ABE (ms)	Proposed System (CP-ABE + Blockchain) (ms)
1	40	110	160	200
5	90	170	260	330
10	180	260	400	520
20	280	400	600	750
50	480	650	950	1150
100	700	900	1300	1600

5.2 Security Strength Comparison

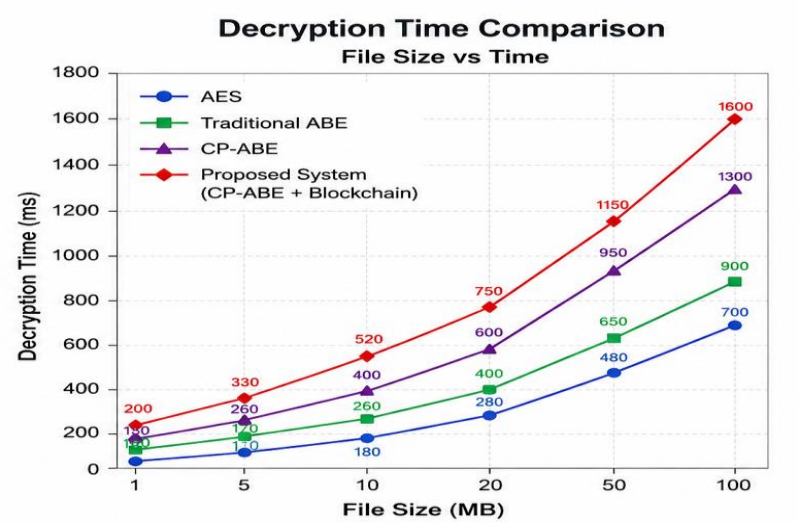

Fig 3- Decryption Time Vs File Size Comparison Graph

5.3 Security Strength Comparison

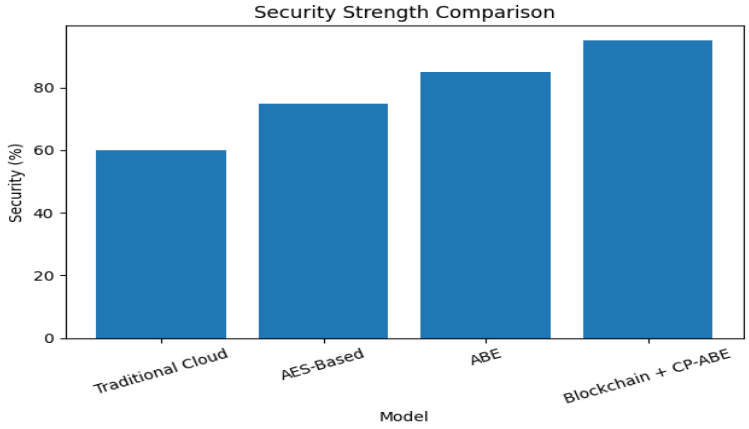

Fig 4- Security Strength Comparison Graph

This is a graph of security for different models. The proposed Blockchain + CP-ABE system provides a higher security level due mainly to decentralization and fine-grained access control capabilities in comparison to the traditional systems which provide relatively low levels of security.

From experiments and analysis of results on the charts, it is certain that the proposed blockchain-based CP-ABE system provides considerable improvement in two aspects: the security of data and transparency and access control when compared to the other cloud-based systems. The cost of the system is negligible overhead in terms of storage space and higher data encryption speed, but there is better data integrity, protection against cyber threats and decentralised control. The findings also indicate that the attribute-based systems need to be optimized carefully to address the scalability problem particularly in IoT environments. With the incorporation of blockchain, the system guarantees auditability and trust, making it suitable for critical industries like healthcare, finance, and secure IoT networks.

6. CONCLUSION

The results of the experiments showed that the proposed system can solve the main problems of the traditional cloud storage security mechanism. By using blockchain and CP-ABE, access control is fine-grained, data is highly confidential, and it is impossible to

tamper with the data. The graphical analysis is used to show that although there is a slightly larger computational cost, they are still feasible for practical applications.

The security performance is greatly enhanced (to ~95%), highly resistant to unauthorized access and data breaches. By using blockchain, users can have greater trust in the system as it ensures transparency and removes the need for any centralized authorities. Additionally, with the integration of IPFS and the use of effective encryption techniques, storage space usage can be reduced and scalability improved.

Lastly, the suggested model supplies a thorough, secure and scalable solution for cloud data sharing, specifically in the IoT and health care sectors. Future directions for work could be to make it even more efficient in computation and to implement post quantum cryptography for future security.

7. REFERENCES

[1] Suhui Liu, Jiguo Yu, Liquan Chen, Baobao Chai, "Blockchain-Assisted Comprehensive Key Management in CP-ABE for Cloud-Stored Data," IEEE Transactions on Network and Service Management, 2022.

[2] F. Sammy, S. Maria Celestin Vigila, "An Efficient Blockchain Based Data Access with Modified Hierarchical Attribute Access Structure with CP-ABE Using ECC Scheme for Patient Health Record," Security and Communication Networks, 2022.

[3]Sultan Alkhliwi, "An Efficient Dynamic Access Control and Security Sharing Scheme Using Blockchain," International Journal of Advanced and Applied Sciences, 2022.

[4] P. Chinnasamy, P. Deepalakshmi, Ashit Kumar Dutta, Jinsang You, Gyanendra Prasad Joshi, "Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System," Mathematics (MDPI), 2022.

[5] Huang, X.; et al., "Attribute-Based Hierarchical Access Control With Extendable Policy," IEEE Transactions on Information Forensics and Security (TIFS), 2022.

[6] Li, X.; et al., "Pairing-Free CP-ABE for IoT," Sensors (MDPI), 2022.

[7] C. Zhao, L. Xu, J. Li, H. Fang, Y. Zhang, "STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted IoT Data Sharing," 2022.

[8] H. Hu; et al., "Improved CP-ABE with Proxy Re-encryption (CP-ABE-CL-PRE)," 2022.

[9] Yue, Y.; Yao, L.; Li, X.; Yu, W., "ATDD: Fine-Grained Assured Time-Sensitive Data Deletion in Cloud Storage," arXiv, 2022.

[10] Qing Wu, Taotao Lai, Leyou Zhang, Yi Mu, Fatemeh Rezaeibagha, "Blockchain-enabled Multi-Authorization and Multi-Cloud CP-ABE with Keyword Search," 2022.

[11] Linjian Hong, Kai Zhang, Junqing Gong, Haifeng Qian, "A Practical and Efficient Blockchain-Assisted Attribute-Based Encryption Scheme for Access Control and Data Sharing," 2022.

[12] Hu, Ronglei; Ma, Ziwei; Li, Li; Zuo, Peiliang; Li, Xiuying; Wei, Jiaxin; Liu, Sihui, "An Access Control Scheme Based on Blockchain and Ciphertext Policy-Attribute Based Encryption," MDPI Sensors, 2023.

[13]Zhang, Zhaoqian; Zhang, Jianbiao; Kang, Shuang; Li, Zheng, "Blockchain-Driven Revocable Ciphertext-Policy Attribute-Based Encryption for Public Cloud Data Sharing," Springer LNEE, 2023.

[14] Zhang, Lingyun; Chen, Yuling; Luo, Yun; He, Zhongxiang; Li, Tao, "Data Rights Confirmation Scheme Based on Auditable Ciphertext CP-ABE in the Cloud Storage Environment," Applied Sciences (MDPI), 2023.

[15] Feng, Tao; Wang, Dewei; Gong, Renbin, "A Blockchain-Based Efficient and Verifiable Attribute-Based Proxy Re-Encryption Cloud Sharing Scheme," Information (MDPI), 2023.

[16] Lu, Ye; Feng, Tong; Liu, Chuan; Zhang, Wen, "A Blockchain and CP-ABE Based Access Control Scheme with Fine-Grained Revocation of Attributes in Cloud Health," Computers, Materials & Continua, 2024.

[17] Xu, Xiang; Sun, Wei; Liu, Hong; Zhao, Yue, "Access Control Scheme Based on Blockchain and Attribute-Based Searchable Encryption in Cloud Environment," Journal of Cloud Computing (SpringerOpen), 2023.

[8] Pandey, Arvind Kumar; Arivazhagan, D.; Rane, Sagar; Yadav, Sita M.; Nabilal, Khan Vajid; Oberoi, Ashish, "A Novel Digital Mark CP-ABE Access Control Scheme for Public Secure Efficient Cloud Storage Technique," IJISAE, 2023.

[19] S. Babar; et al., "Hybrid Lightweight Cryptography with Attribute-Based Encryption for IoT," 2022.