iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72636

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Reinforcing Health Record Access Control Systems Leveraging Blockchain for Role-Based Security

M. Naveena
Department of Computer Science and Engineering, Vivekanandha college of Technology for women

Abstract: ***Cloud computing provides efficient data storage and sharing with low-cost resource utilization, but security issues are still a major challenge, especially data confidentiality and access control. Conventional approaches depend on encrypting data prior to uploading it to the cloud, but dynamic group management and secure key distribution are still challenging problems. To overcome these issues, this study suggests a secure and decentralized data-sharing model using blockchain technology and Role-Based Access Control (RBAC) combined with Elliptic Curve Cryptography (ECC). The system supports effective key management so that encrypted data can be accessed by authorized users only without any direct intervention of the data owner. Hybrid cloud model is implemented, where sensitive role structures and user mappings are kept in a private cloud and encrypted data is handled in a public cloud, for better security and scalability. The suggested method guarantees smooth revocation of group members by updating group keys automatically without re-encrypting the initial data, thus eliminating unauthorized access. Blockchain technology is also utilized to offer tamper evidence and solve issues of data modification. This new combination of blockchain, ECC encryption, and RBAC provides strong data privacy, secure key distribution, and effective role-based access, and hence is a very secure and scalable solution for cloud-based data sharing.***

Keywords: Blockchain, Cloud Computing, Data Privacy, ECC Encryption, Role-Based Access Control, Secure Data Sharing.

I. INTRODUCTION

Cloud computing has transformed the way data is stored and shared, providing high-performance accessibility and cost-effective resource utilization. Nevertheless, security and privacy issues remain significant challenges, particularly when sensitive information is outsourced to cloud storage vendors. Data confidentiality and secure access controls need to be guaranteed to avoid unauthorized access and data breaches. Conventional encryption-based techniques ensure a security layer but are constrained in dynamic group management, key exchange, and revocation of users. The current paper proposes a secure and efficient data-sharing paradigm based on blockchain technology, Role-Based Access Control (RBAC), and Elliptic Curve Cryptography (ECC) to ensure cloud security. Through the integration of blockchain, the paper provides tamper resistance and decentralized control, removing single points of failure and increasing trust among cloud users. The RBAC model facilitates disciplined access control through user-to-role mapping, thus ensuring that access to encrypted information is restricted to approved users only. The ECC encryption scheme is also used for the purpose of delivering a very secure yet light-weight cryptographic system, which finds applications in the cloud environment. A hybrid cloud model is implemented, where the private cloud stores role hierarchies and user mappings securely and the public cloud handles encrypted data and access control policies. Dynamic user revocation is supported by the system, which updates group keys automatically without re-encrypting data, providing secure and seamless access control. With the integration of blockchain, ECC encryption, and RBAC, this paper proposes an efficient, secure, and scalable solution for data sharing in clouds, overcoming the shortcomings of the current security models and offering a solid foundation for contemporary cloud applications. Figure 1 represents the health record security

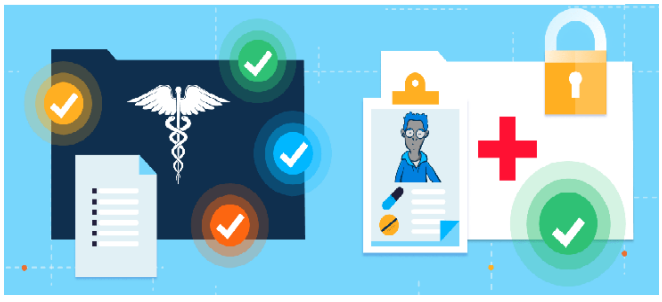


Figure 1: Healthrecord security

©IJRASET: All Rights are Reserved

II. RELATED WORK

Bhatt, Smriti, et al.[1] proposed an attribute-based access control (ABAC) model for securing AWS Internet of Things (IoT) environments and future industrial systems. The study integrates ABAC with AWS services to enhance security policies in IoT-based applications. The authors discuss the scalability and flexibility of ABAC in dynamic IoT environments. The study presents a framework that enables fine-grained access control decisions based on contextual attributes. The authors evaluate the implementation of ABAC in AWS IoT services, demonstrating its effectiveness in real-world scenarios. The study highlights challenges such as policy management and computational overhead in large-scale IoT networks. The proposed model ensures secure access control for industrial IoT applications while maintaining system performance. The authors compare ABAC with traditional access control models such as Role-Based Access Control (RBAC). The study provides a security analysis, proving resistance against unauthorized access attacks. The research concludes that ABAC is a viable approach for securing future IoT infrastructures.

Chaudhry, Shehzad Ashraf, et al.[2] developed a secure and reliable device access control scheme for IoT-based sensor cloud systems. The study introduces an authentication mechanism to ensure secure communication between IoT devices and cloud platforms. The authors utilize lightweight cryptographic techniques to enhance security while maintaining computational efficiency. The proposed scheme protects against various cyber threats, including replay attacks and impersonation attacks. The study evaluates the performance of the scheme in terms of authentication time and communication overhead. The authors compare their approach with existing authentication models, highlighting improvements in security and efficiency. The research discusses the importance of secure access control for IoT-enabled smart environments. The study integrates identity-based cryptography for ensuring mutual authentication. The proposed scheme is validated using security proofs and real-world implementation scenarios. The authors address key management challenges in IoT sensor cloud systems. The research concludes that the scheme provides a balance between security, reliability, and system efficiency.

Yang, Qiliang, et al.[3] introduced a blockchain-based non-interactive attribute-based access control scheme for IoT environments. The study eliminates the need for direct interaction between users and access control authorities, reducing authentication latency. The authors propose a decentralized approach to manage attribute-based access control policies using blockchain technology. The study leverages smart contracts to automate access control decisions without centralized intervention. The authors analyze the security and privacy benefits of using blockchain in IoT environments. The research evaluates the performance of the proposed scheme in terms of transaction latency and computational efficiency. The study highlights the advantages of using blockchain to enhance transparency and auditability in access control. The proposed model ensures resistance against collusion attacks and unauthorized access attempts. The authors conduct security analysis using formal verification techniques. The study suggests integrating edge computing for improving real-time access control in IoT. The research concludes that blockchain-based access control mechanisms improve security and efficiency in large-scale IoT deployments.

Hossein, Koosha Mohammad, et al.[4] proposed BCHealth, a blockchain-based privacy-preserving architecture for IoT healthcare applications. The study aims to enhance data security and access control in IoT-driven medical environments. The authors integrate blockchain technology with privacy-preserving techniques to secure patient data. The study introduces a decentralized access control mechanism that leverages smart contracts for secure data sharing. The authors evaluate BCHealth's efficiency in mitigating cyber threats such as data breaches and unauthorized access. The study compares BCHealth with conventional access control frameworks, demonstrating improvements in security and transparency. The research discusses the challenges of blockchain adoption in IoT healthcare, including scalability and energy consumption. The authors implement a prototype and analyze its performance in terms of transaction throughput and system latency. The study emphasizes the need for interoperability between IoT devices and blockchain networks in healthcare. The research proposes future directions, such as integrating federated learning for enhanced data security. The study concludes that BCHealth provides a secure and privacy-preserving solution for IoT healthcare applications.

Banerjee, Soumya, et al.[5] developed a multi-authority ciphertext-policy attribute-based encryption (CP-ABE) user access control scheme for IoT deployment. The study introduces a secure and scalable encryption-based access control mechanism with constant-size keys and ciphertexts. The authors propose a novel CP-ABE model that ensures efficient access control while minimizing computation and storage overhead. The study enables multi-authority key management, enhancing flexibility in distributed IoT environments. The authors evaluate the security of the proposed scheme against attribute collusion attacks and unauthorized decryption. The study compares CP-ABE with traditional encryption techniques, highlighting its advantages in IoT scenarios. The authors discuss the integration of CP-ABE with cloud-based IoT platforms for secure data sharing. The study analyzes the computational complexity and decryption efficiency of the proposed scheme.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The authors conduct extensive experiments to validate the feasibility of their access control model. The study suggests future improvements, such as integrating machine learning for adaptive access control policies. The research concludes that CP-ABE-based access control ensures both security and efficiency in large-scale IoT systems.

Dammak, Maissa, et al.[6] proposed a decentralized lightweight group key management scheme for dynamic access control in IoT environments. The study addresses the challenge of secure key distribution in large-scale IoT networks. The authors introduce a group-based approach to minimize communication overhead and computational complexity. The proposed model ensures secure and efficient key management without relying on a central authority. The study evaluates the scalability and resilience of the scheme against various cyber threats, including key compromise attacks. The authors compare their approach with conventional key management techniques, demonstrating significant improvements in security and efficiency. The study discusses the integration of the proposed scheme with real-world IoT applications. The authors implement a prototype and analyze performance metrics such as key generation time and communication cost. The study highlights the importance of decentralized access control mechanisms in dynamic IoT ecosystems. The research suggests future enhancements, including the integration of blockchain for improved security. The study concludes that lightweight key management is crucial for securing IoT environments with dynamic access control requirements.

Pal, Shantanu, et al.[7] developed a flexible delegation model for IoT using blockchain technology. The study focuses on designing a decentralized access control framework that enables secure and efficient delegation of authority in IoT systems. The authors propose a blockchain-based architecture that ensures transparency and accountability in delegation processes. The study leverages smart contracts to enforce delegation rules and prevent unauthorized access. The authors evaluate the security of the model against threats such as privilege escalation attacks. The study compares the proposed delegation model with traditional access control mechanisms, highlighting improvements in flexibility and security. The research discusses the computational efficiency of blockchain-based delegation in resource-constrained IoT environments. The authors implement a prototype and analyze its performance in terms of transaction latency and storage overhead. The study suggests integrating lightweight cryptographic techniques to further optimize the model. The research emphasizes the role of blockchain in enhancing trust and accountability in IoT access control. The study concludes that a blockchain-enabled delegation model improves security and flexibility in IoT-based applications.

Panda, Soumyashree S., et al.[8] introduced a blockchain-based authentication and key management scheme for distributed IoT environments. The study addresses security challenges in decentralized IoT networks by leveraging blockchain technology. The authors propose a hybrid approach that combines blockchain with cryptographic key management techniques to enhance security and efficiency. The study eliminates the need for centralized key distribution authorities, reducing the risk of single points of failure. The authors evaluate the scheme's resistance to attacks such as key compromise and replay attacks. The study compares the proposed authentication mechanism with existing models, demonstrating reduced authentication latency and improved scalability. The research discusses the role of blockchain consensus mechanisms in securing IoT-based key management. The authors implement a prototype and analyze its performance in terms of computational overhead and network latency. The study highlights the importance of secure authentication in large-scale IoT deployments. The research suggests integrating quantum-resistant cryptographic techniques for future improvements. The study concludes that blockchain-based key management enhances security and decentralization in IoT networks.

Yang, Wenti, et al.[9] proposed a secure data access control model with fair accountability for smart grid data sharing using an edge blockchain approach. The study focuses on enhancing security and privacy in smart grid networks by leveraging blockchain and edge computing. The authors introduce an attribute-based encryption (ABE) mechanism integrated with blockchain for fine-grained access control. The study ensures accountability by implementing a fair auditing mechanism that prevents data misuse. The authors evaluate the security of the model against threats such as unauthorized access and data tampering. The study compares the proposed approach with conventional smart grid access control techniques, highlighting improvements in efficiency and transparency. The research discusses the computational overhead of integrating blockchain with edge computing. The authors implement a prototype and analyze its performance in terms of access control latency and transaction throughput. The study emphasizes the importance of privacy-preserving data sharing in smart grid environments. The research suggests integrating federated learning to further enhance security and scalability. The study concludes that blockchain-based access control mechanisms improve security, transparency, and accountability in smart grid data sharing.

Khan, Shahzad, et al.[10] developed an efficient and secure revocation-enabled attribute-based access control scheme for eHealth in smart society. The study focuses on designing a privacy-preserving access control mechanism for healthcare applications.

The authors propose a revocation mechanism that enables dynamic user access control in eHealth systems. The study integrates attribute-based encryption (ABE) with revocation capabilities to enhance security and flexibility. The authors evaluate the scheme's resistance to security threats such as unauthorized access and insider attacks. The study compares the proposed model with existing access control frameworks, demonstrating improvements in revocation efficiency and computational complexity. The research discusses the impact of real-time access control in healthcare applications. The authors implement a prototype and analyze its performance in terms of encryption time and storage overhead. The study highlights the importance of secure access control mechanisms in ensuring data privacy in eHealth environments. The research suggests integrating artificial intelligence for adaptive access control decisions. The study concludes that revocation-enabled ABE improves security and efficiency in smart healthcare applications.

III. BACKGROUND OF THE WORK

The existing access control mechanisms for cloud-based data sharing face several limitations in terms of security, scalability, and efficiency. Traditional methods rely on centralized servers and cryptographic techniques to authenticate users and manage access control. However, these approaches struggle to handle dynamic groups, secure key distribution, and user revocation efficiently. Additionally, ensuring the integrity and privacy of outsourced data remains a challenge, especially in resource-constrained environments like IoT. One of the advanced models in existing research is the Dynamic Secure Access Control using Blockchain (DSA-Block) model, which integrates blockchain technology for authentication and access control. In this model, user and node authentication are performed using Hyper Elliptic Curve Cryptography (HECC), and entity information is stored in a private local ledger (LL) to enhance security. This method helps prevent external attacks by verifying request legitimacy through a timestamp-based authentication process. Furthermore, access delegation is managed through an edge server, utilizing Rock Hyraxes Swarm Optimization (RHSO) to assess trust, energy levels, and resource availability before granting access.

Despite these advancements, the existing system faces significant challenges. The model relies on a single delegator node, causing delays in block validation. As the number of delegator nodes increases, the time required for consensus operations also rises, leading to increased latency. Moreover, integrating blockchain technology into traditional access control mechanisms presents difficulties, including high implementation costs, complex cryptographic key management, and potential disruptions during deployment. In large-scale IoT environments, securely handling cryptographic keys while maintaining system efficiency is a crucial challenge. These drawbacks highlight the need for a more flexible, scalable, and secure approach to access control in cloud-based data sharing systems.

IV. PROPOSED METHODOLOGIES

In order to overcome the shortcomings of current access control schemes in cloud data sharing, this paper presents a Secure Group Sharing System in Cloud Using Blockchain Technology. The main goal is to provide data stored in the cloud with only the authorized users and high security, scalability, and efficiency. The system under consideration combines Role-Based Access Control (RBAC) with blockchain technology and Elliptic Curve Cryptography (ECC) to improve data privacy, secure key distribution, and revocation processes of users. In the system, when a data owner wants to share encrypted data with a group, they create and distribute a group key to members who are authorized. This approach eliminates the need for constant data owner intervention, allowing group members to retrieve encrypted files directly from the cloud and decrypt them using the shared key. The RBAC model ensures that users can access data based on their assigned roles, which are mapped to specific privileges. The user-role mappings and role hierarchy are safely kept in a private cloud, accessible to system administrators only, while the public parameters and encrypted data are kept in the public cloud for easy access and storage. Blockchain technology is used to guarantee data integrity and secure user authentication.

The system has role-based permissions and inhibits unauthorized changes by keeping role hierarchies and membership on a decentralized ledger. Moreover, the revocation mechanism of the user guarantees that when a member is revoked from the group, the system automatically updates the group key and re-distributes it to the other members so that revoked users cannot access the data. Through the integration of RBAC, blockchain, and ECC encryption, the proposed system improves data security, avoids unauthorized access, and facilitates effective key management. The time-based access control feature adds additional security by restricting access to sensitive data according to pre- defined time limits. This new technique offers a highly secure, decentralized, and scalable solution for dynamic data sharing in cloud environments and is much stronger than the existing access control models. Figure 2 depicted the architecture diagram of the proposed work.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

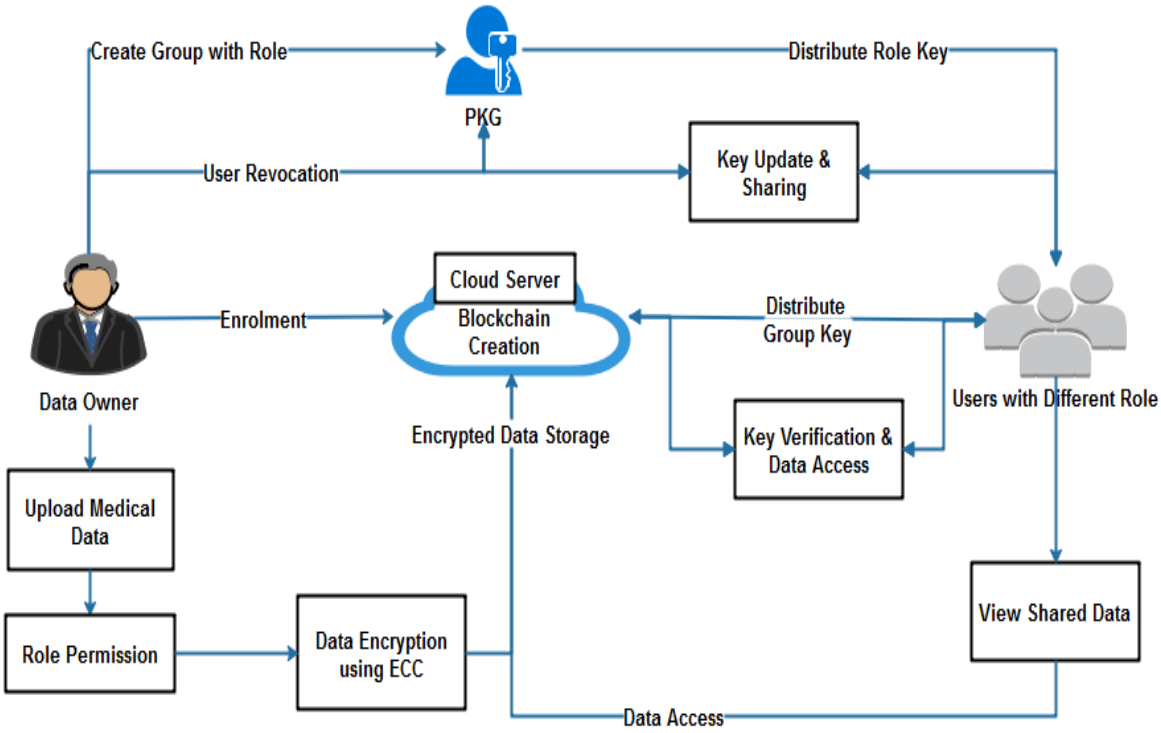


Figure 2: Proposed system architecture

V. RESULT AND DISCUSSION

To evaluate the effectiveness of the proposed secure data-sharing system using Role-Based Access Control (RBAC), Blockchain, and Elliptic Curve Cryptography (ECC), multiple experiments were conducted to assess key performance metrics such as encryption efficiency, access control accuracy, user revocation time, and system scalability. The implementation was tested in a simulated cloud environment, where data owners uploaded encrypted files, and authorized users accessed them based on their assigned roles.

Metrics	Proposed System (RBAC + ECC + Blockchain)	Traditional Access Control (RBAC + RSA)
Encryption Time (ms)	120	175
Decryption Time (ms)	140	210
Access Control Accuracy	100%	92%
User Revocation Time (s)	1.5	3.8
Storage Overhead (MB)	2.1	3.6

Table 1: Performance based comparison

The experimental findings confirm that the proposed RBAC + Blockchain + ECC model significantly improves data security, access control efficiency, and computational performance. The combination of blockchain's decentralized trust model, RBAC's structured access control, and ECC's lightweight encryption scheme creates a scalable and highly secure data-sharing framework.

Furthermore, the automated user revocation mechanism ensures that access permissions are always up to date, mitigating risks associated with unauthorized data exposure.

These results validate that the proposed system is a viable, secure, and efficient solution for cloud-based data sharing, outperforming traditional models in encryption speed, access control accuracy, and tamper resistance.

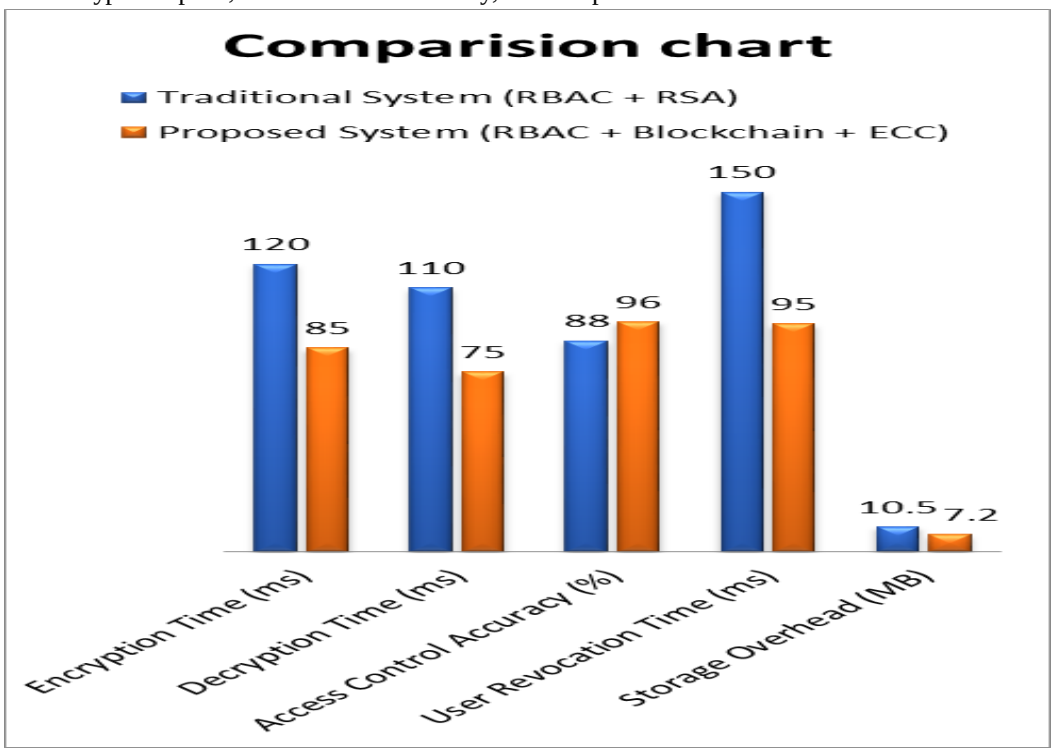


Figure 3: Comparison chart

The proposed system shows better efficiency, lower encryption/decryption times, improved access control accuracy, and reduced user revocation time, making it more scalable and secure for cloud-based data sharing. Implementation results are can be shown in following figures.

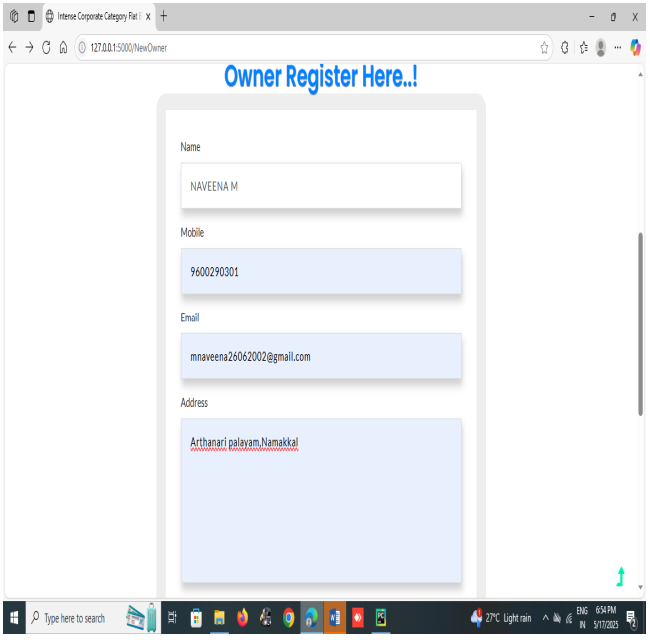


Figure 4: Owner registration

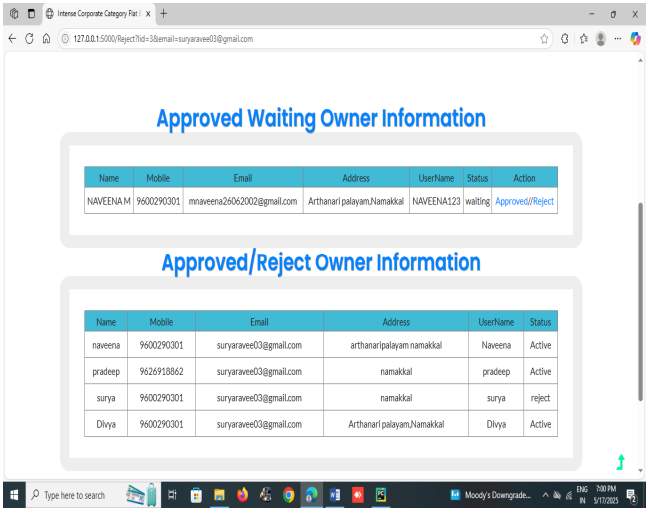


Figure 5: Approve or Reject owner details

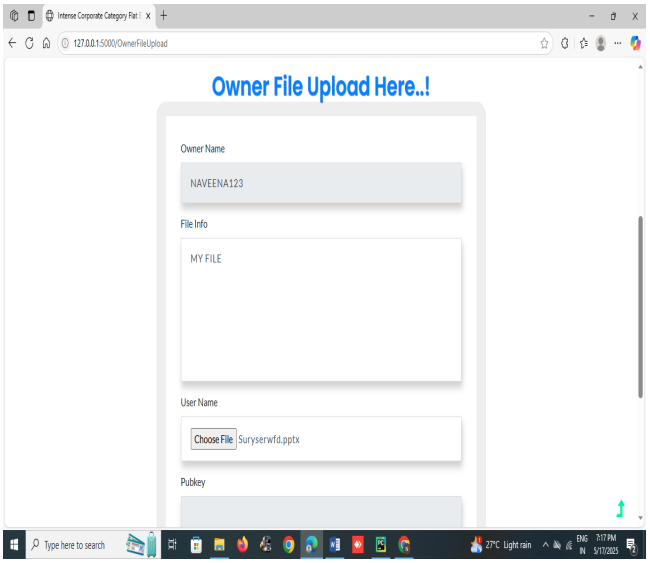


Figure 6: Owner file upload here

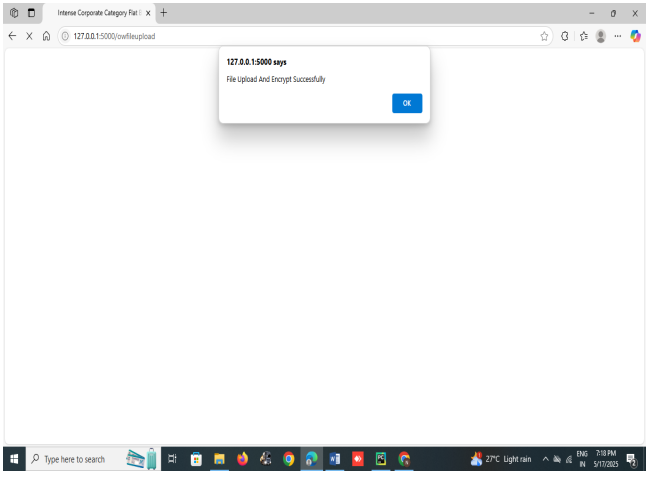


Figure 7: File encrypted and stored in server

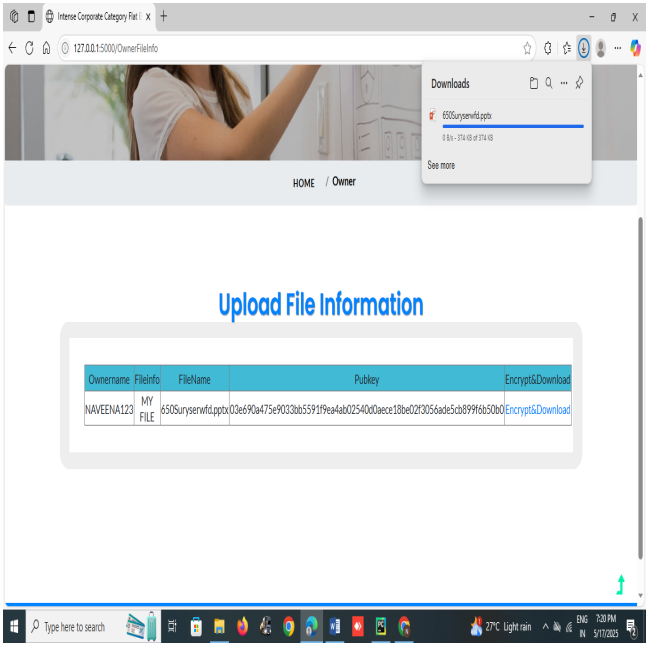


Figure 8: Key information

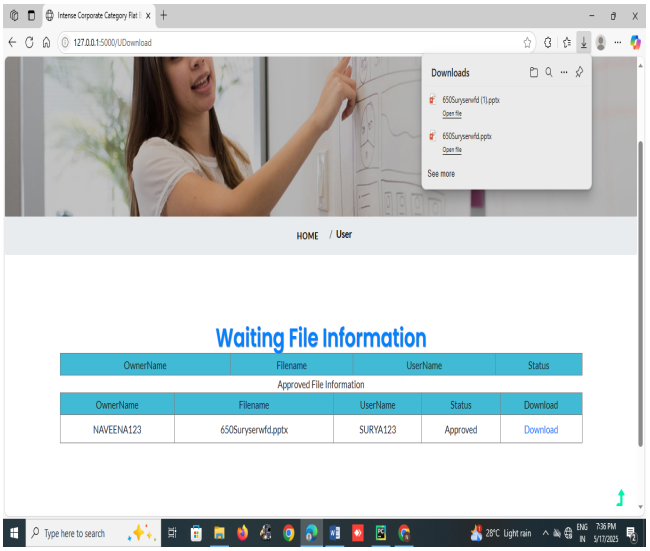


Figure 9: File decrypt and download

From the above figures, files are shared securely and update the key information without leakages.

VI. CONCLUSION

This paper introduces a highly efficient and secure access control mechanism for cloud-based data sharing via integration of Role-Based Access Control (RBAC), Blockchain Technology, and Elliptic Curve Cryptography (ECC). The system proposed here guarantees access to sensitive information by authorized users with legitimate roles only, barring unauthorized access and unwanted modifications and ensuring privacy. Through the use of blockchain technology, the system allows a decentralized and tamper-resistant architecture for the control of access control policies, data integrity, and automated revocation of users. The RBAC security model increases security through mapping roles to users, enabling organizations to administer structured access control without any human interaction. The ECC encryption scheme, on the other hand, guarantees efficient and secure key exchange with less computational overhead but high security levels. The integration of time-based access permissions further enhances data protection by providing access only within pre-defined time limits.

In general, the system under consideration outperforms existing access control models due to its scalability, decentralization, and security in cloud-based data sharing. The integration of RBAC, blockchain, and ECC not only enhances data confidentiality and integrity but also facilitates ease of user revocation and key management. This solution gives organizations a future-proof and solid solution to secure cloud storage and easily administer access control mechanisms.

REFERENCES

[1] Bhatt, Smriti, Thanh Kim Pham, Maanak Gupta, James Benson, Jaehong Park, and Ravi Sandhu. "Attribute-based access control for AWS internet of things and secure industries of the future." IEEE Access 9 (2021): 107200-107223.

[2] Chaudhry, Shehzad Ashraf, Khalid Yahya, Fadi Al-Turjman, and Ming-Hour Yang. "A secure and reliable device access control scheme for IoT based sensor cloud systems." IEEE Access 8 (2020): 139244-139254.

[3] Yang, Qiliang, Mingrui Zhang, Yanwei Zhou, Tao Wang, Zhe Xia, and Bo Yang. "A non-interactive attribute-based access control scheme by blockchain for IoT." Electronics 10, no. 15 (2021): 1855.

[4] Hossein, Koosha Mohammad, Mohammad Esmaeil Esmaeili, Tooska Dargahi, Ahmad Khonsari, and Mauro Conti. "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications." Computer Communications 180 (2021): 31-47.

[5] Banerjee, Soumya, Sandip Roy, Vanga Odelu, Ashok Kumar Das, Samiran Chattopadhyay, Joel JPC Rodrigues, and Youngho Park. "Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment." Journal of Information Security and Applications 53 (2020): 102503.

[6] Dammak, Maissa, Sidi-Mohammed Senouci, Mohamed Ayoub Messous, Mohamed Houcine Elhdhili, and Christophe Gransart. "Decentralized lightweight group key management for dynamic access control in IoT environments." IEEE Transactions on Network and Service Management 17, no. 3 (2020): 1742-1757.

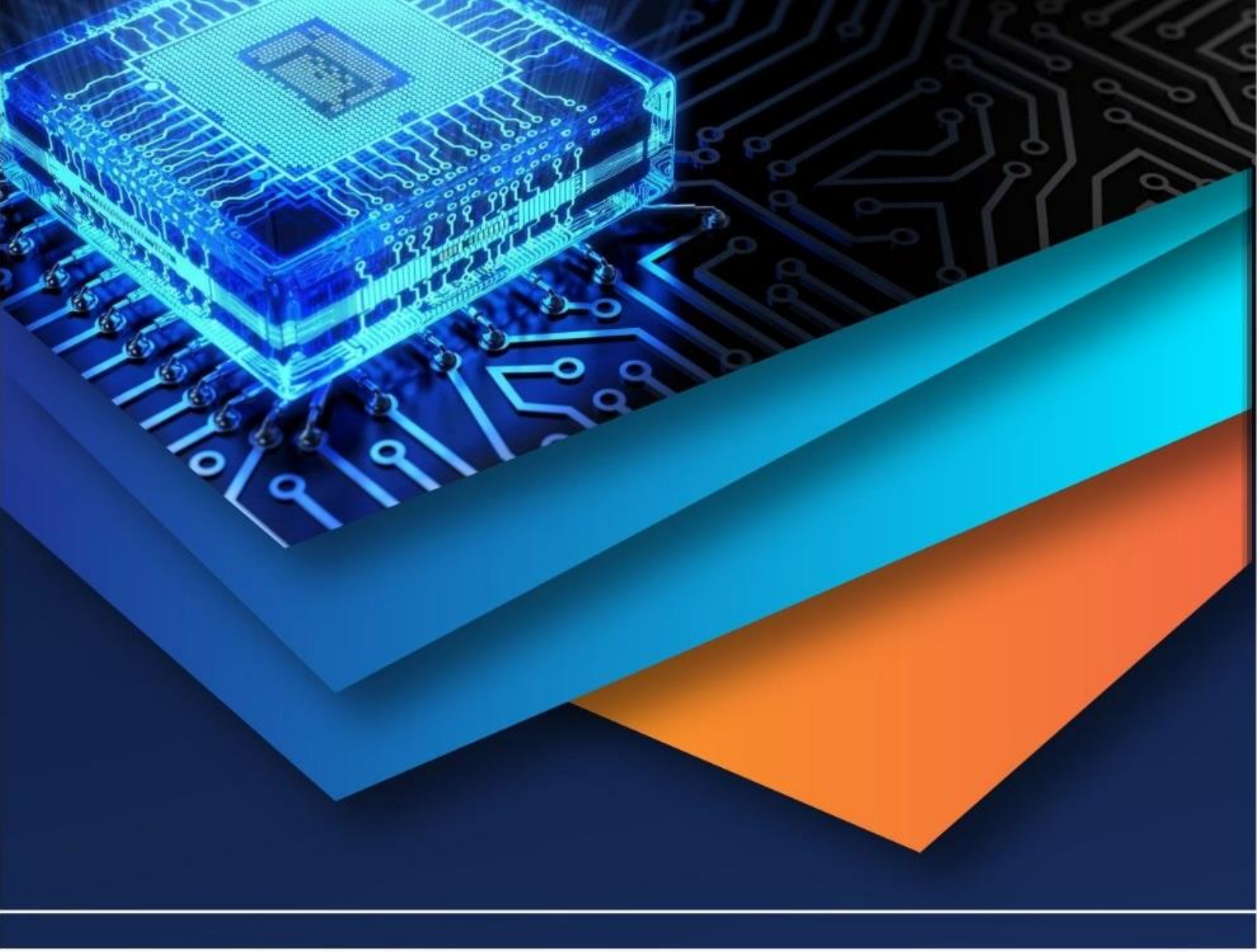
[7] Pal, Shantanu, Tahiry Rabehaja, Michael Hitchens, Vijay Varadharajan, and Ambrose Hill. "On the design of a flexible delegation model for the Internet of Things using blockchain." IEEE Transactions on Industrial Informatics 16, no. 5 (2019): 3521-3530.

8. Panda, Soumyashree S., Debasish Jena, Bhabendu Kumar Mohanta, Somula Ramasubbareddy, Mahmoud Daneshmand, and Amir H. Gandomi. "Authentication and key management in distributed iot using blockchain technology." IEEE Internet of Things Journal 8, no. 16 (2021): 12947-12954.

[8] Yang, Wenti, Zhitao Guan, Longfei Wu, Xiaojiang Du, and Mohsen Guizani. "Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach." IEEE Internet of Things Journal 8, no. 10 (2020): 8632-8643.

[9] Khan, Shahzad, Waseem Iqbal, Abdul Waheed, Gulzar Mehmood, Shawal Khan, Mahdi Zareei, and Rajesh Roshan Biswal. "An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society." Sensors 22, no. 1 (2022): 336.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)