

Streamlined multi-scenario revocation method leveraging blockchain and auxiliary trees

Battula Venkata Satish Babu^{1,2}, Kare Suresh Babu³, Durga Prasad Kare⁴

¹Department of Computer Science Engineering, Jawaharlal Nehru Technological University Hyderabad, Kukatpally, India

²Prasad Vara Potluri Siddhartha Institute of Technology, Vijayawada, India

³Department of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Kukatpally, India

⁴Project Delivery Lead, Deloitte Consulting Limited Liability Partnership, United States

Article Info

Article history:

Received Nov 20, 2023

Revised Dec 11, 2023

Accepted Feb 21, 2024

Keywords:

Access control

Auxillary tree

Blockchain

Revocation

Smart contract

ABSTRACT

Access revocation is a fundamental aspect of modern information systems, ensuring that data remains secure and authorized personnel have appropriate access rights. However, existing access revocation methods address only one type of scenario, offering either partial or complete revocation functionalities but not both, leading to limitations in flexibility and effectiveness. This paper introduces a novel approach called streamlined multi-scenario revocation method (SMSRM) that combines block chain technology and auxiliary trees to streamline the process of multi-scenario access revocation. The SMSRM method defines two separate revoke request formats for partial and complete revocation. Auxiliary trees are used to keep track of non-revoked users, which is very important during the revocation process. In addition, the proposed method utilizes a block chain to record each and every revocation-related operation to provide forward secrecy. Through a comparative analysis, we evaluate the performance of our approach against existing methods. The results highlight that our method performs better in terms of response time and various performance metrics.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Battula Venkata Satish Babu

Department of Computer Science Engineering, Jawaharlal Nehru Technological University Hyderabad
Kukatpally, India

Email: vsatish.phd@mail.com

1. INTRODUCTION

Incontemporary information systems, ensuring data security and regulating who can access it are extremely important. Revocation management is a critical feature of such essential digital security frameworks, playing a significant role in data security by addressing the risks associated with compromised credentials, unauthorized access, and changes in user permissions. It involves promptly revoking or disabling access rights for individuals, devices, or organizations that no longer require or are ineligible to access data resources according to the given policies [1].

Effective revocation management, encompassing both complete and partial revocation, is important for maintaining a dynamic and secure digital environment [2], [3]. Complete revocation terminates all access privileges, especially in response to compromised credentials or critical security incidents, ensuring immediate containment of potential threats. On the other hand, partial revocation adds a layer of granularity to access control, allowing organizations to selectively restrict specific permissions while preserving essential access.

There are several challenges that hinder the effective implementation of revocation management. Existing revocation methods often provide either partial or complete revocation, but not both, limiting the

ability to adapt to specific security scenarios. Operational efficiency of operations like encryption, validation, and revocation request turn-around time remains a challenge, as managing revocation processes across numerous users and devices can be complex and time-consuming. Ensuring forward security [4], which guarantees that past compromises cannot be exploited in the future, poses another challenge. Additionally, the potential for tampering with revocation lists and user operation logs raises concerns about the integrity of revocation mechanisms [5]. Finally, keeping track of unrevoked users can be difficult, especially in dynamic environments with frequent user changes [6].

This paper introduces a novel approach called streamlined multi-scenario revocation method (SMSRM) that directly addresses the aforementioned problems by incorporating the characteristics of blockchain technology [7] and auxiliary trees. The goal is to implement multi-scenario access revocation efficiently and securely. The inclusion of blockchain technology in our approach helps to tackle the tampering issues in traditional access revocation methods [8], [9]. Additionally, attribute-based encryption (ABE) and auxiliary trees enhance this structure by offering an efficient way to organize access rights.

To prove the effectiveness of our approach, we conduct a thorough comparison, measuring our method against existing models. By rigorously evaluating performance metrics such as search time, validation time, and other relevant benchmarks, our study highlights the significant benefits of our approach. The outcomes confirm that our method effectively manages real-world access revocation needs, representing a notable advancement in enhancing information system security.

The upcoming sections of this paper are structured as follows: section 2 includes the introduction to blockchain technology. Section 3 presents a comprehensive review of related work. Section 4 details the proposed method. Section 5 encompasses experimentation and result analysis. Section 6 outlines potential future directions and section 7 provides a concluding summary.

2. BLOCKCHAIN TECHNOLOGY

In a peer-to-peer network, blockchain works by sharing an entire copy of the blockchain with every participant, known as a node. These nodes individually verify and validate transactions without depending on a central authority. The basic structure of a blockchain consists of many blocks, each of which contains a different group of transactions. By using cryptographic hashes, these blocks are connected, forming a chain-like structure [9], [10].

Every block possesses its own individual hash generated by the Merkle tree, timestamp, and chain to the previous block's hash. This internally links the series of blocks and guarantees a sequential arrangement, and establishes a blockchain. When a new transaction happens, it is distributed across the network of nodes. These nodes apply consensus methods like proof of work (PoW) or proof of stake (PoS) to validate the transaction's correctness and achieve consensus on its genuineness [11].

This consensus process is important for preventing double-spending and making sure all nodes unanimously confirm the transaction's legitimacy. After a transaction is validated, it joins other approved transactions to form a fresh block. This block is added to the current blockchain, and its information is distributed across all nodes in the current blockchain network. When a block is inserted into the blockchain, changing or deleting it would require agreement from 51% of the nodes, guaranteeing the blockchain's stability and unchangeable nature.

Due to its decentralized architecture, the blockchain ensures that no single entity or node can have complete control over the blockchain network. As a result, the decentralized nature of blockchain presents significant challenges for malicious individuals attempting to modify the information stored in the blockchain [10]. Figure 1 illustrates a visual representation of the basic ideas and elements of blockchain technology.

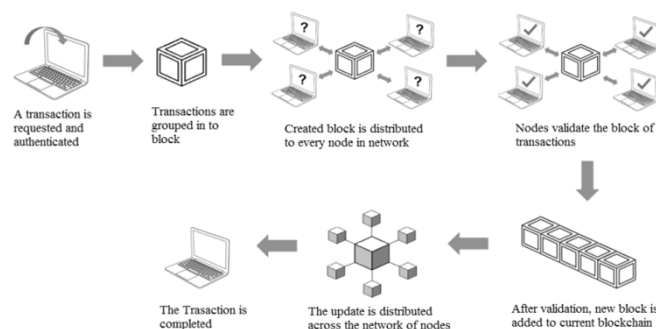


Figure 1. Internal working of blockchain technology

3. RELATED WORK

In this section, we will explore the most recent research works on the ideas of revocation and block chain for the purpose of ensuring secure and efficient management of data. The revocable and lightweight access control (ReLAC) method in [12] utilized cipher text-policy attribute-based encryption (CP-ABE) mechanism along with an auxiliary binary tree for the revocation process. Access policies and revocation list details are stored as cipher text. Nonetheless, to uphold forward and backward security, the ReLAC method introduces a substantial overhead, stemming from the necessity for cipher text updates and key generation for each revoked user.

In their work, Han *et al.* [13] use a CP-ABE scheme for hiding policies and revocation, where cipher text is divided into two parts: one for access policy and one for revocation, only updating the latter during revocation, leading to overhead due to cipher text updates, and key generation for revoked users without specific revocation. Xiang *et al.* [14] carried out attribute revocation, which indirectly invalidates users. However, the task of updating secret keys resulted in higher overhead compared to updating the cipher text.

In their research, Yeh *et al.* [15] used ABE in combination with a Merkle tree for user revocation while upholding data confidentiality for revoked users. However, they applied a method of re-encrypting cipher text to protect data confidentiality, leading to a significant extra overhead for data owners who had to re-encrypt their data each time a revocation period occurred. In their research, Hoang *et al.* [16] created a forward-secure access control system that includes attribute revocation. However, due to the complex process of updating cipher text, the approach also requires updating non-revoked proofs and decryption keys for current users with the revoked attribute.

The CP-ABE system introduced by [17] uses a binary tree linked to the user structure to carry out attribute revocation and user tracing. This method has proven effective in safeguarding against chosen plaintext attacks and specific access policy situations. In their research, Yang *et al.* [18] proposed a data sharing mechanism that supports attribute revocation using attribute authority. However, their method doesn't support partial revocation. In their research, Tan *et al.* [19], a trace list is maintained to directly revoke the malicious users and full revocation is applied on the revocation event. However, in their method, partial revocation is not possible.

4. SMSRM: BLOCKCHAIN BASED REVOCATION

The data owner deploys the access control contract (ACC) and revocation management contract (RMC) smart contracts on the Ethereum block chain network [20]. The ACC is responsible for receiving and evaluating revoke requests from the data owner [21]. Upon receiving a data owner revoke request, the ACC forwards it to the RMC to initiate the revocation process. The entire process of block chain based revocation is illustrated in Figure 2.

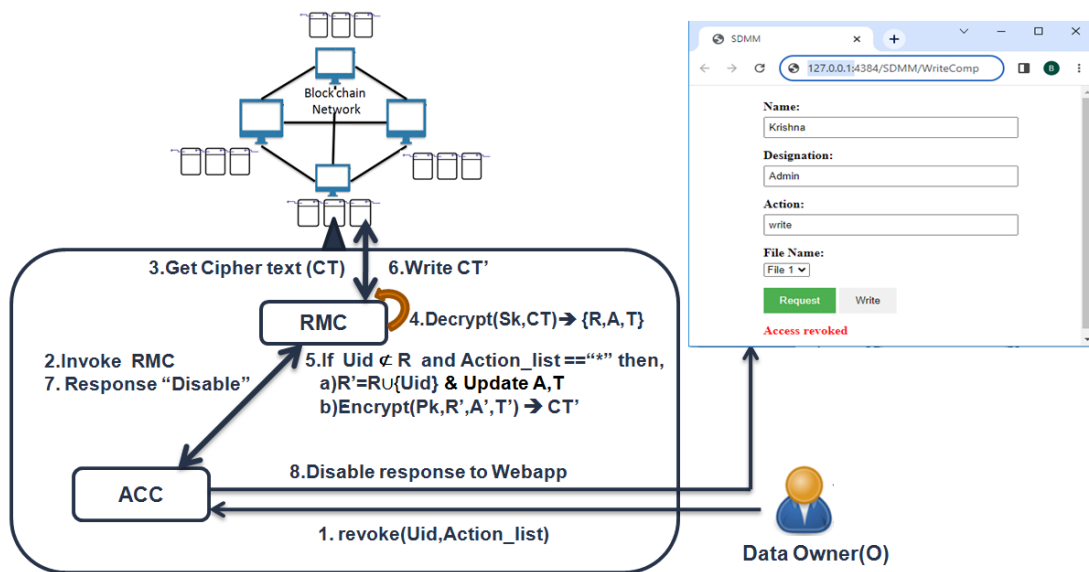


Figure 2. Blockchain based revocation

Every user with access to the resource is assigned a user ID (UID). Auxiliary tree (T) is then constructed using a level-order traversal that incorporates the UIDs of all users with access as leaf nodes within the tree. If the system has $|U|$ users accessing the resource, the auxiliary tree (T) should have a total of $2|U|-1$ nodes [12]. For instance, if $|U|$ equals 5, the auxiliary tree is depicted in Figure 3. Initially, access policies (A), the constructed auxiliary tree (T), and the empty revocation list (R) are encrypted into ciphertext (CT) and then written onto the blockchain.

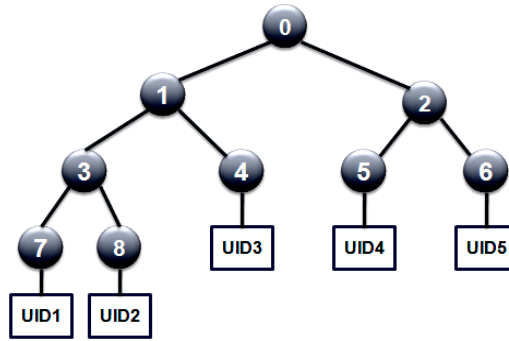


Figure 3. Auxiliary tree (T) for $|U|=5$

The RMC employs $\{R, A, T\}$ to carry out the revocation process in accordance with the data owner's request. Upon receiving data owner(o) revoke request, denoted as $\text{revoke}(\text{Uid}, \text{Action_listACC})$, forwards this request to the RMC. In this context, "UID" represents the user ID, and "Action_list" represents the privileges that are intended to be revoked. The RMC smart contract utilizes the master secret key (Sk) to decrypt the ciphertext (CT) that has been previously written into the blockchain, retrieving $\{R, A, T\}$. Subsequently, RMC applies the following steps to determine revocation.

Algorithm: $\text{Revoke}(\text{UID}, \text{Action_list})$

Input: User ID and List of actions to revoke

Output: Cipher text(CT')

If $\text{Uid} \notin R$ **then,**

a. if $\text{Action_list} = "*" ,$

i. Remove all permissions and update Access policies to A'

ii. Update revocation list to $R' = R \cup \{\text{Uid}\}$

iii. Update Auxiliary tree T to T'

iv. $\text{Encrypt}(Pk, R', A', T') \rightarrow CT'$

b. if $\text{Action_list} \subseteq \text{actions to revoke},$ **then**

i. Remove requested permissions and update A to A'

ii. $\text{Encrypt}(Pk, R, A', T) \rightarrow CT'$

d. Write updated CT' to block chain

e. Send "Disable" response to ACC

f. Update components of webpage

Else: Send "Already Revoked" response to ACC

The revocation algorithm employs ABE to encrypt and decrypt parameters related to revocation, ensuring both forward and backward secrecy [22]. The algorithm mentioned earlier utilizes the "Action_list" to carry out either partial or complete revocation. In the case of complete revocation, the "Action_list" is set to "*" in the revoke request. For partial revocation, the "Action_list" must be a subset of actions, such as {read, write, modify}.

As an example, consider the updating of the auxiliary tree during a complete revocation process: if the revocation request is $\{\text{UID2}, "*" \}$, which signifies the removal of all permissions from the user with the user ID "UID2", the auxiliary tree undergoes the following updates in Figure 4. In the updated tree, a leaf node is marked with an asterisk (*) to indicate complete revocation, while the rest of the tree remains unchanged. Additionally, following the revocation, the access policies (A) and revocation list (R) are updated to A' and R' , respectively. In the subsequent phase, the modified values are encrypted into ciphertext (CT') using the public key (Pk) and recorded on the blockchain. Finally, upon the completion of the revocation process, a "disable" response is transmitted via the ACC to update the components on the webpage.

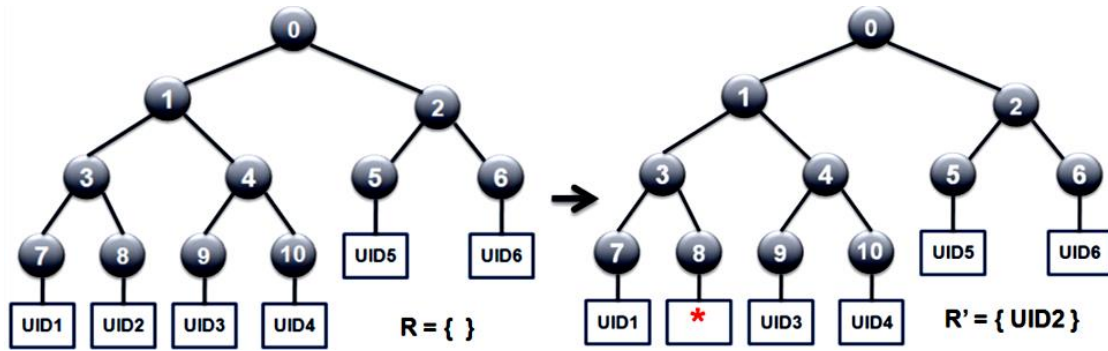


Figure 4. Updation of auxiliary tree

5. RESULTS AND DISCUSSION

For experimental validation, we assessed our model by configuring a local Ethereum block chain test network. This setup with ten fundamental block chain nodes ensured the seamless and effective operation of our model throughout the testing and evaluation phases. We made use of the Ganache software to establish a connection with the local block chain network [23]. Furthermore, we created a user-friendly WebApp using AngularJS, which functions as an interface connecting users with the block chain network.

To create interaction between the WebApp and the block chain network, we have integrated Web3JS into our WebApp [24]. This integration enables us to communicate effectively with the Metamask extension. In turn, Metamask serves as the intermediary for smooth interaction between our WebApp and the localized Ganache block chain network [25].

5.1. Unrevoked user search time analysis

The proposed method has been compared with existing models, namely “ReLAC [12]” and “traceable and revocable cipher text-policy attribute-based encryption (TR-AP-CPABE) [13],” with a primary emphasis on contrasting their individual time complexities. Both of these existing models employ two approaches, cover(R) and path (u), to handle and identify users who have not been revoked. In their suggested approach, the identification of unrevoked users relies on the following operation:

$$k = cover(Revocation_list\ "R") \cap path(user\ "u") \tag{1}$$

The concept of “path (u)” refers to the route from the root node “0” to a specific user leaf node “u” and it takes $O(\log n)$ time. The concept of “cover(R)” refers to the smallest set of nodes required to reach all users not mentioned in the revocation list R and it takes $O(n^2)$ time. After performing intersection(\cap) between the set cover(R) and path (u), if user “u” is not included in the revocation list, there exists a single node k that is shared between cover(R) and path (u). Time complexities of these operations are analyzed in the following Table 1.

Table 1. Operational time analysis

Method	Operation time complexities	
ReLAC [12] and TR-AP-CPABE [13]	Cover(R)	$O(n^2)$
	Path(u)	$O(\log n)$
SMSRM method	Intersection operation	$O(n)$
	Simplified combined time complexity	$O(n^2) + O(\log n) + O(n) = O(n^2)$
		$O(n)$

In our proposed method, we utilize the breadth first search (BFS) traversal operation on a tree consisting of “n” nodes to determine whether a user is unrevoked or not. As a result, the time complexity of our proposed method is “ $O(n)$ ” which offers improved efficiency compared to existing methods. The comparative experimental results for the search time analysis regarding unrevoked users between the proposed and existing methods are presented in Figure 5.

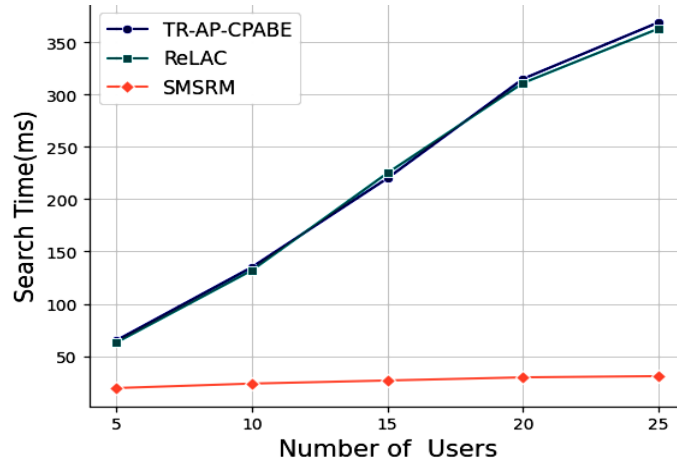


Figure 5. Search time analysis

5.2. Revocation request validation

The existing methods, namely “ReLAC [12]” and “TR-AP-CPABE [13]” support only complete revocation. In contrast, our proposed method supports both partial and complete revocation based on data owner requests. This substantiates that the proposed method offers a more flexible and streamlined approach to revocation assurance for data owners.

To perform a comparative analysis of revocation request validation and acceptance between the existing and proposed methods, we have considered the performance metrics “number of revocation requests” and “number of revocation requests validated.” The results of these metrics are given in Figure 6. The experiment results clearly indicate that our proposed method provides flexible and streamlined revocation request validation. This is due to its support for both complete and partial revocation.

5.3. Revocation request turn around time

Revocation request turnaround time is the time taken for a revocation request to go through the entire revocation process, from its submission to the final completion of the revocation request. This involves various stages of the process, including request creation and propagation, request validation, access policy updates, auxiliary tree updates, time for read and write operations to the block chain, and the time required for encryption and decryption. Assuming the number of access policy rows as “20”, Figure 7 compares the revocation request turnaround time among existing models “ReLAC [12]” and “TR-AP-CPABE [13],” and the proposed method “SMSRM.” The scatter plot below clearly indicates that the proposed method completes the revocation requests with a shorter turnaround time.

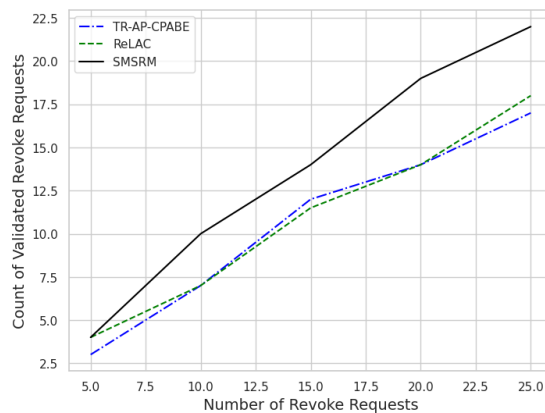


Figure 6. Revocation request validation

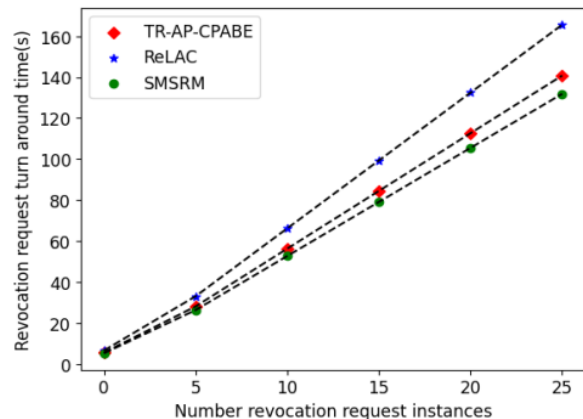


Figure 7. Revocation request turn around time

6. FUTURE RESEARCH DIRECTION

Our future research direction is to concentrate on augmenting the proposed method by refining it with the development of finer-grained and context-aware access control mechanisms. These mechanisms would offer improved forward security and backward security features. In the proposed method, ABE is exclusively employed for the encryption and decryption of revocation-related parameters. In our future studies, we aim to further integrate ABE with additional attribute-related techniques that supports both direct and indirect revocations. This integration is intended to enhance the overall efficiency of access control methods.

7. CONCLUSION

Access revocation stands as a key foundation within contemporary information systems, securing data and ensuring that authorized individuals possess appropriate access privileges. However, the complexity of access scenarios, spanning both complete and partial revocations, introduces challenges to upholding efficient and robust controls. Addressing these challenges, this paper introduces the innovative SMSRM, which ingeniously combines block chain technology and auxiliary trees. This integration not only streamlines the multi-scenario access revocation process but also harnesses the inherent advantages of block chain characteristics and auxiliary tree structures for effective management. Through comparative analysis, we have validated the improved performance of our approach compared to existing methods.





REFERENCES

- [1] C. Daudén-Esmel, J. Castellà-Roca, and A. Viejo, "Blockchain-based access control system for efficient and GDPR-compliant personal data management," *Computer Communications*, vol. 214, pp. 67–87, Jan. 2024, doi: 10.1016/j.comcom.2023.11.017.
- [2] A. Peñuelas-Angulo, C. Feregrino-Urbe, and M. Morales-Sandoval, "Revocation in attribute-based encryption for fog-enabled internet of things: A systematic survey," *Internet of Things*, vol. 23, p. 100827, Oct. 2023, doi: 10.1016/j.iot.2023.100827.
- [3] R. Chen, Y. Li, and R. Rahmani, "Attribute-based Encryption with Flexible Revocation for IoV," *Procedia Computer Science*, vol. 224, pp. 131–138, 2023, doi: 10.1016/j.procs.2023.09.020.
- [4] Y. Lin, X. Wang, Q. Gan, and M. Yao, "A secure cross-domain authentication scheme with perfect forward security and complete anonymity in fog computing," *Journal of Information Security and Applications*, vol. 63, p. 103022, Dec. 2021, doi: 10.1016/j.jisa.2021.103022.
- [5] C. Deng, M. He, X. Wen, and Q. Luo, "Support Efficient User Revocation and Identity Privacy in Integrity Auditing of Shared Data," in *2022 7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, IEEE, Apr. 2022, pp. 221–229, doi: 10.1109/ICCCBDA55098.2022.9778916.
- [6] M. Bouchaala, C. Ghazel, and L. A. Saidane, "TRAK-CPABE: A novel Traceable, Revocable and Accountable Ciphertext-Policy Attribute-Based Encryption scheme in cloud computing," *Journal of Information Security and Applications*, vol. 61, p. 102914, Sep. 2021, doi: 10.1016/j.jisa.2021.102914.
- [7] R. Salama, F. Al-Turjman, C. Altrjman, S. Kumar, and P. Chaudhary, "A Comprehensive Survey of Blockchain-Powered Cybersecurity- A survey," in *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, IEEE, Apr. 2023, pp. 774–777, doi: 10.1109/CICTN57981.2023.10141282.
- [8] K. Kapusta, H. Qiu, and G. Memmi, "Secure Data Sharing with Fast Access Revocation through Untrusted Clouds," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, Jun. 2019, pp. 1–5, doi: 10.1109/NTMS.2019.8763850.
- [9] B. V. S. Babu, K. S. Babu, and D. P. Kare, "BAB-SDMM: Blockchain attribute based secure data management model," *Ingénierie des Systèmes d'Information*, vol. 29, no. 1, pp. 1–8, 2024, doi: 10.18280/isi.290101.
- [10] B. V. S. Babu and K. S. Babu, "The purview of blockchain appositeness in computing paradigms: A survey," *Ingénierie des Systèmes d'Information*, vol. 26, no. 1, pp. 33–46, 2021, doi: 10.18280/isi.260104.
- [11] T. Roy and M. A. Yousuf, "Secure E-commerce Trading Using Blockchain with Smart Contract Based on Proof of Work," in *2022 International Conference on Recent Progresses in Science, Engineering and Technology (ICRPSET)*, IEEE, Dec. 2022, pp. 1–6, doi: 10.1109/ICRPSET57982.2022.10188532.
- [12] J. Zong, C. Wang, J. Shen, C. Su, and W. Wang, "ReLAC: Revocable and Lightweight Access Control with Blockchain for Smart Consumer Electronics," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023, doi: 10.1109/TCE.2023.3279652.
- [13] D. Han, N. Pan, and K.-C. Li, "A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 316–327, Jan. 2022, doi: 10.1109/TDSC.2020.2977646.
- [14] G. Xiang, B. Li, X. Fu, M. Xia, and W. Ke, "An Attribute Revocable CP-ABE Scheme," in *2019 Seventh International Conference on Advanced Cloud and Big Data (CBD)*, IEEE, Sep. 2019, pp. 198–203, doi: 10.1109/CBD.2019.00044.
- [15] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-Based Fine-Grained Health Information Access Control Framework for LightweightIoT Devices with Dynamic Auditing andAttribute Revocation," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 532–544, Apr. 2018, doi: 10.1109/TCC.2015.2485199.
- [16] V.-H. Hoang, E. Lehtihet, and Y. Ghamri-Doudane, "Forward-Secure Data Outsourcing Based on Revocable Attribute-Based Encryption," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, Jun. 2019, pp. 1839–1846, doi: 10.1109/IWCMC.2019.8766674.
- [17] S. Wang, K. Guo, and Y. Zhang, "Correction: Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage," *PLOS ONE*, vol. 13, no. 10, p. e0206952, Oct. 2018, doi: 10.1371/journal.pone.0206952.
- [18] Y. Yang, R. Shi, K. Li, Z. Wu, and S. Wang, "Multiple access control scheme for EHRs combining edge computing with smart contracts," *Future Generation Computer Systems*, vol. 129, pp. 453–463, Apr. 2022, doi: 10.1016/j.future.2021.11.002.
- [19] 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 Blockchain-Empowered Approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1,





- pp. 271–281, Jan. 2022, doi: 10.1109/TNSE.2021.3101842.
- [20] “Deploying and interacting with smart contracts.” [Online]. Available: <https://docs.openzeppelin.com/learn/deploying-and-interacting>, accessed: 2/08/2023.
- [21] W. Dai, C. Wang, C. Cui, H. Jin, and X. Lv, “Blockchain-Based Smart Contract Access Control System,” in *2019 25th Asia-Pacific Conference on Communications (APCC)*, IEEE, Nov. 2019, pp. 19–23, doi: 10.1109/APCC47188.2019.9026509.
- [22] E. H. Nurkifli and T. Hwang, “A Secure Lightweight Authentication Scheme in IoT Environment with Perfect Forward and Backward Secrecy,” in *2022 7th International Workshop on Big Data and Information Security (IWBIS)*, IEEE, Oct. 2022, pp. 113–118, doi: 10.1109/IWBIS56557.2022.9924876.
- [23] N. N. Ahamed and R. Vignesh, “A Build and Deploy Ethereum Smart Contract for Food Supply Chain Management in Truffle - Ganache Framework,” in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Mar. 2023, pp. 36–40, doi: 10.1109/ICACCS57279.2023.10112889.
- [24] “The web3.js - Ethereum JavaScript API.” [Online]. Available: <https://web3js.readthedocs.io/en/v1.10.0/>, accessed: 15/08/2023.
- [25] M. developer Documentation, “Integrate with and extend upon the world’s leading self-custodial crypto wallet.” [Online]. Available: <https://docs.metamask.io/>, accessed: 21/08/2023.

BIOGRAPHIES OF AUTHORS







Battula Venkata Satish Babu     is a research scholar at the Department of Computer Science and Engineering (CSE), JNT University Hyderabad. He is currently working as an assistant professor at Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada. He is a Certified Ethereum Developer, and his research interests include computer networks, data security, big data analysis, and image processing. He can be contacted at email: vsatish.phd@gmail.com.



Kare Suresh Babu     is a Professor of Computer Science and Engineering (CSE) at the Department of Information Technology (IT) at JNT University Hyderabad, CISCO Certified Academic Instructor. He has an impressive publication record, with over 60 research papers published in various national and international journals and conferences. His research interests encompass both computer networking and network security. A significant portion of his work is dedicated to enhancing the understanding, design, and performance of computer networks and their security. This is achieved primarily through the application of routing mechanisms, statistics, and performance evaluation. Notably, he has also focused on improving security mechanisms in mobile ad hoc networks (MANETs) using cross-layer design techniques. He can be contacted at email: kare_suresh@jntuh.ac.in.



Durga Prasad Kare     is a technology enthusiast with more than 18 years of experience. He worked with fortune 500 clients managing large and complex engagements. He is currently working as Technology Leader managing large and complex engagements, Deloitte Consulting, Buffalo Grove, Illinois, United States. He can be contacted at email: durgaprasadllp@gmail.com.