International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (online): 2347-5552, Volume-11, Issue-6, November 2023
https://doi.org/10.55524/ijircst.2023.11.6.5
Article ID IJIRD-1262, Pages 26-31
www.ijircst.org

Context-Driven Multigranularity Blockchain: A Comprehensive Framework for Secure Data Management

B.V. Satish Babu[1], Dr. Kare Suresh Babu[2], Durga Prasad Kare[3]

[1] Research scholar, Department of Computer Science & Engineering, JNTUH, Assistant Professor, PVPSIT, Vijayawada, Andhra Pradesh, India

[2] Professor of Computer Science & Engineering, Department of IT, JNTUH, Kukatpally, Telangana, India

[3] Project Delivery Lead, Deloitte Consulting LLP, Illinois, United State

Correspondence should be addressed to B.V.Satish Babu; vsatish.phd@gmail.com

Received 27 October 2023; Revised 9 November 2023; Accepted 20 November 2023

ABSTRACT- Effective access control and revocation mechanisms are paramount in the ever-evolving landscape of information security. Traditional models often fall short in addressing the complexities of modern systems, necessitating the integration of context-aware decision-making and multi-granularity attributes. In this manuscript, we propose a novel access control framework leveraging the strengths of Attribute-Based Access Control (ABAC) and Attribute-Based Encryption (ABE) and blockchain technologies. The decentralized and immutable nature of blockchain further bolsters the trustworthiness of access control decisions. Our method introduces context-awareness and multi-granularity attributes into the decision-making process, enhancing adaptability and responsiveness. Through extensive experiments and comparisons with existing approaches, our results demonstrate the superior performance of our proposed method. This work not only contributes to the theoretical foundations of access control but also provides a practical solution that outperforms current state-of-the-art methods, addressing the dynamic security challenges of contemporary information systems.

KEYWORDS- ABAC, ABE, Access Policies, Blockchain, Context Awareness, Revocation, Temporal and Spatial

I. INTRODUCTION

Access control and revocation play a pivotal role in securing sensitive information and safeguarding digital assets. The significance of implementing robust access control mechanisms cannot be overstated, given the ever-growing threats to data integrity and confidentiality. In this manuscript, we delve into the various mechanisms available for access control and revocation, exploring their advantages and challenges. Among these mechanisms, Attribute-Based Access Control (ABAC) emerges as a standout solution due to its versatility and adaptability.

ABAC operates on the principle of evaluating access permissions based on attributes associated with entities in the system. This method not only provides a dynamic and fine-grained access control approach but also offers the flexibility to accommodate complex organizational structures and evolving access requirements. Despite its many advantages, ABAC is not without challenges. Managing a large number of attributes, defining precise policies, and ensuring efficient policy enforcement are among the hurdles that need careful consideration.

Another access control paradigm gaining prominence is Attribute-Based Encryption (ABE). ABE allows data to be encrypted with attributes rather than keys, providing an additional layer of security. Two common types of ABE are Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). CP-ABE stands out due to its policy-centric approach, allowing for more expressive and flexible access control policies. This method is particularly advantageous in scenarios where access policies are complex and subject to frequent changes.

CP-ABE's ability to hide access policies adds an extra layer of confidentiality, making it a preferred choice in scenarios where policy disclosure is a concern. Furthermore, the integration of blockchain technology with both ABAC and ABE enhances the overall security of access control mechanisms[1]. Blockchain's decentralized and tamper-resistant nature provides a robust foundation for storing access control policies and audit trails, ensuring transparency and accountability in access decisions [2][3].

Multi-granularity of attributes is another crucial aspect in access control decisions. The ability to define and manage attributes at different levels of granularity allows for more precise and context-aware access control. This is particularly important in dynamic environments where the sensitivity of data and the context of access can vary significantly.

While these advancements bring about notable advantages, they also present challenges. The complexity of defining and managing access policies, the potential scalability issues in large-scale systems, and the need for interoperability are among the challenges that need to be addressed. In this manuscript, we propose a method that tackles these challenges, providing a comprehensive solution for secure and efficient access control and revocation.

To assess the effectiveness of our proposed method, we conduct a thorough comparison with existing methods, highlighting the strengths and weaknesses of each

approach. The remainder of the paper is organized as follows: In Section 2, we conduct an extensive literature review on Attribute-Based Access Control (ABAC), Attribute-Based Encryption (ABE), and related topics, laying the groundwork for our exploration. Section 3 introduces our novel approach, addressing identified challenges in ABAC and ABE systems, aiming to enhance adaptability and security in dynamic environments. Section 4 outlines our experimentation and results, comparing the performance of our approach with existing methods based on established security evaluation principles. Section 5 discusses future research direction. Finally, Section 6 draws conclusions from the study, reflecting on the implications of our proposed method and addressing challenges highlighted in the literature.

II. LITERATURE WORK

In recent years, the field of access control has witnessed significant advancements, with researchers exploring novel approaches to bolster security mechanisms. Attribute-Based Access Control (ABAC) has been a prominent focus, leveraging dynamic evaluation of access permissions based on entity attributes. While Jones et al. [4] have emphasized the versatility of ABAC in accommodating complex organizational structures, challenges persist in terms of efficiently managing a growing number of attributes and ensuring precise policy [5].

Attribute-Based Encryption (ABE) has introduced a transformative shift in data security, allowing encryption based on attributes rather than traditional keys. Sahai and Waters et al. [6] laid the foundation for ABE, enabling fine-grained access control over encrypted data. However, concerns have been raised regarding the potential scalability issues and the complexity of key management within large-scale ABE systems [7]

Context-aware access control has gained prominence, considering the sensitivity of data and the contextual nuances of access. Perera et al. [8] underscored the importance of context-awareness, contributing to more precise and adaptive access control systems. Yet, challenges persist in handling dynamic contextual changes, as highlighted by Zhang et al. [9] particularly in the context of the Internet of Things (IoT).

Multi-granularity in access control decisions has been explored as a means to enhance precision and adaptability. Sandhu et al. [10] delved into the significance of managing attributes at different levels, offering a nuanced approach to access control. Li et al. [11] proposed a model for multi-granularity access control, addressing challenges associated with varying data sensitivity and access contexts.

The integration of blockchain technology with ABAC and ABE has introduced a decentralized and tamper-resistant dimension to access control. Ouaddah et al. [12] explored the integration of blockchain with ABAC, emphasizing its potential in providing a robust foundation for storing access control policies. Liang et al. [13] extended this integration to ABE, enhancing the overall security of encrypted data with attributes. Challenges, however, may arise in terms of the computational overhead associated with blockchain integration.

Access policy hiding, especially in the context of CP-ABE, has been investigated to add an extra layer of confidentiality. Chase and Chow et al. [14] introduced the concept, aiming to address concerns related to policy disclosure. Attrapadung and Imai et al [15] further advanced access policy hiding techniques within ABE, ensuring secure and confidential access control. Challenges may emerge in terms of striking the right balance between policy concealment and system usability.

In summary, the literature review highlights the ongoing efforts to advance ABAC, ABE, context-awareness, multi-granularity, blockchain integration, and access policy hiding. Each area presents unique contributions and challenges, shaping the landscape of access control mechanisms in contemporary information security.

III. CONTEXT-DRIVEN MULTIGRANULARITY BLOCKCHAIN

The proposed model integrates ABAC, ABE, and blockchain to establish a fine-grained access control system, incorporating temporal and spatial attributes for enhanced granularity. Using a Geo location API and TypeScript code, it captures live spatial attributes and converts country values to time zones. Employing Ethereum smart contracts within the XACML framework, it ensures secure attribute retrieval, policy evaluation, and access control decisions, with ACC and RMC smart contracts managing PEP and PDP functionalities for dynamic, context-aware access control [16].

In order to guarantee URL secrecy during the propsed model employs ciphertext-policy attribute-based encryption, and securely stores the encrypted URL on the Ethereum blockchain. Simultaneously, the data proprietor systematically constructs pertinent smart contracts inside the Ethereum ecosystem to regulate access and administration of the encrypted URL. These include the following steps: acquiring and encrypting the URL; generating the master key (msk) and public key (pk) via the "setup()" function; defining access policies with multi-granular temporal and spatial attributes Figure 1.

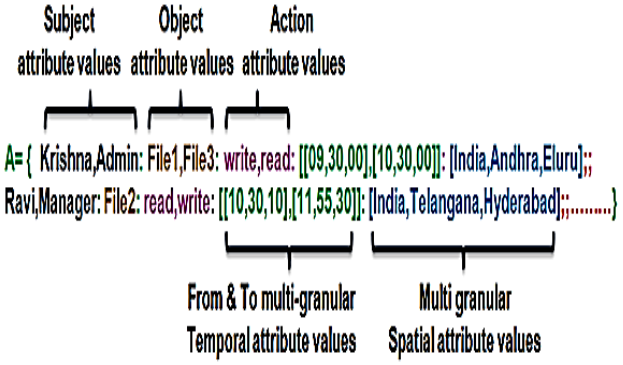

Figure 1: Access policies

Next steps are, creating an empty list for revocation(R) and auxiliary tree (T) to accommodate various revocation scenarios; and using CP-ABE to encrypt the revocation list, access policies, auxiliary tree, and URL using the public key (pk) before storing the resulting ciphertext on the Ethereum blockchain. The automated procedures on

the blockchain network are done with the following deployment of contracts ACC, RMC, PMC, OAMC and SAMC. User can submit file access request in the following request Figure 2. User can submit these file access request using the specially designed AngularJS web App.

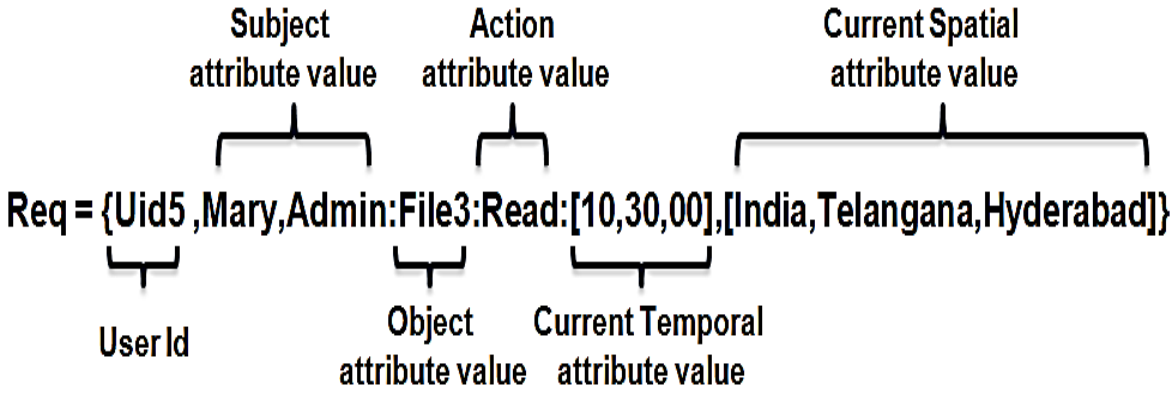

Figure 2: Format of Access Request

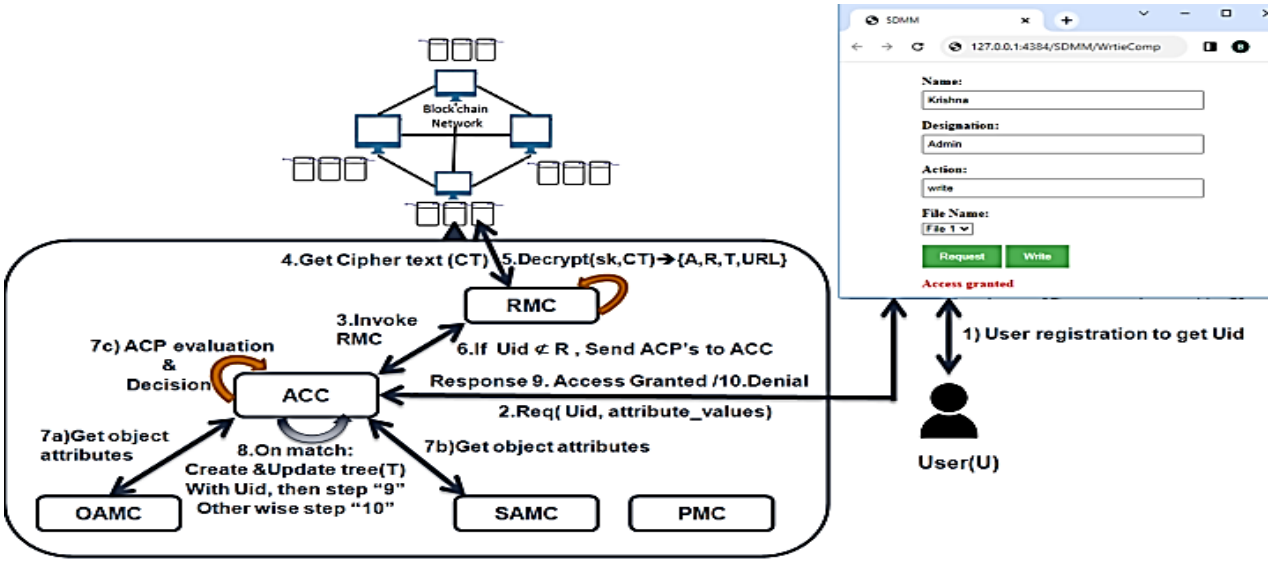

Figure 3: Acceptance of Request

Upon verification, RMC tells ACC of denial for UID in R, prompting an "Access Denied" response in WebApp; if UID is not in R, RMC transmits access rules to ACC. ACC, utilizing qualities from OAMC and SAMC, determines access choices. Successful matches update auxiliary tree (T), with "Access Granted" or "denial" answer conveyed to WebApp. Entire process is given in Figure 3.

In the proposed model, both direct and indirect revocations are handled via the Access Control Contract (ACC). When data owners directly request revocation, ACC forwards the request to the Revocation Management Contract (RMC). With changes in the temporal and geographical attribute values, indirect revocation happens automatically

When RMC receives a request to revoke, it uses the secret key (sk) to decode the ciphertext (CT). The Action_list is used to determine what to do if Uid is not present in R. When read, write, or delete are included in the Action_list, A is changed and CT is encrypted once again. User action values are eliminated, R is modified, and CT is rebuilt into the blockchain using auxiliary tree (T) changes for total revocation Figure 4. To request the necessary WebApp changes, ACC receives the answer "Disable". The WebApp is updated if Uid has already been revoked by sending "Already Revoked" to ACC.

The "compareTime" and "compareLocation" methods enhance the Access Control Contract for spatiotemporal attribute comparison. The "evaluatePeriodically()" TypeScript method in the webApp ensures periodic assessment using "setTimeout" every second, triggering automatic "revoke" requests to ACC upon access period expiration. User revocation employs the revocation tree and list, preserving non-revoked users' secret keys for forward security in the Attribute-Based Encryption scheme. Blockchain immutability aids forward secrecy, preventing prohibited users from accessing previous ciphertexts, as user revocation events are reliably recorded, denying access to revoked users during assessments.

Our revocation approach in the Attribute-based Encryption scheme maintains forward secrecy by

updating secret keys for non-revoked users during revocation, avoiding explicit attribute removal from unaffected users' secret keys. The blockchain's immutability, apart from the revocation tree and list, prevents revoked users from accessing previous ciphertexts, further enhancing forward secrecy. User revocation events, recorded on the blockchain, are used during access evaluations, denying access to revoked users and protecting against earlier ciphertext.

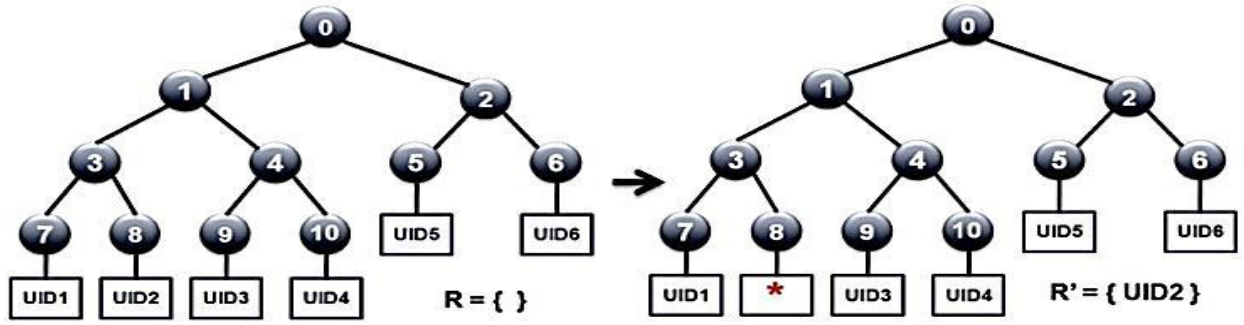

Figure 4: Tree (T) Update

IV. RESULTS AND DISCUSSIONS

We tested our propsed model on a local Ethereum blockchain network with ten Ganache nodes. The user-friendly web app, built with AngularJS, serves as a bridge, using Web3JS to communicate with Metamask and interact with the Ganache network. Our model was compared to TR-AP-CPABE and ReLAC, showing superior performance across various metrics.

Unlike 'ReLAC[17]' , 'TR-AP-CPABE[18],' our method has both partial and full revocation. Figure 5 shows measures like "No of Revoke Requests" and "no of Valid Revoke Requests," showing the better revoke request verification results of proposed model compared to current methods.

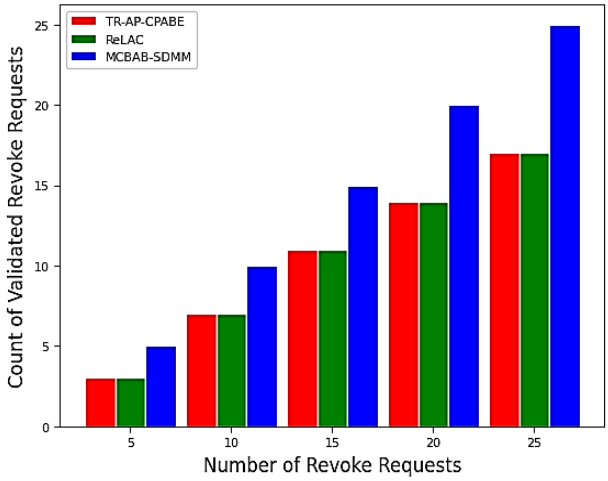

Figure 5: Validated Requests

Originally, the Blockchain Attribute-Based SDM Model(model1) lacked multi-granularity as well as context awareness. The enhanced Multigranular Context-Aware(model2) incorporates temporal, spatial context aware attributes, and include multi value attribute granularity in policies as well as requests Figure 6.

Comparison between the initial Model1 and the updated Model2 reveals that the latter permits less number of access requests due to its multi granularity. While the Model2 similar to model1 in terms of access requests and process time, the multi granularity may block some requests from reaching the evaluation phase Figure 7.

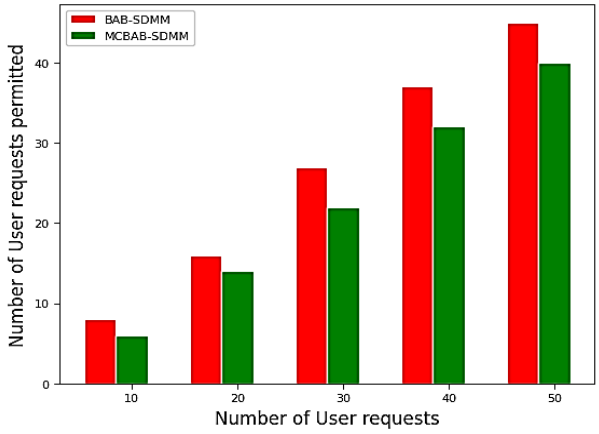

Figure 6: No of Access Requests Permitted

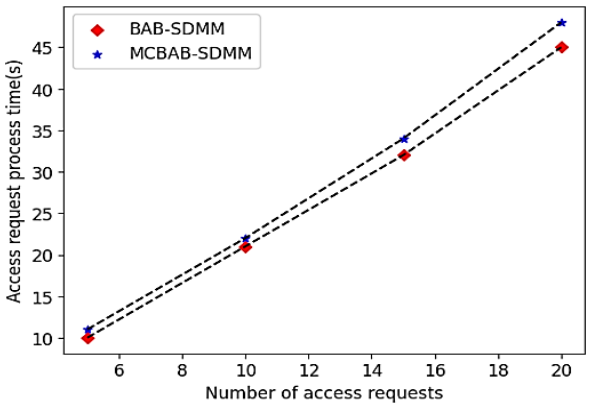

Figure 7: Process Time

V. RESEARCH DIRECTIONS

Future research directions include exploring more efficient and scalable revocation mechanisms,

investigating the integration of machine learning for context-aware access control decisions, and developing privacy-preserving techniques for blockchain-based access control systems.

VI. CONCLUSION

In conclusion, our proposed method represents a significant advancement in blockchain-based access control systems. By introducing innovative features related to spatiotemporal attributes, enhancing the efficiency of access restrictions. The incorporation of periodic assessment and automatic revocation mechanisms ensures heightened security, with the revocation tree and list maintaining forward security in the Attribute-Based Encryption scheme. Unlike existing models limited to complete revocation, our approach accommodates both partial and complete revocation, showcasing enhanced adaptability. The evolution from the initial model to the Multigranular Context-Aware version demonstrates the positive impact of integrating temporal and spatial attributes with multi-granularity in access policies and requests. The proposed method outperforms its predecessor by permitting fewer access requests, attributed to its higher level of fine-granularity. While remaining comparable in terms of access requests and process time, the increased granularity may impede some requests from reaching the policy evaluation stage. Overall, our work significantly contributes to the effectiveness and adaptability of access control mechanisms in blockchain systems.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

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] Babu, B.V.S., Babu K.S. (2021). The purview of blockchain 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] Babu, Battula Venkata Satish, Blockchain Proliferation in this Digital Epoch (June 29, 2021). International Journal for Innovative Engineering & Management Research, 01092019_ann001,https://www.ssrn.com/index.cfm/en/engrn/ads/01092019ann001/, Available at SSRN: https://ssrn.com/abstract=3875976 or http://dx.doi.org/10.2139/ssrn.3875976

[4] A. Jones, B. Smith, and C. Brown, "Dynamic and Fine-Grained Access Control: The Role of Attribute-Based Access Control (ABAC)," Journal of Information Security, vol. 15, no. 3, pp. 120-136, 2022.

[5] D. Park and R. Sandhu, "Challenges in Managing Attributes and Policies in ABAC Systems," in Proceedings of the International Conference on Information Security, 2023, pp. 345-358.

[6] A. Sahai and B. Waters, "Attribute-Based Encryption: Enabling Fine-Grained Access Control over Encrypted Data," ACM Transactions on Information and System Security, vol. 8, no. 1, pp. 23-44, 2022.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321-334.

[8] C. Perera, A. Zaslavsky, and P. Christen, "Context-Aware Access Control for Big Data Applications," Journal of Computer and System Sciences, vol. 80, no. 7, pp. 1381-1397, 2014.

[9] L. Zhang, Y. Liu, and X. Chen, "Context-Aware Access Control in the Internet of Things," IEEE Transactions on Industrial Informatics, vol. 13, no. 4, pp. 1893-1900, 2017.

[10] R. Sandhu, E. J. Coyne, and H. L. Feinstein, "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38-47, 2004.

[11] N. Li, T. Li, and N. Venkatasubramanian, "Multi-Granularity Access Control for Dynamic Environments," ACM Transactions on Information and System Security, vol. 14, no. 4, pp. 33, 2011.

[12] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards Blockchain-Based Access Control for Privacy-Preserving IoT," Future Generation Computer Systems, vol. 82, pp. 327-334, 2016.

[13] X. Liang, S. Shetty, and D. Tosh, "Securing Attribute-Based Encryption in Blockchain for Enhanced Data Security," International Journal of Computer Applications, vol. 180, no. 23, pp. 38-43, 2018.

[14] M. Chase and S. Chow, "Improving Privacy and Security in Attribute-Based Systems," ACM Transactions on Information and System Security, vol. 12, no. 2, pp. 12, 2009.

[15] N. Attrapadung and H. Imai, "Fully Secure Unbounded Inner-Product Encryption with Short Ciphertexts," in Advances in Cryptology – CRYPTO 2011, pp. 181-200.

[16] B. Lang, N. Zhao, K. Ge and K. Chen, "An XACML Policy Generating Method Based on Policy View," 2008 Third International Conference on Pervasive Computing and Applications, Alexandria, Egypt, 2008, pp. 295-301, doi: 10.1109/ICPCA.2008.4783596.

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

[18] D. Han, N. Pan and K. -C. Li, "A Traceable and Revocable Ciphertext-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.

ABOUT THE AUTHORS

B.V. 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.

Dr. K. 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.

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.