North Asian International Research Journal of Sciences, Engineering & I.T.

ISSN: 2454-7514 Vol. 9, Issue-8 August-2023

IRJIF. I.F. : 3.821

Index Copernicus Value: 52.88 Indian Citation Index Thomson Reuters ID: S-8304-2016

NAIRJC

A Peer Reviewed Refereed Journal

DOI: 10.5949/nairjseit.2023.10.8.4

ENHANCED UNIFIED REVOCATION MECHANISM UTILIZING BLOCK CHAIN

B.V.SATISH BABU[1], DR. KARE SURESH BABU[2] & DURGA PRASAD KARE[3]

[1]Research scholar, CSE Dept, JNTUH, Asst Professor, PVPSIT, Vijayawada
[2]Professor of CSE, Department of IT, JNTUH, Kukatpally
[3]Project Delivery Lead, Deloitte Consulting LLP,United States

ABSTRACT

In modern digital information systems, access revocation plays a pivotal role in safeguarding data and ensuring that authorized individuals retain appropriate access privileges. This paper presents a novel approach for unified revocation mechanism which seamlessly integrates blockchain technology and tree data structure to process of different access revocation. This synergistic integration presents a comprehensive solution that markedly enhances the speed and effectiveness of access revocation. Our method's performance is established through a comprehensive and rigorous experimental evaluation. Benchmarking our method against existing approaches reveals significant improvements in response time and a wide range of performance metrics.

***KEYWORD*: Blockchain, Revocation, Encryption, smart contract**

I. INTRODUCTION

Access revocation is a critical aspect of modern information security systems, ensuring that only authorized personnel have access to sensitive data. Existing access revocation methods, however, are limited in their flexibility and effectiveness, typically offering only partial or complete revocation functionalities. To address these limitations, this paper introduces unified revocation method, which combines blockchain technology and auxiliary trees to streamline the process of unified access revocation.

The traditional access control models, such as Role-Based Access Control (RBAC) and Discretionary Access Control (DAC), have limitations in addressing the dynamic and granular access requirements of modern

information systems. To address these limitations, Attribute-Based Access Control (ABAC) and Attribute-Based Encryption (ABE) have emerged as promising approaches to access control and revocation. ABAC provides a flexible and expressive framework for defining access control policies based on user attributes, resource characteristics, and environmental conditions. ABE enables secure data access by encrypting data with attributes and allowing decryption only for users with the corresponding attributes.

Integrating ABAC and ABE with blockchain technology in proposed method furthxer enhanced the security and efficiency of access control and revocation. Blockchain provides a tamper-proof and transparent ledger for recording access control decisions and revocation events. This ensures that access control policies and revocation actions are immutably recorded and cannot be tampered with. Additionally, blockchain enables decentralized and distributed access control management, eliminating the need for a central authority [1].

The proposed method trees to efficiently identify non-revoked users, a crucial aspect of the revocation process. Additionally, it defines two distinct revoke request formats for partial and complete revocation, providing greater flexibility in managing access permissions. A comprehensive comparative analysis is conducted to evaluate the performance of proposed method against existing approaches.

The results demonstrate that the proposed method significantly outperforms existing methods in terms of response time and various performance metrics. This enhanced performance is attributed to the synergistic integration of blockchain technology and auxiliary trees, which enables efficient, secure, and flexible access revocation.

In summary, this paper presents a novel unified approach to access revocation which effectively addresses the limitations of existing methods. By combining blockchain technology and auxiliary trees, the proposed method streamlines the process of multi-scenario access revocation, providing greater flexibility, effectiveness, and security. In the rest of this paper, Section 2 explores blockchain technology, Section 3 delves into the proposed method, Section 4 details the Experimentation and results, Section 5 addresses Future Research Directions, and Section 6 concludes the paper.

II. BLOCKCHAIN TECHNOLOGY

Blockchain technology's underlying mechanism relies on cryptography, specifically hash functions and digital signatures, to ensure data integrity and prevent unauthorized alterations. When a transaction occurs, it is added to a block, which is then linked to the preceding block, forming a chain of blocks. This chain, known as a blockchain, is replicated across the network, ensuring that all participants have a consistent view of the transaction history Figure 1.

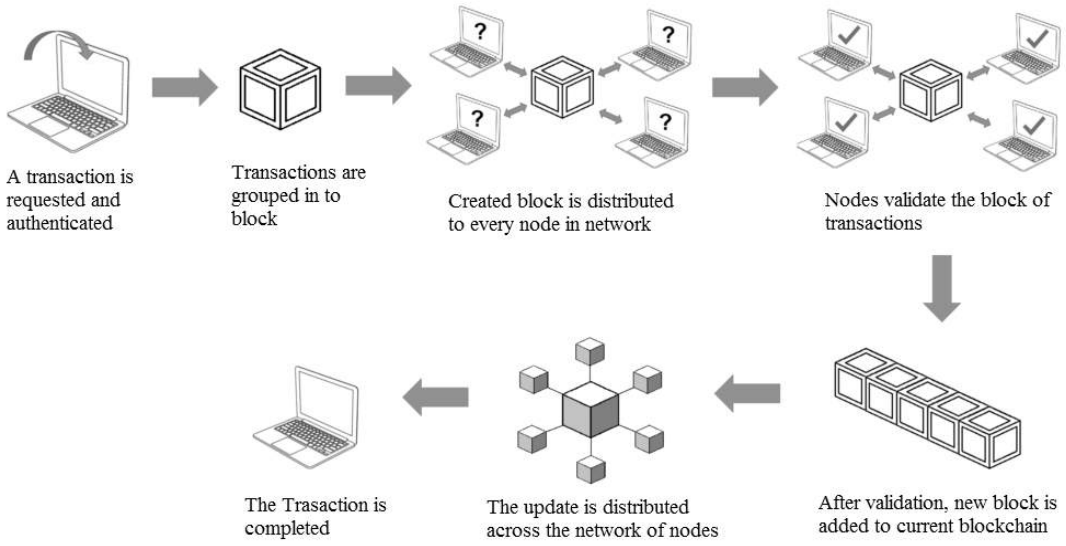


Figure 1. Blockchain Technology

The immutability of blockchain records stems from the cryptographic linkages between blocks. Once a block is added to the chain, it becomes virtually impossible to modify or remove it without altering subsequent blocks. This tamper-proof nature provides a secure and auditable record of transactions, eliminating the risk of fraud or manipulation.

Blockchain technology's potential extends far beyond financial transactions [2]. Its decentralized and secure nature makes it applicable to a wide range of industries, including supply chain management, healthcare, and governance. In supply chain management, blockchain can track the movement of goods and ensure product authenticity, enhancing transparency and efficiency. In healthcare, it can secure patient records and streamline drug distribution processes, safeguarding sensitive information and improving patient care. In governance, blockchain can promote transparency and accountability in public administration, fostering trust and reducing corruption.

While blockchain technology offers immense promise, it also faces challenges, including scalability and regulatory uncertainty. The need to process a growing volume of transactions can strain the network's capacity, potentially slowing down transaction processing. Additionally, the evolving nature of blockchain technology raises questions about regulatory frameworks and oversight, requiring careful consideration and adaptation.

Despite these challenges, blockchain technology is poised to revolutionize the way we interact and transact in the digital world. Its decentralized, secure, and transparent nature offers a foundation for trustless interactions, enabling new business models and empowering individuals to control their data and assets. As blockchain technology matures and its applications expand, it is likely to reshape the global digital landscape, fostering innovation and transforming industries across the spectrum.

III. RELATED WORK

This section reviews recent research on revocation and blockchain for secure data management. The Revocable and Lightweight Access Control method [3] employed CP-ABE and an auxiliary binary tree for revocation. However, to ensure forward and backward security, the ReLAC method introduces significant overhead due to the need for cipher text updates and key generation for each revoked user.

In their study [4], the authors employ concealing policies and revocation, dividing the cipher text into two parts—one for access policy and one for revocation. However, the approach introduces overhead due to cipher text updates. Meanwhile, in [5], the authors focus on attribute revocation, indirectly invalidating users, but the process of updating secret keys leads to higher overhead compared to cipher text updates.

In their study, Yeh et al. [6] employed Merkle tree for user revocation, ensuring the confidentiality of data for revoked users. Nevertheless, their approach of re-encrypting cipher text to maintain data confidentiality resulted in a substantial additional overhead. Hoang et al. [7] for implementing forward-secure access control introduced intricate procedure of cipher text updates necessitates the concurrent updating of non-revoked proofs and decryption keys for users currently possessing the revoked attribute.

A binary tree connected to the user structure is used by the CP-ABE system, which was first shown by [8], to perform user tracing and attribute revocation. This technique has shown to be successful in defending against targeted plaintext attacks and particular access policy scenarios.
Y. Yang et al. [9] suggested a data sharing mechanism in their study that makes use of attribute authority to support attribute revocation.Nevertheless, partial revocation is not supported by their approach. Liang Tan et al. [10] conducted research in which they maintained a trace list for the purpose of directly robbing malevolent users and applying full revocation upon a revocation occurrence. Partial revocation is not achievable with their approach, though.

IV. PROPOSED METHOD

The data owner initiates the revocation process by deploying the Access Control Contract and Revocation Management Contract smart contracts on the Ethereum blockchain network. The ACC receives and evaluates revocation requests from the data owner, and upon receiving a valid request, it forwards the request to the RMC to trigger the revocation mechanism. The detailed steps of this blockchain-based revocation process are depicted in Figure 2.

Upon receiving revocation request from the Access Control Contract, the Revocation Management Contract utilizes {R, A, T} to execute the revocation procedure according to the data owner's specifications. Here, "UID"

denotes the user identifier, and "Action_list" refers to the privileges to be revoked. The RMC smart contract then retrieves required parameters by decrypting the cipher text (CT) previously stored on the blockchain [5]. Subsequently, the RMC applies the following steps to determine revocation

The revocation process incorporates Attribute-Based Encryption (ABE) for secure parameter encryption and decryption, ensuring both forward and backward secrecy [11]. This method utilizes the "Action_list" to execute either partial or complete revocation, setting the

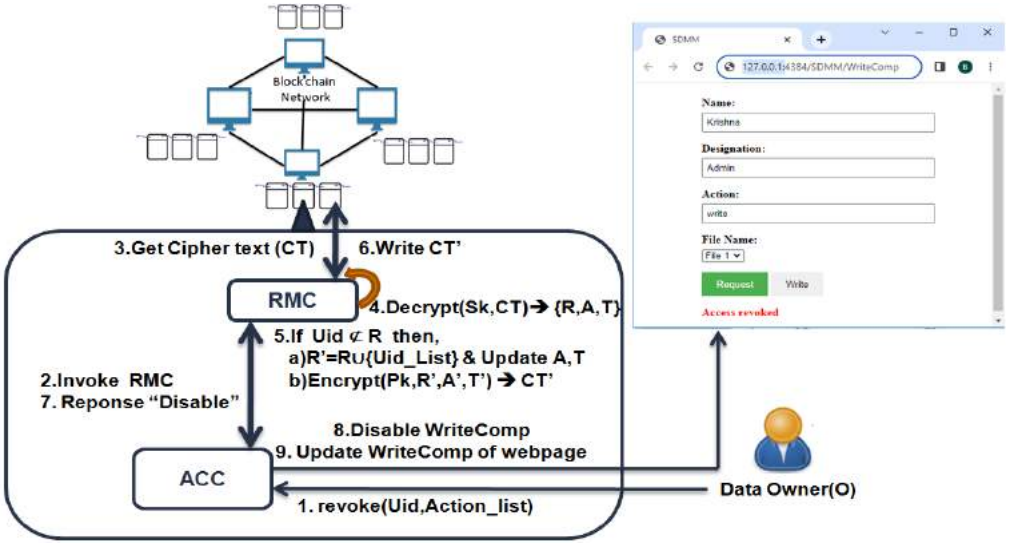


Figure 2. Unified Revocation

"Action_list" as "*" in complete revocation scenarios and limiting it to a subset of actions. For example, in the context of a complete revocation process, suppose the revocation request is with Action_ist => "*" indicating the withdrawal of all user permissions associated with the user ID "UID2." This prompts specific updates within the auxiliary tree, as illustrated in Figure 3.

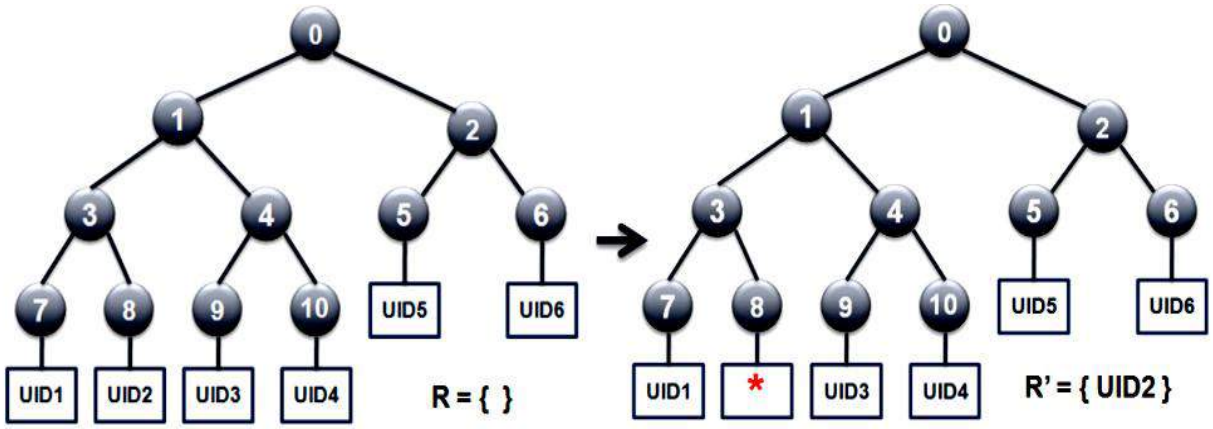


Figure 3. Tree updation

In this revised tree, a leaf node marked distinctly signifies complete revocation, while the remainder of the tree undergoes no alteration. Additionally, after the revocation, adjustments are made to the access policies (A) and the revocation list (R), resulting in A' and R', respectively. Following these modifications, the encrypted values, denoted as cipher text (CT'), are securely recorded on the blockchain. To conclude the revocatisron process, the Access Control Contract transmits a "deactivate" response, updating the relevant components on the webpage.

V. EXPERIMENTATION AND RESULTS

For experimental validation, we configured a local Ethereum blockchain test network with ten nodes using Ganache software, ensuring seamless model operation. Additionally, we developed a user-friendly AngularJS-based WebApp that serves as an interface connecting users with the blockchain network, integrating Web3JS for effective communication with the MetaMask extension, facilitating interaction with the localized Ganache blockchain network.

The comparative assessment among ReLAC[3], TR-AP-CPABE[4], and the proposed method on revocation request validation and acceptance, utilizing performance metrics like "No of revocation requests" and "No of requests validated," is outlined in Figure 4. The revocation request turnaround time refers to the duration it takes for a revocation request to progress through the entire revocation process, starting from its submission to the ultimate fulfillment of the revocation request. Results of the comparison are given in Figure 5.

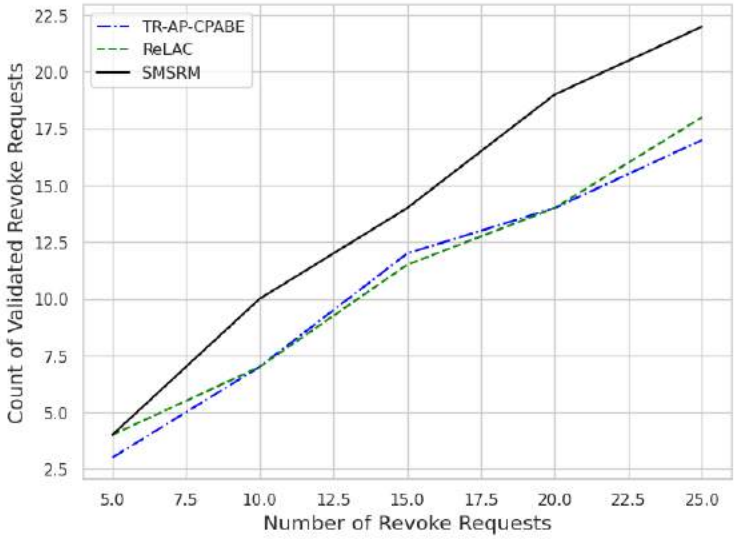
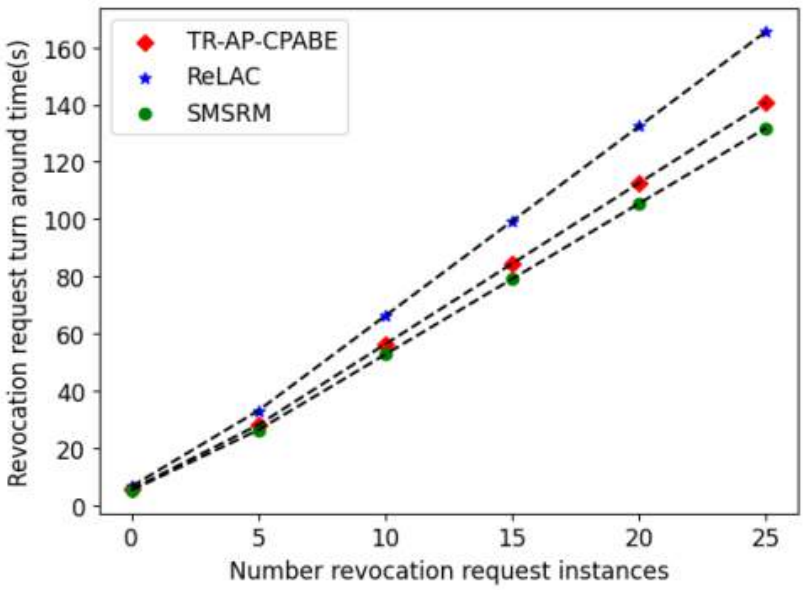


Figure 4. Request validation Figure



5. Request turn-around time

When it come to search time analysis, BFS traversal has been used on a tree with "n" nodes to ascertain the revocation status of a user. Consequently, the time complexity of our method is "O(n)," demonstrating enhanced efficiency when compared to current methodologies. The comparative experimental outcomes for the analysis of search time concerning unrevoked users in both the proposed and existing methods are illustrated in Figure 6.

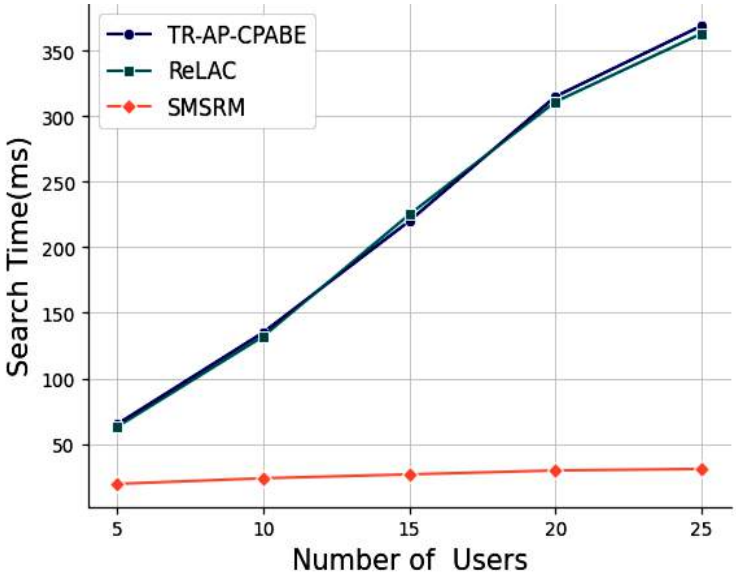


Figure 6. Time analysis

VI. CONCLUSION

Access revocation is a fundamental pillar in modern information systems, ensuring data security and authorizing individuals appropriately. However, the intricacies of access scenarios, encompassing both complete and partial revocations, pose challenges to maintaining efficient and robust controls. To address these challenges, this paper presents an innovative unified revocation method that cleverly combines blockchain technology and auxiliary trees. This integration not only streamlines the multi-scenario access revocation process but also leverages the inherent advantages of blockchain characteristics and auxiliary tree structures for effective management. Through a comparative analysis, we have substantiated the enhanced performance of our approach compared to existing methods.

REFERENCES

[1]. Satish Babu, B.V., Suresh Babu, K. (2020). Materializing Block Chain Technology to Maintain Digital Ledger of Land Records. In: Raju, K., Govardhan, A., Rani, B., Sridevi, R., Murty, M. (eds) Proceedings of the Third International Conference on Computational Intelligence and Informatics . Advances in Intelligent Systems and Computing, vol 1090. Springer, Singapore. https://doi.org/10.1007/978-981-15-1480-7_16

[2]. The “Purview of block chain appositeness in computing paradigms: A survey”., Ingénierie des Systèmes d’Information, Vol. 26, No. 1, pp. 33-46. https://doi.org/10.18280/isi.260104.

[3]. J. Zong, C. Wang, J. Shen, C. Su and W. Wang, "ReLAC: Revocable and Lightweight Access Control with Block chain for Smart Consumer Electronics," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2023.3279652.

[4]. D. Han, N. Pan and K. -C. Li, "A Traceable and Revocable Cipher text-Policy Attribute-based Encryption Scheme Based on Privacy Protection," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 316-327, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2977646.

[5]. G. Xiang, B. Li, X. Fu, M. Xia and W. Ke, "An Attribute Revocable CP-ABE Scheme," 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD), Suzhou, China, 2019, pp. 198-203, doi: 10.1109/CBD.2019.00044.

[6]. L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, “Cloud based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation,” IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 532–544, 2018.

[7]. V. Hoang, E. Lehtihet, and Y. Ghamri-Doudane, “Forward-secure data outsourcing based on revocable attribute-based encryption,” in 15th International Wireless Communications & Mobile Computing Conference, IWCMC 2019, Tangier, Morocco, June 24-28, 2019. IEEE, 2019, pp. 1839–1846.

[8]. S. Wang, K. Guo, and Y. Zhang, "Traceable cipher text policy attribute-based encryption scheme with attribute level user revocation for cloud storage," PLOS ONE, vol. 13, no. 9, pp. 1–23, 09 2018.

[9]. Yifan Yang, Run-hua Shi, Kunchang Li, Zhiwei Wu, Shuhao Wang, Multiple access control scheme for EHRs combining edge computing with smart contracts, Future Generation Computer Systems, Volume 129, 2022, Pages 453-463, ISSN 0167-739X, https://doi.org/10.1016/j.future.2021.11.002.

[10]. L. Tan, K. Yu, N. Shi, C. Yang, W. Wei and H. Lu, "Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Block chain-Empowered Approach," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 1, pp. 271-281, 1 Jan.-Feb. 2022, doi: 10.1109/TNSE.2021.3101842.

[11]. J. Zhang, Y. Xin, Y. Gao, X. Lei and Y. Yang, "Secure ABE Scheme for Access Management in Block chain-Based IoT," in IEEE Access, vol. 9, pp. 54840-54849, 2021, doi: 10.1109/ACCESS.2021.3071031.Lee, S.hyun. & Kim Mi Na, (2008) "This is my paper", ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.