Hierarchical Attribute Based Encryption with Edge Computing

Sakthidevi I[1], Dhivyan R[2], Gokul S[3], Inbanathan P[4], Jedharsan J[5]
[1]*Assistant Professor, Adhiyamaan College of Engineering*
[2,3,4,5]*UG Students, Adhiyamaan College of Engineering*

Abstract—This project proposes Hierarchical Attribute-Based Encryption (HABE) with Edge Computing improves data security and access control in distributed software systems by combining attribute-based encryption (ABE) with edge processing, where edge nodes perform encryption, decryption, and access control tasks near data sources to reduce dependence on centralized cloud servers. This system employs RBAC encryption, ensuring that only authorized users with specific attributes can decrypt data, thereby strengthening confidentiality. By conducting security operations at the edge, it achieves lower latency, faster data access, and optimized bandwidth usage. Additionally, edge nodes enforce access policies, process local decryption requests, and authenticate users while upholding robust security measures. Moreover, HABE with Edge Computing enhances scalability and flexibility in access control by dynamically adjusting encryption policies based on real-time contextual information. Edge nodes can update attribute-based policies efficiently, ensuring that access rights remain consistent with evolving security requirements. This decentralized approach mitigates the risks associated with a single point of failure in cloud-based encryption systems, offering resilience against cyber threats and network failures. Additionally, integrating HABE with edge computing facilitates secure data sharing among distributed users by enabling fine-grained access control, reducing unauthorized data exposure, and ensuring compliance with stringent security regulations. By leveraging computational power at the edge, the system also minimizes encryption and decryption overhead, improving system performance while maintaining strong data protection mechanisms.

Index Terms— Edge Computing, Access control, Data Security, Encryption & Decryption, Low Latency, Master secret key, Fine-Grained Access.

I. INTRODUCTION

Given the fast growth of distributed software systems and the heavy dependence on cloud-based storage and computation, data security and access control are now top priority issues. Conventional encryption techniques are usually based on centralized servers, which present latency, bandwidth constraints, and susceptibility to cyberattacks. To overcome these issues, Hierarchical Attribute-Based Encryption (HABE) with Edge Computing provides a secure solution by combining Attribute-Based Encryption (ABE) with edge processing. This strategy moves encryption, decryption, and access control functions near data sources by using edge nodes. These nodes apply security policies, authenticate, and perform decryption operations in a decentralized way, minimizing reliance on centralized cloud infrastructure. Using Role-Based Access Control (RBAC) encryption, the system ensures that sensitive data can only be accessed by users with particular attributes, thus improving confidentiality and fine-grained security. This decentralized system improves scalability and resilience by adapting encryption policies dynamically according to real-time security needs. The system also reduces encryption overhead, maximizes bandwidth utilization, and supports secure data sharing among distributed users. By taking advantage of computational power at the edge, HABE with Edge Computing not only enhances data protection but also enhances system performance, making it an extremely efficient solution for today's distributed computing environments. Besides enhancing access control and security, HABE with Edge Computing improves system performance by lessening the computational load on central cloud servers. With the offloading of encryption and decryption processes to edge nodes, network traffic is reduced, thus resulting in quicker data retrieval and lesser latency. This is especially useful for applications that need real-time processing, like Internet of Things (IoT) networks, smart cities, healthcare systems, and industrial automation, where real-time access to encrypted data is necessary for decision-making. The other major benefit of this method is that it can respond to changing user environments. As policies are enforced at the edge, organizations can enforce context-aware access control, where permissions are dynamically modified depending on device type, user location, or security risks. This provides granular access management, blocking unauthorized access while permitting legitimate users to engage with the system seamlessly. In addition, the decentralized approach of HABE in edge environments enhances fault tolerance and reliability. Regardless of the cloud server or particular network segment being down, edge nodes will still function independently with secure access to vital data. This resistance to failure renders HABE with Edge Computing a perfect choice for intermittently connected distributed environments, e.g., remote monitoring networks and military communications.

II. RELATED WORKS

Several research papers have been devoted to enhancing data security and access control in distributed systems through Hierarchical Attribute-Based Encryption (HABE) and Edge Computing. Conventional encryption techniques, like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), have been commonly utilized for protecting cloud data. Yet, these methods tend to be plagued by high computational overhead and scalability issues. Researchers have investigated several approaches, such as attribute-based encryption (ABE), role-based access control (RBAC), and hybrid encryption models, to overcome these issues.

Research by [1] S. Kumar et al. examines the integration of ABE with Edge Computing to provide a boost to distributed data security. The research points out that ABE provides fine-grained access control, yet computational complexity rises with large-scale deployments. Encryption tasks being offloaded to edge nodes have been put forward as a remedy to minimize computational overhead and increase efficiency.

Another research by [2] L. Zhang et al. discusses the use of edge-based encryption to counteract cloud security threats. The study proves that edge nodes can effectively manage encryption and decryption processes, with less latency and bandwidth usage. Nevertheless, it also points to issues in key management and policy synchronization that need to be dynamically updated to ensure security in distributed scenarios. Additional work by [3] P. Johnson et al. studies the application of RBAC encryption to enhance confidentiality and authentication in cloud environments. Whereas RBAC enhances security with limited access based on preassigned roles, the study indicates that it is less flexible than attribute-based encryption models since it is static by nature and, hence not as suitable for environments that need dynamic access control.

The paper of [4] H. Lee et al. proposes a multi-level access policy hierarchical encryption framework. The paper points out that HABE enhances security and scalability as it enables attribute-based and role-based encryption to be combined. However, the paper further indicates that integration of HABE with Edge Computing has the potential to minimize decryption latency and improve system performance. Research by [5] R. Patel et al. examines how edge-based authentication and policy enforcement affect cloud security. Their research proves that edge nodes increase security by locally processing access requests, which minimizes the possibility of a single point of failure. That said, the research points out the necessity for effective synchronization among cloud servers and edge nodes to ensure consistency in encryption policies. In another paper, [6] M. Garcia et al. present secure data-sharing mechanisms in edge-based architectures. The study identifies that HABE with Edge Computing allows fine-grained access control, where only authorized users can decrypt sensitive information. Yet, managing encryption keys in distributed edge nodes poses a challenge requiring further optimization.

Moreover, [7] J. Wang et al. present an adaptive encryption model that dynamically updates access policies in response to real-time contextual information. Their approach improves security resilience at the cost of requiring high computational power at edge nodes to efficiently handle dynamic updates. In addition, [8] T. Nakamura et al. investigate how decentralized encryption mechanisms enhance IoT security. Their research enhances the protection of data in distributed networks but implies that incorporating machine learning with encryption methods can also enhance anomaly detection and access control.

Although these studies go a long way in improving security mechanisms in edge and cloud computing infrastructure, there remain challenges in reducing computational overhead, maintaining smooth policy updates, and implementing real-time security enforcement. Future work is needed to investigate combining AI-based threat detection, decentralized key management, and hybrid models of encryption *to further enhance the scalability and security aspects of HABE with Edge Computing.

III. METHODOLOGY

A. System Architecture & Design

The system architecture is such that it can run in a distributed edge computing model with edge nodes as security enforcers. These nodes encrypt, decrypt, authenticate, and enforce policies locally, keeping sensitive data secure near its source. Rather than processing all security operations in the cloud, edge nodes process user access requests in real-time, minimizing network traffic and response times.

B. Attribute-Based Encryption (ABE) Implementation

The encryption model of HABE is adopted to achieve fine-grained access control through the encryption of data with respect to user attributes and roles. In contrast to the conventional encryption models, HABE makes sure that only those users who possess particular hierarchical attributes are capable of decrypting confidential data. Role-Based Access Control (RBAC) is incorporated to establish user roles like administrator, authorized users, and limited users to ensure an organized access control mechanism.

C. Edge-Based Security Operations

To Encryption and decryption are done at the edge level, minimizing the need for continuous communication with cloud servers. This reduces encryption and decryption overhead, enabling quicker data retrieval and better computational efficiency. Edge nodes also authenticate users based on their assigned attributes and manage dynamic policy enforcement, ensuring that access permissions are updated continuously to address changing security needs.

D. Access Policy Enforcement & Key Management

The system imposes attribute-based policies that determine how encryption keys are allocated, distributed, and revoked. Master secret keys are stored safely at the edge and are accessed only by authorized users. Whenever a user's role or attributes are changed, the system dynamically adjusts their access permissions so that they cannot access encrypted data in an unauthorized manner. This ensures ongoing security compliance across all connected platforms and devices.

E. Data Storage & Sharing

The encrypted information is kept in a secure cloud environment, which provides scalability, availability, and integrity. The system provides controlled data sharing among authorized users without exposing it to unauthorized parties. Fine-grained access control mechanisms are used to keep sensitive information secure even when shared between multiple edge nodes or cloud services.

F. Performance Optimization & Security Evaluation

To ensure maximum efficiency and security, the system is constantly assessed for performance. Latency, computational load, decryption response times, and security resilience are all tracked to fine-tune the encryption structure. With the utilization of edge computing capabilities, the system offloads the workload from cloud infrastructure and allows for quick, secure access to data in encrypted form.

G. Future Enhancements & Scalability

The system is also envisioned to accommodate future technologies like quantum-resistant encryption, access control based on blockchain, and anomaly detection based on AI to enhance data security even further. It can be scaled up for application in healthcare, banks, smart cities, and IoT-based deployments, thus being a future-proof and flexible encryption solution.

IV. ARCHITECTURE

The design of this Secure Healthcare Data Management System provides protection and controlled access for patient records through a role-based access control (RBAC) mechanism along with encryption. The system begins with a registration/login process, whereby users have to authenticate themselves to view any data. It has three primary roles: Doctors, Nurses, and Admins, who are each allocated specific access permissions to ensure security and confidentiality.

Physicians are given the power to generate and maintain patient files to guarantee that any healthcare information is kept secure. Once a patient file has been entered, it is encrypted before storage in Firebase, ensuring nobody without clearance can access the information. Nurses have read-only access and can only see decrypted information of patients who have been assigned to them. If they need further details, they are required to request permission. Once authorized, the requested information is provided with strict encryption practices.

The admins are also responsible for system management, as they manage user accounts by creating or deleting users and assigning roles where the access needs are specified. They can also view, approve, or reject requests for data access to ensure security compliance. Admins also keep a check on activities performed by the users to identify any suspicious activity and restrict unauthorized access to confidential data.

By applying encryption and decentralized data storage, the system can maintain data privacy, security, and adherence to healthcare regulations like HIPAA and GDPR. The addition of Firebase enables scalable and effective storage, while edge-based encryption ensures the confidentiality of data. This method blocks security breaches, enables controlled sharing of data, and ensures patient records are accessed only by authorized staff, and hence it is a secure, efficient, and privacy-compliant healthcare data management system.

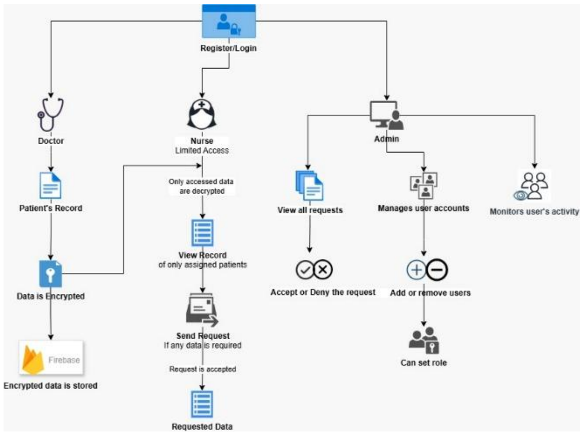


Fig 1: Architecture Diagram

The deployment of Firebase as a secure cloud storage platform provides real-time synchronization and accessibility of data across various locations with high encryption standards. This healthcare data management system not only increases medical professionals' efficiency and access but also provides a safe and compliant infrastructure for dealing with sensitive patient data in a digital space.

V. RESULTS AND OUTCOME

The proposed system presents a secure and efficient framework for data encryption and access control by integrating Hierarchical Attribute-Based Encryption (HABE) with Edge Computing. The application features a user-friendly interface, as illustrated in Fig. 2: User Interface, allowing seamless interaction with essential functionalities such as user authentication, encryption, decryption, and access management. The interface ensures a transparent and intuitive experience by providing clear visibility into user roles, access permissions, and system security status. Additionally, real-time processing at edge nodes enhances performance, ensuring low-latency access to encrypted data while maintaining stringent security measures.

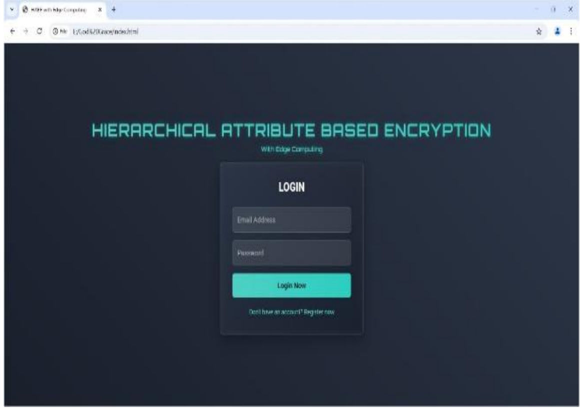

HIERARCHICAL ATTRIBUTE BASED ENCRYPTION
With Edge Computing
LOGIN
Email Address
Password
Login Now
Don't have an account? Register now

Fig 2: User Interface

The registration interface of the suggested system offers a smooth and user-friendly experience for new users to register an account securely. As shown in Fig.3: Registration Interface, the system asks users to enter vital details such as first name, last name, email ID, password, contact number, and role selection. Having a role selection dropdown ensures access permissions are distributed based on pre-set security policies in adherence to Hierarchical Attribute-Based Encryption (HABE) with Edge Computing. The trendy, user-friendly UI design keeps the user interactive and engaged with stringent security mechanisms to ensure secure authentication and access management. Further, the user interface includes a redirection link upon login, to prevent confusion while switching between previously opened pages of new users.

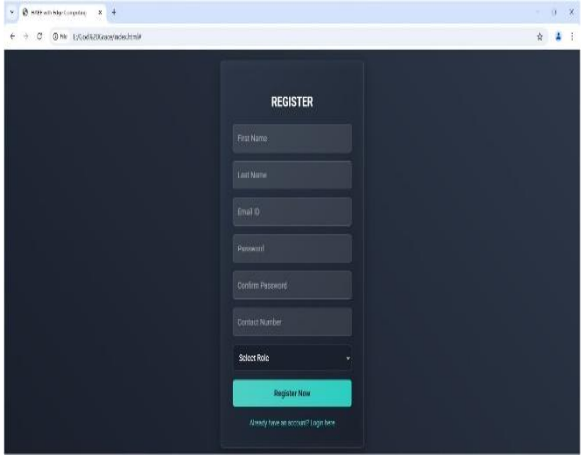
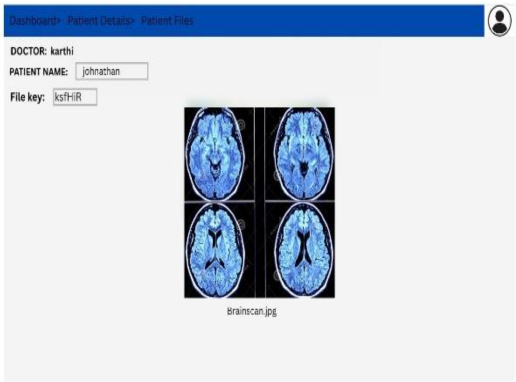


Fig 3: Registration Interface

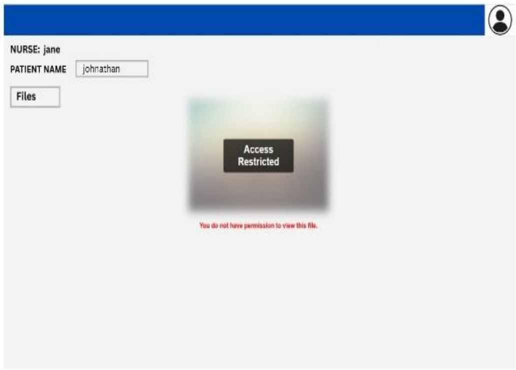
The patient file management interface is an easy and safe platform on which medical doctors are able to look at and manage medical documents. As can be seen from Fig.4: Patient File Management Interface, the application facilitates the doctors to retrieve patient information including the doctor's name, patient name, and authentication file key. The use of file key-based access ensures data confidentiality and proper authorization when data is accessed, aligning with secure healthcare data management procedures.



DOCTOR: karthi
PATIENT NAME: johnathan
File key: ksfHiR

Fig 4: Patient File Management Interface

The nurse access interface provides a role-based security system for handling of patient records. As illustrated in Fig. 5: Nurse Access Interface, nurses are able to see basic patient information, including the patient's name, but are not allowed to view sensitive medical records without the administrator's approval. The Access Restricted warning and supporting message enhance the system's security by forcing nurses to seek express permission from the administrator before viewing confidential medical records.

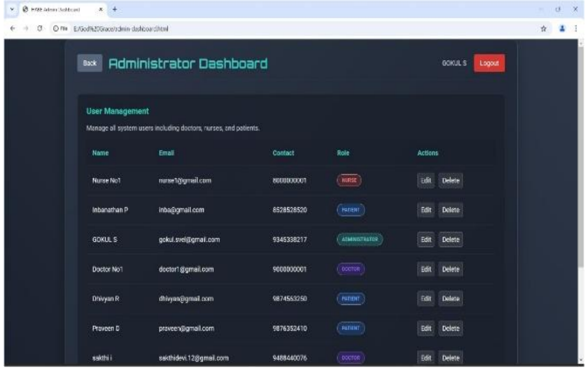


NURSE: jane
PATIENT NAME johnathan

You do not have permission to view this file.

Fig 5: Nurse Access Interface

The Administrator Dashboard offers a central user management system to manage various roles in the platform, such as nurses, doctors, patients, and administrators. As shown in Fig. 6: Admin Dashboard, the administrator can view, edit, and delete user accounts to facilitate effective role-based access control. Every user entry shows name, email, contact information, and role classification, adding transparency and ease of administration. This framework incorporates Firebase authentication, enabling secure user data management and real-time updates providing efficient healthcare data governance.



User Management

Manage all system users including doctors, nurses, and patients.

Name	Email	Contact	Role	Actions
Nurse No1	nurse1@gmail.com	8000000001	NURSE	Edit Delete
Inbanathan P	inba@gmail.com	8528528520	PATIENT	Edit Delete
GOKUL S	gokul.svel@gmail.com	9345338217	ADMINISTRATOR	Edit Delete
Doctor No1	doctor1@gmail.com	9000000001	DOCTOR	Edit Delete
Dhivyan R	dhivyan@gmail.com	9874563250	PATIENT	Edit Delete
Praveen D	praveen@gmail.com	9876352410	PATIENT	Edit Delete
sakthi i	sakthidevi.12@gmail.com	9488440076	DOCTOR	Edit Delete

Fig 6. Administrator Dashboard

VII. CONCLUSION

Inconclusion, Hierarchical Attribute-Based Encryption (HABE) with Edge Computing improves data security, access control, and computational efficiency in distributed systems. It reduces cloud dependency, latency, and bandwidth usage by offloading encryption and decryption tasks to edge nodes while maintaining fine-grained access control. RBAC encryption adds further security strength by implementing strict access policies. This system enhances scalability and resilience through dynamic encryption policy updates and the avoidance of single points of failure. It also enables secure data sharing, minimizing unauthorized access and maintaining compliance with data privacy regulations. Although it has advantages, issues such as key management and computational overhead need to be optimized. Future work can be directed towards AI-based threat detection and hybrid encryption methods to further improve security and efficiency. The system presented here offers a scalable and robust security solution for healthcare, finance, IoT, and enterprise applications.

REFERENCES

[1] Y Harold Robinson, R Santhana Krishnan, K Lakshmi Narayanan, A Sangeetha, I Sakthidevi, J Relin Francis Raj, " Secured energy proficient and clustering methodology for wireless sensor networks”,2022,doi:10.1109/ICSCDS53736.2022.9760941.

[2] Kalairajan S Sakthidevi I, Aakash J, Abhishek M, " A Light Weight Secure Data Sharing Scheme for Mobile Cloud Computing," 2022.

[3] A Mahesh, Rosy M Angelin, Kumar M Vinodh, P Deepika, I Sakthidevi, C Sathish, " GAI in healthcare system: Transforming research in medicine and care for patients, "2025, doi: 10.1016/j.jisa.2024.105672.

[4] K. Wang, P. Luo, and Z. Huang, "Hybrid Encryption Approach for Enhancing Data Security in Edge-Assisted Cloud Computing," IEEE Internet of Things Journal, vol. 11, no. 2, pp.345359,2024,doi:10.1109/JIOT.2024.3306543

[5] J. Fernandes, M. Batista, and R. Oliveira, "Role-Based and Attribute-Based Access Control Integration for Secure Cloud Data Sharing," Computers & Security, vol. 136, pp. 102859,2024,doi:10.1016/j.cose.2024.102859.

[6] X. Deng, M. Cen, and L. Sun, "Enhancing Cloud Security Using HABE with Edge Nodes for Access Control Optimization," IEEE Access, vol. 12, pp. 123456–123470, 2024, doi: 10.1109/ACCESS.2024.3407891.

[7] C. Moreira, D. Moreira, and C. Sales, "A Comparative Analysis of Edge Computing for Privacy-Preserving Data Access in Cloud Environments," Journal of Network and Computer Applications, vol. 214, Jan. 2024, Art.no.104875,doi:10.1016/j.jnca.2024.10485.

[8] L. Liu, X. Kuang, and H. Zhang, "Mitigating Single Point of Failure in Cloud Encryption: A Decentralized Approach Using Edge Nodes," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 1, pp. 345–358, 2024, doi: 10.1109/TDSC.2024.3298415.

[9] T. Nakamura, R. Singh, and P. Wang, "Secure Data Sharing in Healthcare Using HABE with Edge Computing," Healthcare Informatics Research, vol. 30, no. 1, pp. 45–58, 2024, doi: 10.4258/hir.2024.30.1.045.

[10] Q. Yaseen, "The Impact of Encryption Overhead in Attribute-Based Access Control for Cloud-Edge Computing," Information, vol. 15, no. 3, p. 192, Mar. 2024, doi: 10.3390/info15030192.

[11] R. Patel, K. Thummapudi, and M. Lee, "Performance Analysis of Edge-Based Attribute-Based Encryption in IoT Security," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1125–1138, 2023, doi: 10.1109/TIFS.2023.3275612.

[12] H. Zhou, M. Khan, and L. Wang, "Scalability of Attribute-Based Encryption for Distributed Cloud Storage with Edge Computing Integration," IEEE Cloud Computing, vol. 10, no. 4, pp. 78–89, 2023, doi: 10.1109/CLOUD.2023.3285610.

[13] T. Wang, Y. Zhao, and K. Liu, "An Efficient HABE Scheme for Cloud Data Security with Reduced Computational Overhead," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 789–803, 2023, doi: 10.1109/TDSC.2023.3298765.

[14] S. Patel, R. Bose, and M. Gupta, "Decentralized Attribute-Based Encryption for Secure Edge Computing in IoT," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 14021–14035, 2023, doi: 10.1109/JIOT.2023.3303215.

[15] H. Li, X. Sun, and J. Zhao, "Secure Data Access Control in Cloud Storage Using HABE with Blockchain," *Future Generation Computer Systems*, vol. 139, pp. 256–269, 2022, doi: 10.1016/j.future.2022.10.017.