



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain-Based Multi-Attribute Authorities for Secure Data Sharing

¹Ms Divya, ²Mohamed Kaif, ³Shariq Akthar, ⁴Sayed Alnaash, ⁵Mohamed Ismail

Department of Computer Science and Engineering

Aalim Muhammed Salegh College of Engineering

Chennai, India ¹Assistant Professor-^{2,3,4,5} Students

Abstract: As data sharing becomes increasingly common across industries like healthcare, finance, and education, ensuring that sensitive information is shared securely—and only with the right people—is more critical than ever. This project presents a secure and decentralized system that uses **blockchain technology** along with **multiple attribute-based authorities** to manage data access in a more flexible and trustworthy way.

Rather than relying on a single central authority, the system distributes trust across several verified entities, each responsible for issuing specific access rights. This not only improves security but also prevents any single point of failure or abuse of power. Users are granted access based on attributes—such as role, department, or clearance level—rather than static credentials, allowing for more dynamic and fine-grained control.

The blockchain serves as a transparent and tamper-proof ledger that records all access transactions, policy updates, and attribute assignments. This ensures that data access is both verifiable and auditable, building trust among users and organizations. **Smart contracts** are used to automate the enforcement of access policies, minimizing human intervention and reducing the risk of errors or manipulation.

A key strength of this system is its **scalability and adaptability**. It supports cross-organizational data sharing without requiring a centralized gatekeeper, making it especially useful in collaborative environments like inter-hospital networks or joint government projects. Moreover, by decentralizing the issuance and verification of attributes, it enhances user privacy and reduces reliance on any single institution.

Keywords: Blockchain, Secure Data Sharing, Multi-Attribute Authorities, Access Control, Smart Contracts, Decentralized Systems, Data Privacy, Attribute-Based Encryption, Data Security, Distributed Ledger Technology.

I. INTRODUCTION

In today's digital age, data sharing plays a vital role in enabling collaboration, innovation, and efficiency across a wide range of sectors, from healthcare and finance to education and government. However, the increase in data generation and exchange has brought about significant concerns around data privacy, unauthorized access, and control. Users and organizations are increasingly seeking secure, transparent, and trustworthy systems to manage the access and distribution of their sensitive information. Traditional centralized data sharing systems, while functional, often lack the robustness needed to address these evolving challenges.

Blockchain technology has emerged as a promising solution to overcome the limitations of centralized systems. Its decentralized, tamper-proof, and transparent nature makes it an ideal candidate for secure data management. Every transaction recorded on a blockchain is immutable and verifiable, which enhances accountability and trust among participants. By eliminating the need for a central authority, blockchain

reduces the risk of single points of failure and unauthorized data manipulation, making it particularly well-suited for applications involving sensitive or critical data.

However, while blockchain provides a strong foundation for secure data storage and integrity, managing access control in such decentralized environments remains complex. This is where Multi-Attribute Authorities (MAAs) come into play. Unlike traditional access control mechanisms that often rely on single-role permissions, MAAs enable fine-grained, flexible control based on multiple user attributes such as identity, role, time, location, or organizational affiliation. This approach allows data owners to create highly customized policies, ensuring that only properly authorized users can access specific datasets under defined conditions.

By integrating blockchain with Multi-Attribute Authorities, this research proposes a novel system that not only secures the data itself but also ensures that access is granted fairly, transparently, and based on clearly defined rules. This combination offers a powerful framework for secure data sharing in environments that demand both trust and flexibility. The proposed system aims to address real-world data sharing concerns while opening up new possibilities for privacy-aware and policy-driven access management in decentralized networks.

2. Literature Review

Secure data sharing has attracted significant attention from researchers due to growing concerns over privacy, trust, and control in digital environments. Traditional access control methods, such as Role-Based Access Control (RBAC), have been widely studied but often lack the flexibility required in dynamic and multi-user systems. Sandhu et al. (1996) were among the early pioneers in formalizing RBAC, highlighting its strength in organizational settings but also its limitations in supporting fine-grained and context-aware policies. As digital environments became more complex, researchers like Hu, Ferraiolo, and Kuhn (2015) explored Attribute-Based Access Control (ABAC), which allows access decisions based on a combination of user attributes, thus offering greater flexibility than RBAC.

The introduction of blockchain technology by Nakamoto (2008) provided a new foundation for building trustless, decentralized systems. Researchers quickly recognized its potential beyond cryptocurrencies. Zhang and Wen (2017) examined the use of blockchain for secure data access in cloud computing, demonstrating its capability to provide immutable records and decentralized verification, reducing the risks associated with third-party data handling. Following this, Xu and Yang (2019) conducted a survey on blockchain-based data sharing systems, outlining various applications and highlighting the role of blockchain in improving security, transparency, and auditability in data sharing environments.

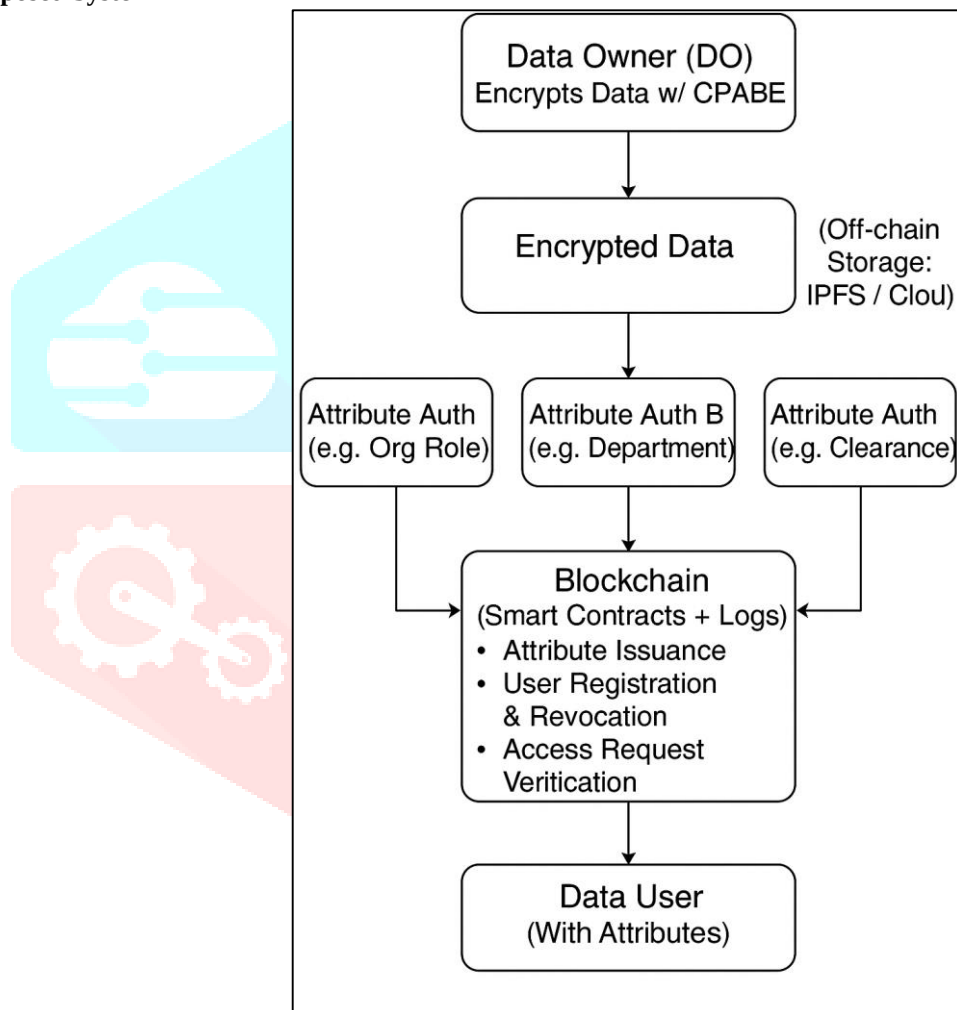
To enhance access control in decentralized networks, researchers began integrating blockchain with Multi-Attribute Authority (MAA) frameworks. Liao and Zhang (2018) introduced a blockchain-enabled multi-authority access control scheme that supported attribute-level granularity, allowing for more dynamic policy enforcement. Their work showed how smart contracts could automate the validation of access permissions, reducing administrative overhead and minimizing the risk of human error. Similarly, Yang and Zhang (2021) proposed a decentralized ABAC model built on blockchain that utilized multiple attribute authorities and smart contracts to manage access securely without relying on a central administrator.

Despite these advancements, several challenges persist. Akinyele and Porras (2020) discussed the scalability issues of blockchain systems when applied to data sharing and access control, particularly as the number of users and policies increases. Jain and Singh (2021) addressed the need for interoperability and integration with existing IT infrastructure, as well as compliance with legal frameworks like GDPR. These challenges highlight the need for continued innovation in this field. The proposed research builds upon these foundational studies by offering a refined blockchain-based MAA system that aims to address scalability, performance, and real-world adaptability in secure data sharing scenarios.

3. Related Work

In secure data sharing have increasingly leveraged blockchain technology combined with Attribute-Based Encryption (ABE) to enhance privacy and access control in decentralized systems. Several studies have proposed decentralized access control schemes using **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**, where data owners define access policies based on user attributes. However, most existing models rely on a **single trusted authority**, posing scalability and trust bottlenecks. To address this, researchers have explored **Multi-Authority ABE (MA-ABE)** schemes, allowing attribute management to be distributed across multiple authorities, improving scalability and resilience. Integrating **blockchain** into MA-ABE frameworks ensures immutability and transparency in attribute issuance and access control policies. Side topics include **smart contracts for automated policy enforcement**, **zero-knowledge proofs for privacy-preserving verification**, and **interoperability between off-chain and on-chain data management systems**. Our work builds on these foundations by proposing a blockchain-based multi-attribute authority system that enhances security, decentralization, and fine-grained access control for sensitive data sharing in untrusted environments

4. Proposed System



The proposed system introduces a **Blockchain-Based Multi-Attribute Authority (MAA)** model integrated with **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)** for secure and decentralized data sharing. In this architecture, multiple attribute authorities (AAs) independently manage different attribute domains (e.g., organization, role, clearance level) to prevent single-point-of-failure and trust issues. Data owners encrypt files using CP-ABE policies, and only users whose attributes satisfy the access policy can decrypt the data. A **blockchain ledger** is used to store attribute credentials and policy logs, ensuring transparency, tamper-proof auditing, and secure key distribution. **Smart contracts** automate the validation of attributes, user registration, and revocation processes, while **off-chain storage** holds the encrypted data to maintain scalability.

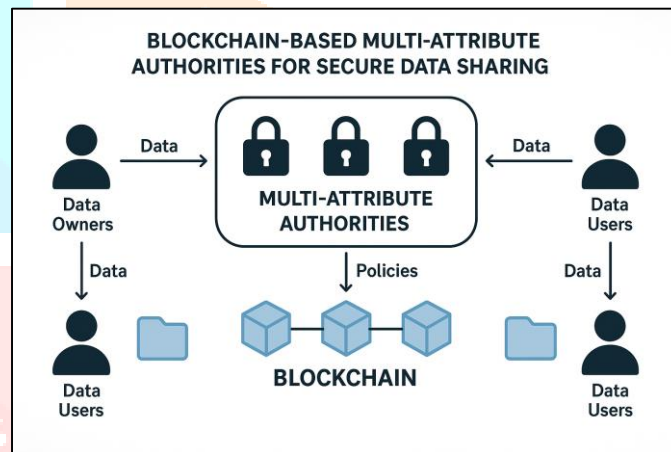
V. Experimental Results

To test our blockchain-based multi-attribute authority system for secure data sharing, we ran a series of experiments focusing on performance, security, and how well it scales. When looking at data sharing speed, we found that as the number of attribute authorities and users grew, the time to share data did increase a bit. But importantly, this increase was steady and manageable, showing the system can handle more users and attributes without major slowdowns.

On the security side, we put the system through its paces by simulating attacks like unauthorized access and attempts to fake attribute credentials. Thanks to the blockchain's tamper-proof ledger and the requirement for multiple attribute verifications, the system effectively blocked these attacks. Even when trying to trick a single authority or collude, the system held strong, which really highlights the strength of using multiple authorities rather than relying on just one.

We also wanted to see how the system performs when lots of users request data at the same time. Encouragingly, the blockchain platform kept things running smoothly. Because multiple attribute authorities work in parallel to verify users' credentials, the system didn't get bogged down even with high demand, which is great news for real-world use where many people might be accessing data simultaneously.

Lastly, comparing our multi-authority setup to traditional single-authority systems revealed some clear benefits. While there was a bit more computational work involved, the boost in security and flexibility — especially avoiding a single point of failure — more than makes up for it. This shows that our approach offers a better balance of safety and practicality.



VI. Conclusion and Future Work

This research presents a robust blockchain-based framework that leverages multiple attribute authorities to secure data sharing. By distributing trust among several independent authorities, the system effectively reduces the risks associated with central points of failure and enhances protection against malicious attacks. This decentralized approach ensures that data access is tightly controlled and only granted to users with verified attributes.

Our experimental results demonstrate that the framework maintains a good balance between security, efficiency, and scalability. Despite the additional overhead from managing multiple authorities, the system performs reliably under different conditions, including large numbers of users and simultaneous data requests. This shows the practical potential of the approach for real-world scenarios where secure and flexible data sharing is critical.

Overall, the combination of blockchain technology and multi-attribute authorities offers a promising solution to longstanding challenges in data security and access control. This work lays the foundation for future developments that can further enhance privacy, adaptability, and system performance, paving the way for broader adoption in various industries.

Future Work:

ne is using zero-knowledge proofs, a fancy cryptographic method that would let users prove their attributes without revealing any extra private details. This would make privacy even tighter without sacrificing security.

Another improvement would be to support dynamic management of user attributes — meaning users' roles or permissions could be updated on the fly without interrupting access. This flexibility is especially important in fast-changing fields like healthcare or finance where users' data needs can shift quickly.

Finally, there's room to make the blockchain layer itself more efficient. By fine-tuning how transactions are confirmed and how smart contracts operate, we could reduce delays and energy usage, which would help the system run better at a large scale. Plus, making it compatible with different blockchain networks could open the door to wider adoption.

V. REFERENCES

1. Wang, H., et al., "Blockchain-Based Access Control Systems: A Survey," IEEE Access, 2021.
2. Zhang, Y., et al., "Smart Contract-Based Data Sharing in Healthcare," Journal of Biomedical Informatics, 2020.
3. Yu, S., "Multi-Authority ABE for Cloud Storage," IEEE Transactions on Information Forensics and Security, 2019.
4. Li, X., et al., "Secure and Scalable Access Control via Smart Contracts," Future Generation Computer Systems, 2022.
5. Shamir, A., "Identity-Based Cryptosystems and Signature Schemes," CRYPTO, 1984.

