International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

SECURE AND FINE-GRAINED ACCESS CONTROL MECHANISM FOR IOT-BASED HEALTHCARE DATA SHARING SYSTEMS

Divya C
PG,Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
divyacmca2025@gmail.com

Mridula Shukla
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
mridulatewari@theoxford.edu

ABSTRACT

The Internet of Things' (IoT) rapid expansion in the healthcare sector has increased the need to ensure that confidential medical data shared among IoT-enabled devices is secure and accessible only by authorized parties. This study proposes a precise and secure access control solution for Internet of Things-based healthcare data sharing platforms. Data owners can enforce specific access restrictions based on attributes such as time, location, user roles, and data sensitivity using the proposed framework's attribute-based encryption (ABE) feature, which provides fine-grained access control. Additionally, by ensuring data integrity and traceability, the framework combines multi-factor authentication (MFA) with blockchain technology to enhance data interchange security.

A centralized access control server is part of the system architecture, which controls access permissions and validates patient, healthcare provider, and other stakeholder requests for data access.

Keywords: Internet of Things (IoT) Sharing of Health Data Attribute-Based Encryption for Access Control (ABE) Fine-Structured Access Management Authentication with multiple factors (MFA) Inferentiality of Blockchain Data Security Integrity of Data Individual privacy.

INTRODUCTION

The way medical data is collected has radically altered as a result of deployment of Internet of Things (IoT) devices in healthcare, tracked, and shared. Examples of IoT-enabled technologies that provide the smooth transmission and monitoring of real-time health data across healthcare systems include wearables, smart medical devices, and sensors. But when it comes to data security, privacy, and access control, the increasing amount of sensitive health data poses serious problems, particularly when it is shared across several parties, including patients, healthcare providers, and outside businesses. Ensuring the confidentiality and privacy of sensitive health data while limiting access to only authorized

parties is essential in an Internet of Things-based healthcare data exchange system.

This project intends to propose and develop a fine-grained, secure access control mechanism to efficiently manage the sharing of healthcare data across IoT systems. With the help of attribute-based encryption (ABE), the proposed solution will provide fine-grained access control, enabling data owners, such as patients or healthcare organizations, to define specific access policies based on attributes such as time, location, user roles, and data sensitivity. When it comes to providing fine-grained access control—which is essential in dynamic and complex healthcare environments—traditional access control mechanisms frequently fall short.

.

LITERATURE SURVEY

The use of Internet of Things devices in healthcare has greatly improved real-time patient monitoring, diagnosis, and treatment. However, sharing private health information across various systems, devices, and stakeholders raises significant security and privacy concerns. Because they ensure that only authorized users can access healthcare data, prevent unauthorized access, and protect patient privacy, secure and fine-grained access control systems are essential to lowering these risks. The current research on IoT-based healthcare data sharing systems, security solutions, and access control systems is examined in this review of the literature.

EXISTING WORK

To protect data confidentiality, cryptographic techniques such as identity-based and public-key cryptosystems could be used to limit access to authorized devices. These methods only allow for coarse-scale data collaboration, and the encryptor must know the corresponding decryptor's facts before attempting to create the ciphertext. In this approach, the mechanism for data exchange is one cipher for one decryptor rather than a collection of decryptors. Many users with similar or related features who are part of an unknown group size, like a team of on-call doctors and other medical professionals, often post private information in an IoT network for healthcare.

PROPOSED SYSTEM

We create a unique, safe, and efficient fine-grained access control method termed server-aided dual-policy attribute-based encryption (SA-DP-ABE) to concurrently address current system issues with ultra-light devices. The five different types of entities that comprise our IoT system for healthcare are key generate center (KGC), data owners (DOs), data users (DUs), edge server (ES), and cloud server (CS). We can combine CS and ES into a single entity without accounting for geography, assuming that CS is a remote server and ES is a server situated closer to DUs. Furthermore, our system paradigm does not require a secure connectivity.

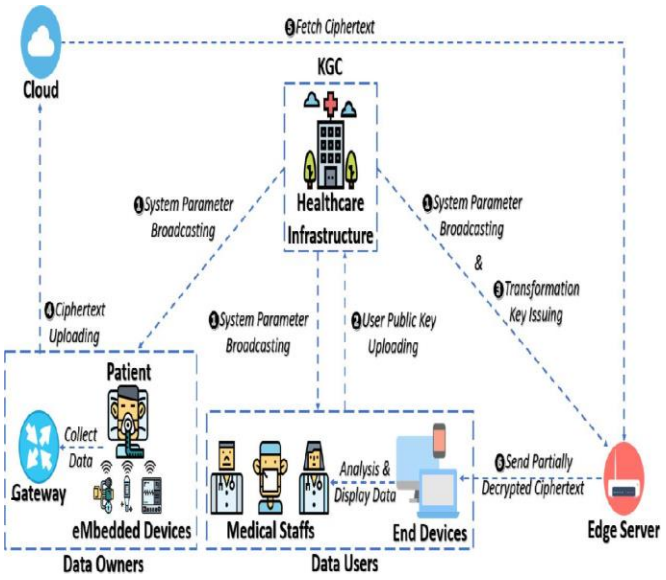
The proposed method is developed using the Java programming language, which benefits from its flexibility and resilience.

Numerous contextual factors, including user roles, time constraints, device characteristics, and patient consent, can be used to define and manage access rights. With this framework, healthcare organizations can fine-tune their access policies.

METHODOLOGY

The suggested method combines encryption, policy-based access control, and secure communication to guarantee precise and safe access control in IoT-based healthcare data sharing systems. Sensitive patient health data is gathered by IoT devices and sent to a cloud server via edge gateways. Information is encrypted and stored there using Elliptic Curve Cryptography (ECC) and other low-power cryptographic methods. The Attribute-Based Access Control (ABAC) paradigm is used to manage access to this data. Policies are set according to user roles, data categories, time, location, and access purpose. To guarantee that only authorized users can access particular data segments, these policies are assessed by a Policy Decision Point (PDP) and implemented by a Policy Enforcement Point (PEP).

Transparency and tamper-proof recordkeeping can also be achieved by integrating a blockchain-based audit mechanism that records all access events. Key performance indicators like policy accuracy, security strength, access latency, and user control over data sharing are used to assess the system.



For IoT-based healthcare data sharing, the suggested system offers a safe and precise access control mechanism. The following crucial steps are part of the methodology:

1. **System Setup:** Use Internet of Things-enabled medical devices to gather patient health data, which is then safely sent to a cloud server via edge gateways.

2. Data Encryption: To guarantee end-to-end data confidentiality during storage and transmission, implement lightweight encryption (such as ECC) at the device level.

3. Fine-Grained Access Control: Use Attribute-Based Access Control (ABAC) to establish and implement rules according to user characteristics (e.g., role, location, purpose). This guarantees that certain health data can only be accessed by authorized users.

4. Policy Management: Provide a user-friendly interface for administrators and patients to establish access control policies, guaranteeing adherence to healthcare laws (e.g., GDPR, HIPAA).

EXPERIMENTAL RESULTS

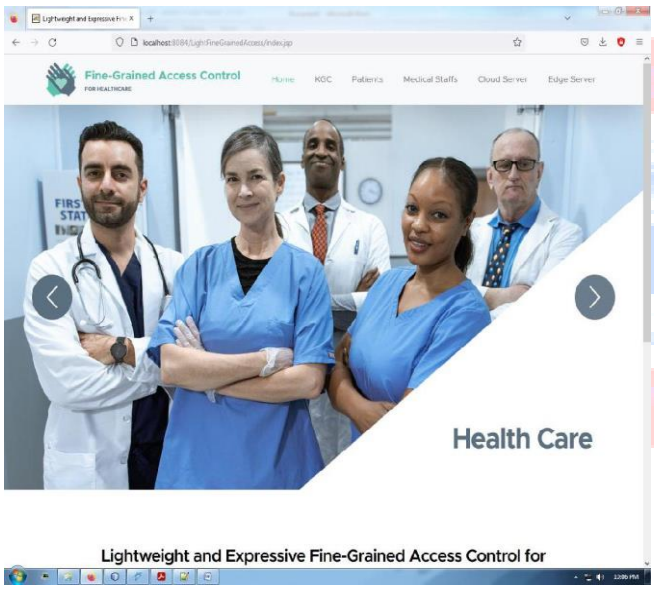
KEY GENERATE CENTER (KGC)

Initialization of the device with cryptographic key management is the responsibility of the Key Generation Center (KGC). It generates the parameters for the procedure, including transformation keys and public-private key pairs. In order to provide secure decryption, the KGC safely distributes the transformation-related Edge Server keys (ES) for Data Users (DU). The KGC acts as a completely reliable organization, guaranteeing the confidentiality and veracity of the keys. KGC is responsible for managing the login credentials for DUs, initializing the entire system, and supplying transform keys to ES. We assume that the KGC and DOs are completely trustworthy. Owner of Data Users who have private messages and wish to safely share them are represented by the Controller of Data module.

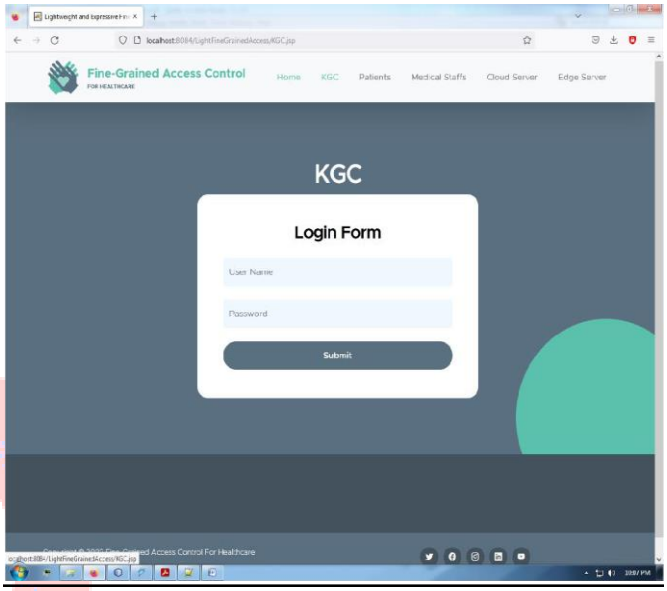
After that, the ciphertexts—encrypted messages—are uploaded to a Cloud Server (CS) for distribution and storage. A group of individuals who have uploaded private conversations to CS for safe dissemination to DU are known as Data Owners (DOs). User of Data Those who obtain the appropriate credentials from the KGC are granted access to data users. The amount of money available to each data user

Processing limits the amount of data that can be stored, and their objective is to safely read and decode ciphertexts. After requesting the encrypted data from CS, Data User obtains the necessary transformation keys from ES. With these keys, the data user performs the decryption process, which can be partial or full and suitable for any encryption.

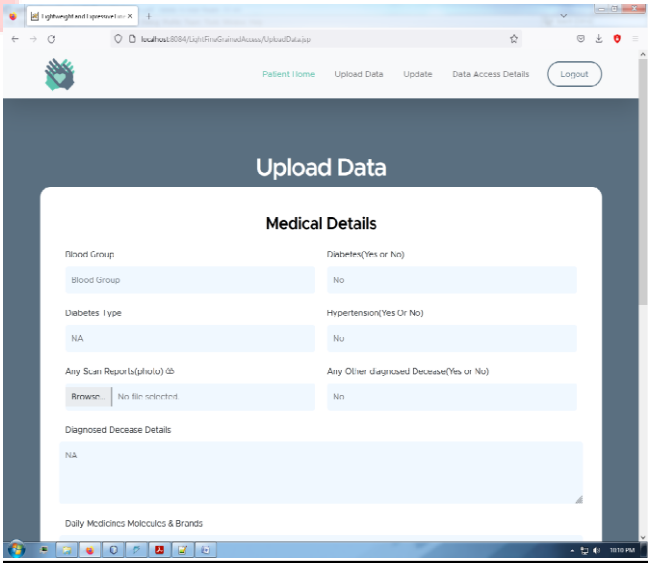
- Home Page



- Login Page



- Upload Data Page



CONCLUSION

The proposed fine-grained and safe access control technique effectively enhances the security and privacy of IoT-based healthcare data sharing systems. The system integrates lightweight encryption, attribute-based access control, and optional blockchain-based audit tracking to ensure that only authorized users may access critical health information. In addition to protecting patient data, this approach offers flexibility, scalability, and compliance with healthcare standards, making it a solid choice for modern healthcare environments.
We looked at IoT network issues in a healthcare setting in this study and developed a solution that enables secure IoT connectivity with source-restricted devices and granular permission. The suggested system's structure, threat model, and risk criteria were introduced. To demonstrate how much more efficient our architecture is than earlier solutions, we also presented preliminary testing and evidence of our suggested design.

REFERENCES

1. D. Reinsel, J. Gantz, and J. Rydning, “Data age 2025: Data's progression into lifecritical,” 2017. [Online]. Available: https://www.seagate.com/www-content/our-story/trends/files/Seagate-WPDataAge2025-March-2017.pdf
2. T. D. T. Report, “Thales Data danger report: Trends in data protection security,” 2018. [Online]. Available: https://dtrhealthcare.thalesesecurity.com/pdf/2018-thales-data-threatreport-healthcare-edition-executive-summary.pdf
3. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge technology: Visualization challenges,” IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016.
4. M. Chiang and T. Zhang, “Fog with iot: A summary of the studies opportunities,” IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, Dec. 2016.
5. J. Ren, H. Guo, C. Xu, and Y. Zhang, “Serving scalable Internet of Things structure built around transparent computing,” IEEE Netw., vol. 31, no. 5, pp. 96–105, Aug. 2017.