IRJCS: International Research Journal of Computer Science
Volume 12, Issue 04, April 2025
ISSN: 2393-9842
https://www.irjcs.com/archives

Auth Privacy Chain: A Blockchain-based Access Control Framework With Privacy Protection

Thrishula N T, Vasanth A, V Shricharan
Computer Science and Engineering, Vemana Institute of Technology
Bengaluru, India
thrishulant1@gmail.com, vasanthappaji00@gmail.com
shricharanbhat79@gmail.com
Veena G
Assistant Professor, Vemana Institute of Technology
Bengaluru, India
veenag@vemanait.edu.in

Publication History
Manuscript Reference: IRJCS/RS/Vol.12/Issue04/APCS10087 | Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.12/Issue04/APCS10087 Received: 06, April 2025, Revised: 12, April 2025 Accepted: 21 April 2025 Published Online: 05 May 2025 http://www.irjcs.com/volumes/Vol12/iss-04/07.APCS10087.pdf
Article Citation:Thrishula,Vasanth,Scricharan,Veena(2025). Auth Privacy Chain: A Block chain-Based Access Control Framework with Privacy Protection. IRJCS: International Research Journal of Computer Science, Volume 12, Issue 04 of 2025 pages 154-159 **doi:>** https://doi.org/10.26562/irjcs.2025.v1204.07
BibTeX Veena@2025Auth

Abstract: Scalable and adaptable services are provided via cloud computing, which also drastically lowers customer expenses. Notwithstanding these benefits, the centralized architecture of the cloud creates risks such potential data breaches, insider threats, and illegal data access. Single points of failure plague traditional access control systems, which mainly rely on central authority verification. Furthermore, the dynamic requirements of contemporary cloud applications are frequently not met by static access control mechanisms. Systems that guarantee sensitive data privacy and safe access are becoming more and more in demand from users. Decentralized, dynamic, and privacy-enhancing solutions are essential as cloud computing's size and complexity increase. Because decentralized architectures like blockchain provide transparency, immutability, and resilience to manipulation, they present a possible substitute. AuthPrivacy Chain was developed in response to these characteristics.

Keywords: Blockchain, Access Control, Privacy Protection, Smart Contracts, Face Recognition, Time-based Access Revocation

I. INTRODUCTION

Cloud computing explosive expansion has fundamentally changed how people and organizations access and handle data. An alluring substitute for conventional on-premises data management solutions, cloud services provide highly scalable and affordable on-demand computing resources. However, protecting sensitive data has grown to be a major worry as cloud environments continue to grow. Cloud computing frequently uses centralized access control systems, which are inherently vulnerable in a number of ways. These systems are frequently vulnerable to single points of failure, data breaches, and insider attacks. The usage of a central authority for user authentication and authorization in traditional approaches might lead to bottlenecks and make users a possible target for bad actors. A promising answer to these problems is provided by blockchain technology. Because blockchain technology is decentralized, it does not require a central authority, making access control systems more impervious to attacks. Additionally, blockchain offers immutability and transparency, which makes it a great option for protecting private data in cloud settings. But while as blockchain increases accountability and security, it also raises new issues, especially in the area of privacy. All participants may be able to view transaction data on public blockchains, which would not be ideal in situations where user identities and actions must be kept private. In this work, we provide Auth Privacy Chain, a unique access control framework that uses blockchain technology to offer safe and private access management. In order to automate access revocation and solve major issues like unlawful access and privacy concerns, the system integrates decentralized identity management, face-based authentication, and smart contracts. Auth Privacy Chain hopes to offer a scalable, transparent, and safe cloud access control system that also protects user privacy by combining these technologies.

II. LITERATURE SURVEY

In recent years, the idea of employing blockchain technology for access control has drawn a lot of interest, with numerous studies examining how it might be able to get around the drawbacks of conventional centralized systems. For example, Zhang et al. (2019) presented a blockchain-based architecture that used smart contracts to decentral allow access in order to facilitate safe data sharing in industrial Internet environments. By using this method, data owners were able to keep control over who had access to their resources without depending on a centralized authority. Similarly, BacCPSS, a privacy-preserving blockchain approach for Cyber-Physical-Social System (CPSS) big data, was presented by Wang et al. (2020).

By using symmetric encryption to manage access privileges, their method made sure that private information was safe even when it was shared over a decentralized network. To handle access control in certain situations, including cloud storage systems and the Internet of Things (IoT), a number of alternative frameworks have been developed. A blockchain-based access control system was created by Yan et al. (2018) for Internet of Things applications where availability and scalability were major considerations. They gave an example of how blockchain technology could be applied to contexts with limited resources and high dispersion to offer safe access control. A decentralized storage access strategy was developed by Lei et al. (2020) to reduce the dangers of key abuse and privacy leaks in cloud environments. Their system improved transparency by utilizing the immutability of blockchain technology to provide auditable and traceable data access. Blockchain-based access control systems have seen encouraging advancements, but there are still a number of obstacles to overcome. Scalability is a big issue, especially with public blockchains where network congestion can cause processing times and transaction fees to rise sharply. Additionally, privacy concerns pertaining to access control rights and the storage of biometric data must be addressed. Sensitive user data is exposed because many current frameworks ignore the necessity of privacy-preserving authentication procedures.

III. SYSTEM ANALYSIS

The majority of access control systems in use today are centralized, with trusted third parties handling user authorization and authentication. These systems usually use techniques like Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), in which user attributes or roles are used to determine access permissions. However, there are serious security vulnerabilities associated with these conventional systems. Potential sites of attack for malevolent actors are created by the central storage of private user data, including passwords and biometric data. Furthermore, because this system depends on a central authority, any intrusion could result in extensive data breaches. The absence of transparency is a significant weakness in centralized systems. Most of the time, the data owner cannot audit the decision-making process used to give or restrict access, which erodes responsibility and trust. Blockchain provides a solution to this issue with its immutable and decentralized ledger. It guarantees that all actions are transparent and unchangeable once they are recorded on the blockchain by logging user activity and access control decisions. Blockchain does not, however, automatically resolve privacy issues, even though it increases security by decentralizing access control. By their very nature, public blockchains make transaction data—including potentially sensitive data about user identities and access rights—available to all participants. In order to maintain the confidentiality of users' personal information while utilizing blockchain's security characteristics, privacy-preserving technologies like encryption and cryptographic algorithms must be integrated.

IV. PROPOSED SYSTEM

A new access control framework called Auth Privacy Chain combines privacy-preserving authentication methods with the benefits of blockchain technology. The technology is made to protect users' privacy by limiting access to cloud resources to authorized users only. Each user is represented by a distinct blockchain address in this decentralized identity management system. Users can take charge of their own identities with this method, which does away with the necessity for centralized authentication systems. Only authorized parties can view or alter access control permissions since they are encrypted and recorded on the blockchain. Integrating face-based authentication is one of Auth Privacy Chain's primary advances. For reliable facial identification, the system uses the Local Binary Patterns Histogram (LBPH) method. By successfully identifying users without keeping their biometric information in a central database, this system reduces the possibility of data breaches. The access control procedure is further secured by the facial recognition system, which makes sure that only authorized users are able to authenticate themselves. Automatic access revocation is another important aspect of Auth Privacy Chain. To make sure that rights are time-bound, the system can use smart contracts to automatically revoke access after a specified amount of time.

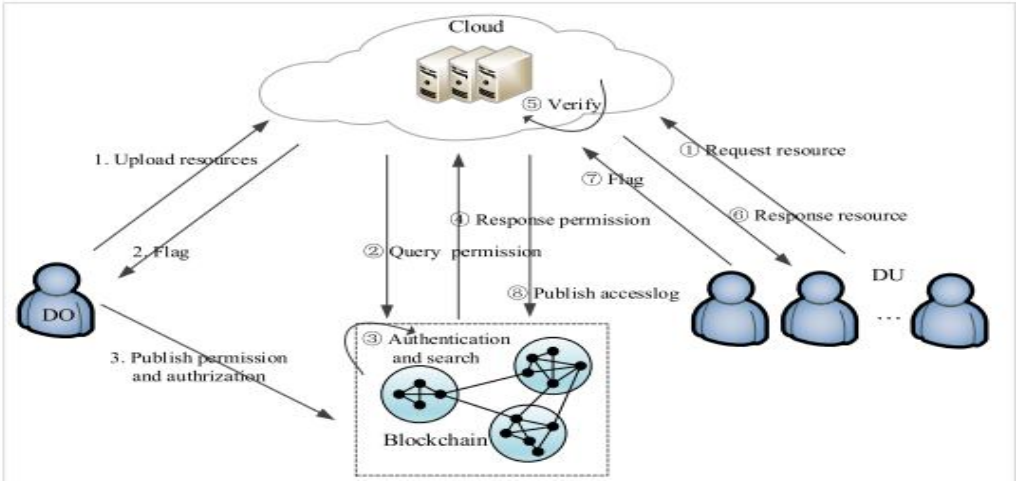

Fig 1: Overall System Architecture

ISSN: 2393-9842
https://www.irjcs.com/archives

When temporary access is needed, as for contractors or visitors, this function is quite helpful. Additionally, by automating the authorization and revocation procedures, smart contracts minimize human error and the need for manual intervention.

V. SYSTEM ARCHITECTURE AND DESIGN

Each of the interrelated parts that make up the Auth Privacy Chain system's architecture is essential to maintaining the security and privacy of the access control procedure. The system's backbone is the blockchain network, which is where smart contracts are run and encrypted access rights are kept. Data owners can create access permissions, including time-based restrictions, and upload encrypted files to the cloud using the data owner module. Before requesting access to resources, users can authenticate themselves using facial recognition thanks to the data user module. The authentication, authorization, and revocation procedures are managed by the smart contract module. By automating these procedures, smart contracts are implemented on the blockchain, guaranteeing that decisions about access restriction are made openly and without the involvement of a central authority. Because all actions are recorded on the blockchain and cannot be changed, using blockchain for these jobs improves system security.

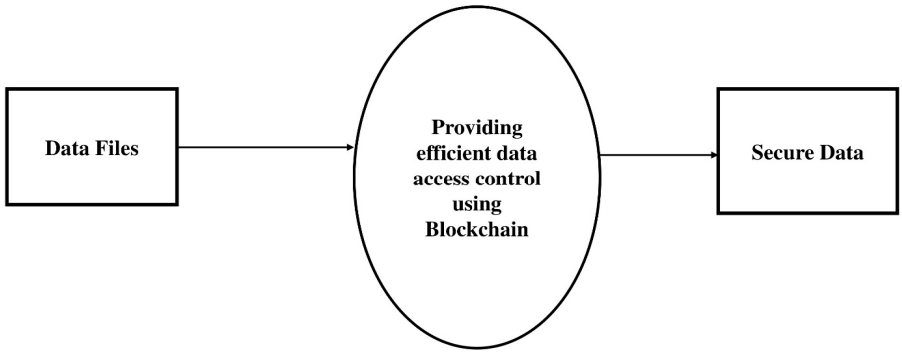

Fig 2: Data Flow Diagram (Level 0)

Access control systems must be strong and effective due to the growing amount and sensitivity of digital data. When it comes to handling complex permission structures, traditional centralized approaches can become bottlenecks, have vulnerabilities, and lack transparency. This study suggests a unique framework that uses blockchain technology to enable effective and secure data access control in order to overcome these limitations. As seen in Figure 1, the system uses pre-existing data files as input and uses the immutability, decentralization, and cryptographic security that are intrinsic to blockchain technology to impose granular access controls. In terms of security, integrity, and accountability, the desired result is "Secure Data," where access is openly controlled and auditable, providing notable benefits over traditional approaches.

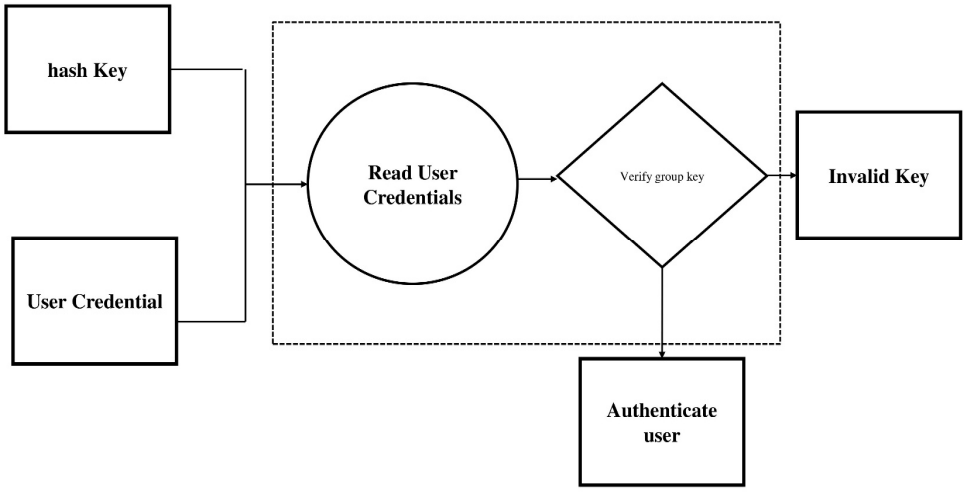

Fig 3: Data Flow Diagram (Level 1)

The suggested authentication method starts by reading a hash key and user-provided credentials. Following that, this data is put through a verification procedure that focuses on the user's group key. Unauthorized access is prevented if the authentication process ends with a 'Invalid Key' result if the supplied hash key does not match the expected group key. On the other hand, if the group key is successfully verified, the user is granted access and moves on to the 'Authenticate user' stage. By requiring the validation of two different pieces of information before granting system access, this multi-factor approach—which combines user-specific credentials with a group-based hash key—aims to improve security and reduce the risks associated with compromised individual credentials.

 https://doi.org/10.26562/irjcs

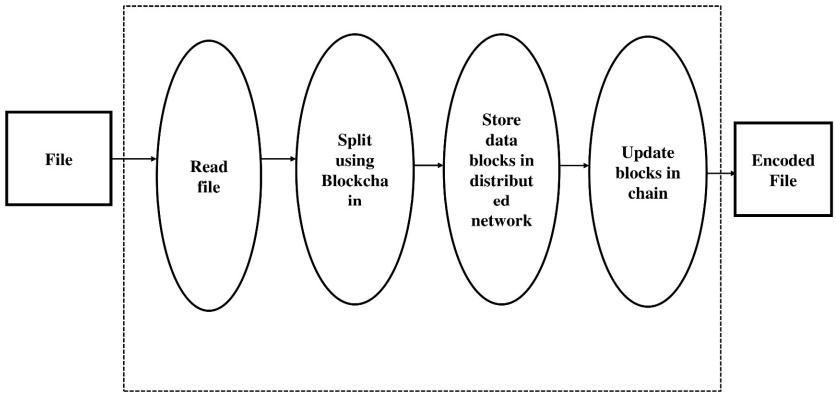

Fig 4: Data Flow Diagram (Level 2)

The process depicted explains how to encode a file using a blockchain. After receiving the input "File," the system divides the data into smaller blocks by "Splitting using Blockchain." Then, in order to increase robustness, these blocks are 'Store data blocks in [a] distributed network,' utilizing blockchain's decentralized storage. The system then 'Update blocks in [the] chain,' logging the information and related metadata onto the unchangeable ledger for a history that can be independently verified. The end result is a "Encoded File," which is a representation of the original material that has been protected by distributed storage and fragmentation, with its provenance and integrity rooted in the blockchain. This guarantees tamper resistance and data security.

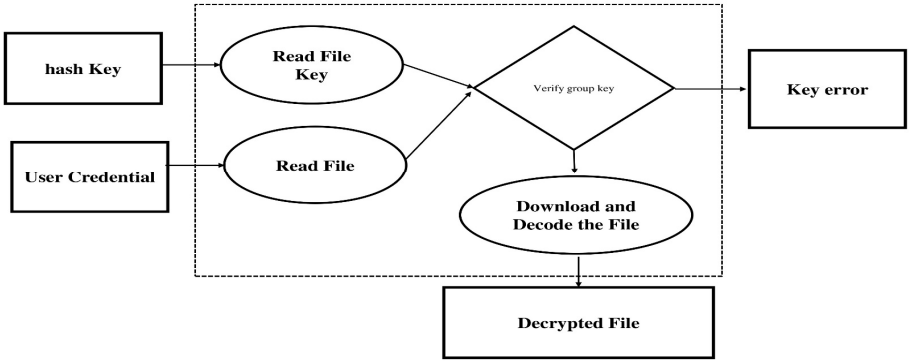

Fig 5: Data Flow Diagram (Level 3)

A secure file retrieval and decryption procedure is shown in this diagram. The user first supplies a hash key and their login credentials. The encrypted file and related encryption key are then read by the system. The integrity and legitimacy of the recovered file key are then confirmed using the supplied hash key. A 'Key error' is raised in the event that the verification is unsuccessful, blocking access. However, the system uses the verified encryption key to 'Download and Decode the File' when the group key has been successfully verified. By converting the encrypted data into a readable "Decrypted File," this decryption procedure makes sure that the original material can only be accessed by authorized users who possess the right credentials and a working key.

VI IMPLEMENTATION

There were multiple steps involved in Auth Privacy Chain's implementation. EOSIO, a high-performance blockchain platform renowned for its scalability and low transaction costs, was used to construct the blockchain and smart contract. The main functions of access control, such as automatic access revocation, authorization assignment, and user authentication, were handled by the smart contracts. LBPH algorithm, which was trained on a dataset of facial images, was used to construct the face-based authentication system. Users can swiftly and effectively authenticate themselves because to the system's real-time design. To guarantee the algorithm's resilience, it was tested on a variety of devices and adjusted for use in various lighting scenarios. Access permissions were given expiration timestamps in order to implement the time-based access control functionality. The smart contract makes sure that permissions are not left active for longer than necessary by automatically terminating the user's access once the predetermined amount of time has passed. Ultimately, a web application built with Django was created to serve as the system's user interface. Through this web application, users could request access to cloud resources, authenticate using facial recognition, and communicate with the block chain back end.

VII RESULTS AND DISCUSSION

To assess the Auth Privacy Chain framework's privacy, security, and performance, it underwent extensive testing. In order to quantify important metrics including authentication accuracy, access latency, and resilience to common security threats, the system was evaluated under a variety of scenarios.

The accuracy of authentication

Auth Privacy Chain's facial recognition module showed remarkable accuracy in a variety of test settings. With high-quality photos and controlled conditions, the system's authentication accuracy was over 95%. Tests were also conducted in less controlled settings, such as with variable lighting and facial expressions, to further confirm the system's resilience. The system maintained a high degree of accuracy even under these situations, demonstrating the Local Binary Patterns Histogram (LBPH) algorithm's practicality.

Latency of Access

A crucial component of any access control system is access latency, especially for cloud-based apps where lag can impair user experience. On average, it was found that the blockchain transactions for access control and authentication took less than two seconds. The EOSIO blockchain platform, which is designed for high throughput and quick transaction processing, was used to achieve this low latency. Given that many blockchain platforms struggle with transaction speed and network congestion, this outcome is very noteworthy.

Protection of Privacy

Providing strong privacy protection was one of the main objectives of the Auth Privacy Chain framework. In order to do this, the system made sure that neither the blockchain nor the application servers retained any biometric information in plaintext, including facial photographs. Rather, before being stored, all sensitive data was encrypted. Further safeguarding user privacy was the system's design, which stopped access control data from leaking to unapproved parties.

Scalability

Scalability becomes an important consideration for access control systems as cloud environments expand. To assess Auth Privacy Chain's scalability, it was tested with an increasing number of users and cloud resources. The system's use of a hybrid edge-cloud deployment technique showed that it could effectively manage growing loads. With this strategy, the system may grow horizontally to support more users without sacrificing security or performance.

Limitation

There are several limits to take into account, even if the framework produced encouraging results. The blockchain's transaction costs were one of the main obstacles. Transaction fees rose in tandem with the number of users and transactions. Compared to other blockchain platforms like Ethereum, EOSIO offers a comparatively inexpensive option; nonetheless, this can still be problematic in settings with high transaction volumes. Furthermore, network congestion may cause blockchain transaction latency to rise, which could have an impact on real-time access control scenarios. Future iterations of the framework might look into Layer-2 scaling options or investigate hybrid blockchain designs that mix the advantages of public and private blockchains in order to overcome these difficulties. This could increase scalability and cut expenses even more.

VIII CONCLUSION AND FUTURE ENHANCEMENTS

To sum up, the Auth Privacy Chain architecture combines the benefits of blockchain technology with privacy-preserving features like face-based authentication to provide a strong, decentralized solution for cloud access management. The approach greatly improves security and privacy while giving consumers more control over their data by automating access revocation through smart contracts and decentralizing identity management. By addressing many of the issues that traditional centralized systems encounter, including insider threats, single points of failure, and limited transparency, the system's architecture and design show that integrating blockchain technology into contemporary access control systems is feasible. Users' personal information is protected during the authentication process thanks to the system's privacy-preserving features, which include the encryption of sensitive data and the use of facial recognition without keeping biometric data in plaintext. The performance and applicability of the framework can be significantly improved in a number of ways in the future. Integrating Decentralized Identity (DID) frameworks is one such improvement that would offer a more uniform method of managing identities across many platforms. The accuracy and dependability of the system could also be increased by integrating multi-modal biometric authentication and using artificial intelligence (AI) in fraud detection. Optimizing the system for high-throughput blockchain networks, lowering transaction costs, and enhancing scalability is another exciting avenue for future research. Additionally, further research into more sophisticated cryptographic approaches may provide for even better privacy guarantees, especially in situations when secret sharing of sensitive user data across entities is required. In conclusion, Auth Privacy Chain not only pushes the boundaries of decentralized access control but also lays the groundwork for future cloud environments that are more secure and protect user privacy.

REFERENCES

1. X.Zhang,W.Zhang, and H.Chen, “A Blockchain-Based Access Control Framework for Secured Data Sharing in Industrial Internet,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10016–10027, 2019.
2. Y.Wang, G.Han, and J. Yang, “BacCPSS: A Blockchain-Based Access Control Scheme for Cyber-Physical-Social System Big Data,” Future Generation Computer Systems, vol. 107, pp. 250–261, 2020.
3. Z.Yan,P.Zhang, and A.V.Vasilakos, “A Blockchain-Based Access Control Framework for IoT Systems,” Journal of Network and Computer Applications, vol. 124, pp. 42–52, 2018.
4. L.Lei,H.Zhou, and K.Zhang, “Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System,” Journal of Cloud Computing, vol. 9, no. 1, 2020.

5. S.Singh and N.Sharma,"A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environments," Journal of Cloud Computing: Advances, Systems and Applications, vol. 10, no. 1, 2021.
6. G.Zyskind, O.Nathan, and A.Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proceedings of the IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184.
7. M.Ali,J.Nelson, R.Shea, and M. J. Freedman, "Blockstack: A Global Naming and Storage System Secured by Blockchains," in USENIX Annual Technical Conference (ATC), 2016, pp. 181–194.
8. A.Dorri,S.S.Kanhere, and R.Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv:1608.05187, 2016.
9. B.S.K.H.Challa, P.J.S.G.Kiran, and S.R.C.S.Subrahmanyam, "Secure and Scalable Access Control in Cloud Environments using Blockchain," Journal of Cloud Computing, vol. 9, pp. 16-30, 2022.
10. C.M.K.Karuppiah and R.S.Maheswari,"Efficient Blockchain-based Authentication for IoT Devices in Cloud Platforms," International Journal of Cloud Computing and Services Science, vol. 9, no. 3, pp. 225-238, 2021.

