IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

ENHANCINNG PRIVACY AND SECURITY IN CLOUD-BASED PERSONAL HEALTH RECORD SHARING USING ATTRIBUTE BASED ENCRYPTION

[1]Dhanya P, [2]Sameer Ahmed Z, [3]Mohammed Rakhshan R , [4]Raja Pandi S, [5]Mohammed Aslam A
[2,3,4,5] Student, [1] Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Aalim Muhammed Salegh College of Engineering, Thiruvallur, Tamil Nadu India

Abstract: The increasing use of cloud services in healthcare enables cost-effective sharing of Personal Health Records (PHRs), but it also raises serious privacy and security concerns. To address this, we propose a framework based on Attribute-Based Encryption (ABE), which provides fine-grained, attribute-driven access control over encrypted PHRs stored on untrusted cloud servers. A trusted authority manages key generation, attribute distribution, and access policies, ensuring protection against insider threats as well as forward and backward access control. Formal analysis using High-Level Petri Nets (HLPN) and performance evaluation show that the ABE-based system offers an effective and secure solution for sharing PHRs in the cloud.

I. INTRODUCTION

The healthcare industry's quick embrace of cloud-based services has revolutionized the management, sharing, and storage of personal health records (PHRs). Cloud computing provides a scalable, affordable, and practical means for patients and healthcare providers to access and share medical data across various e-Health system entities. But even though the cloud offers these benefits, there are also serious issues about the security, privacy, and confidentiality of private medical data. Patient privacy is seriously compromised when PHRs are stored on third-party cloud servers, which are frequently unreliable and increase the risk of data breaches, illegal access, and insider threats. Strong security measures that provide fine-grained control over who can access what information and under what circumstances are necessary to protect this data. These measures go beyond simple encryption.

This paper uses Attribute-Based Encryption (ABE) to provide a secure framework for cloud-based PHR sharing in order to overcome these issues. By defining specific access policies based on user attributes (like roles or qualifications), ABE allows patients to encrypt their PHRs and guarantees that only authorized individuals can view particular parts of the records. To improve security against insider and external threats, the system integrates a trusted authority to oversee attribute assignment, policy enforcement, and key generation. Furthermore, the framework can manage changes in user permissions over time by supporting both forward and backward access control, which guarantees that old users lose access while new users acquire it when necessary. High-Level Petri Nets (HLPN) are used to formally analyze the suggested solution, offering a systematic assessment of its architecture and functionality. Performance reviews also show that the system is scalable, efficient, and able to provide secure, privacy-preserving PHR sharing in cloud environments.

II. BACKGROUND

In recent years, the integration of cloud computing into the healthcare sector has drastically improved the way medical records are created, managed, stored, and shared. One of the most significant advancements is the cloud-based handling of Personal Health Records (PHRs), which allows patients and healthcare providers to interact with medical data in a more flexible and accessible manner. These cloud solutions offer cost-effectiveness, centralized data storage, and accessibility across various platforms and users in the e-Health ecosystem. However, this widespread adoption of cloud services also introduces a serious concern: the risk of unauthorized access, data breaches, and loss of patient privacy. The sensitive nature of health information makes it a prime target for cyber-attacks, and traditional security measures often fall short in providing the necessary fine-grained control and confidentiality.

One of the core challenges is that PHRs are stored on cloud servers, which may not always be fully trusted. While these servers make data access more convenient, they also increase the vulnerability to data exposure and misuse, particularly in cases where access is not carefully regulated. To tackle these issues, researchers have turned to cryptographic solutions that can enforce security at the data level, regardless of where the data is stored. Among these, **Attribute-Based Encryption (ABE)** has proven to be a highly effective approach. Unlike traditional encryption schemes where access is granted based on user identity, ABE enables access control based on a set of attributes — such as a user's role (doctor, nurse, insurance agent), department, or clearance level.

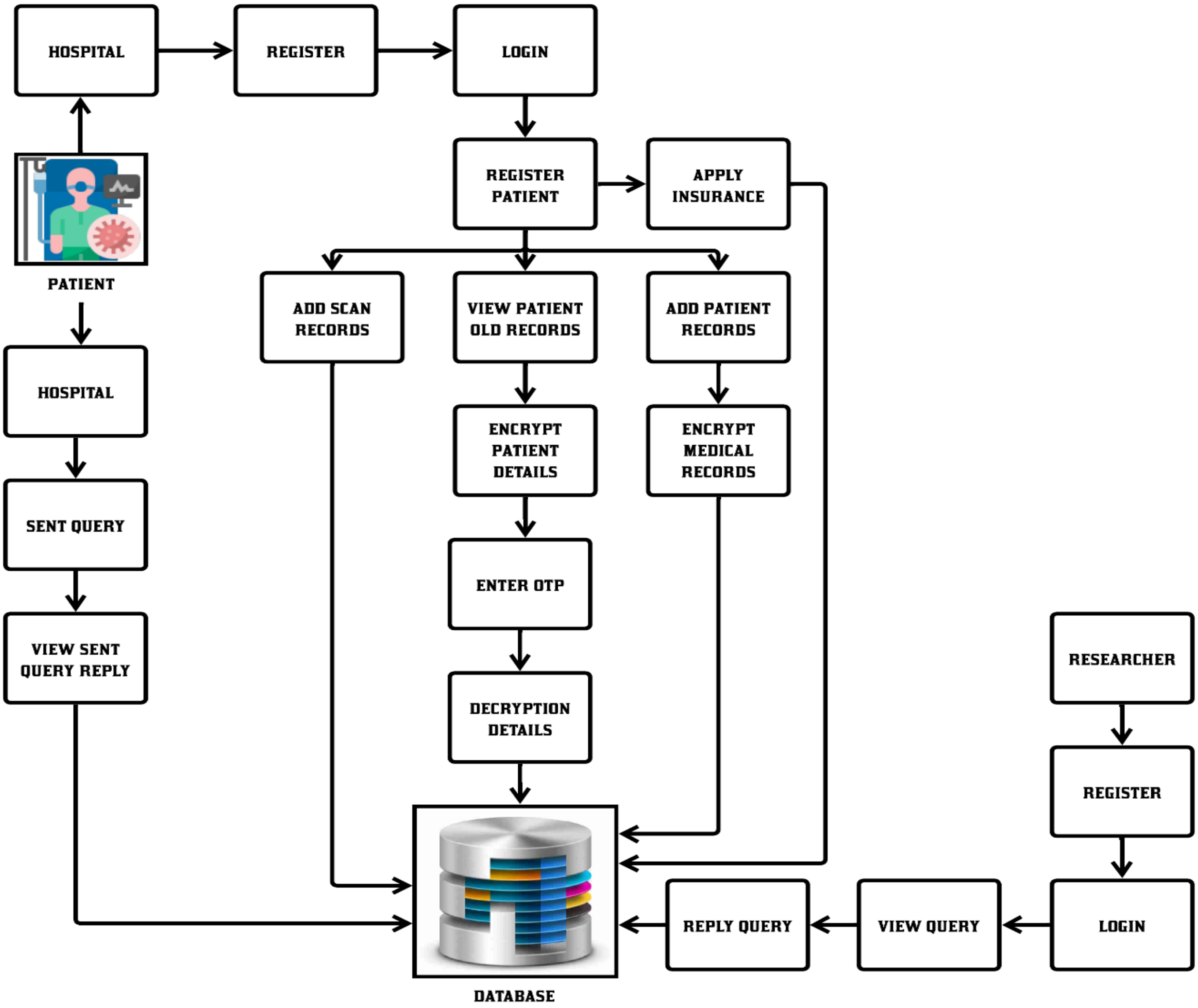
In an ABE system, patients encrypt their health records using specific access policies defined over a set of attributes. Only users whose attributes match the policy can decrypt the relevant portions of the data. This enables **fine-grained, role-based control**, allowing patients to selectively grant access to different users depending on the nature of the health information. A **trusted authority** is used to manage the generation and distribution of cryptographic keys, assign attributes to users, and ensure that the access policies are enforced correctly. The approach also supports **forward and backward access control**, meaning that changes in a user's permissions over time (such as revoking access) are handled securely and consistently.

While ABE addresses the issue of secure data sharing, it is equally important to **formally verify** whether the encryption system behaves as intended — especially in terms of access policy enforcement, data flow, and timing. This is where **High-Level Petri Nets (HLPN)** come into play. HLPN is a graphical and mathematical modeling tool used to describe and analyze the behavior of distributed systems. It extends basic Petri Nets by incorporating tokens that carry data values (not just plain tokens), enabling more expressive modeling. HLPN allows system designers to **simulate, verify, and validate** complex processes such as encryption, key distribution, and user access. In the context of the proposed ABE-based system, HLPN is used to formally represent the interactions between the cloud, patients, users, and the trusted authority.

By modeling the system with HLPN, researchers can identify potential issues like incorrect data flows, unauthorized access paths, or deadlocks. The simulation also allows for performance evaluation under various scenarios, such as increased user load or frequent policy updates. This ensures that the framework not only secures the data but also maintains system reliability and efficiency. HLPN thus plays a crucial role in both **design validation** and **system performance analysis**, making it a vital part of the overall security architecture.

In summary, the background of this research is rooted in the need for a secure, efficient, and verifiable method to store and share PHRs in untrusted cloud environments. By combining Attribute-Based Encryption with formal verification using HLPN, the proposed framework addresses critical concerns related to data confidentiality, access control, and system reliability. It aims to contribute a scalable and patient-centric solution to the growing demands of secure health information management in the digital age.

III. ARCHITECTURE



This architecture represents a secure cloud-based system designed for managing and sharing Personal Health Records (PHRs) among multiple stakeholders: patients, hospitals, insurance providers, and researchers. The system integrates Attribute-Based Encryption (ABE) to ensure that sensitive patient data is encrypted before storage and shared only with authorized users according to fine-grained access policies.

The system includes the following key components and workflows:

---

1. Patient Module

- **Patient → Hospital:**
  The patient initiates interaction by visiting the hospital for treatment or consultation.
- **Registration & Login:**
  Patients, hospitals, and researchers must register and log in to the system to access functionalities.
- **Register Patient / Apply Insurance:**
  After logging in, hospital staff can register a patient's details and apply for their insurance coverage in the system.
- **Add Scan Records / View Old Records:**
  Hospital staff can upload new scan records (e.g., X-rays, MRIs) or retrieve previous patient records.

- **Encrypt Patient & Medical Records:**
  Before storing any sensitive information, the system encrypts both patient personal details and medical records using Attribute-Based Encryption (ABE). This ensures only authorized users (based on their attributes) can decrypt and access the data.

2. Encryption and Access Control

- **Enter OTP (One-Time Password):** To access certain sensitive operations (like decryption or updating records), an OTP is required to enhance security.
- **Decryption Details:**
  Once the OTP is validated, authorized users receive the necessary decryption keys managed by the trusted authority, allowing them to access specific encrypted data.
- **Database Storage:**
  All encrypted data — including patient records, scan reports, and insurance details — are securely stored in the cloud database. The database is untrusted, meaning it cannot see or modify the actual data without the encryption keys.

3. Hospital-Patient Queries

- **Sent Query / View Sent Query Reply:**
  Patients can send medical queries to the hospital (e.g., about lab results or follow-up appointments).
- **Hospital Reply Query:**
  Hospitals respond to these queries, and patients can view the replies. All exchanges are logged in the system for accountability.

4. Researcher Access

- **Researcher Register / Login:**
  Researchers who need access to anonymized or permitted patient data for studies must register and log in.
- **View Query / Reply Query:**
  Researchers can submit queries (e.g., requesting aggregated or anonymized data) and view hospital responses. Importantly, they only receive data permitted under the access policy defined by patients or hospital administrators.

Key Security Features

Attribute-Based Encryption (ABE):
Controls access by enforcing policies based on user attributes (role, department, research permission, etc.), ensuring only authorized parties can decrypt and view sensitive data.

Trusted Authority:
Manages key generation, attribute assignment, and policy enforcement, preventing unauthorized data access.

Forward & Backward Access Control:
Ensures that when a user’s permissions are updated or revoked, their access to past or future data is securely adjusted.

OTP-Based Security Layer:
Adds an extra verification step before sensitive operations like decryption or data updates.

Secure Cloud Storage:
Even though the cloud server stores the data, it cannot interpret or misuse it due to the encryption mechanisms.

Query-Response Mechanism:
Allows structured communication between patients, hospitals, and researchers without compromising data privacy.

Role of High-Level Petri Nets (HLPN)

The system's workflows (e.g., registration, encryption, query handling) are formally modeled using High-Level Petri Nets. HLPN helps in:

- Simulating the flow of tokens (representing data or permissions) through system components.
- Verifying correctness (ensuring no unauthorized access paths exist).
- Identifying performance bottlenecks (e.g., during encryption or query processing).
- Validating timing constraints (ensuring OTPs and responses work within secure time windows).

By using HLPN, the design guarantees that the system meets both functional and security requirements under various scenarios

IV. CONCLUSION

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access pro-vided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we formally analyzed and verified the working of ABE methodology through the HLPN, SMT-Lib, and the solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the ABE methodology to securely share the PHRs in the cloud environment.

V. REFERENCE

[1] ANTONIO LOPEZ MARTINEZ , MANUEL GIL PEREZ , AND ANTONIO RUIZ-MARTINEZ, "A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario," VOLUME 11,September 2023.

[2]HUA SHEN,"EnhancingDiagnosis Prediction in Healthcare With Knowledge-Based Recurrent Neural Networks.," VOLUME11, September 2023.

[3],VISHWA AMITKUMAR PATEL , PRONAYA BHATTACHARYA , SUDEEP TANWAR , RAJESH GUPTA , GULSHAN SHARMA , PITSHOU N. BOKORO AND RAVI SHARMA "Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions" VOLUME 10, September 2022

[4]ABDULLAH AL MAMUN, SAMI AZAM AND CLEMENTINE GRITTI.,"Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction." VOLUME 10, January 18 2022.

[5] ALAA HADDAD, MOHAMED HADI HABAEBI , MD. RAFIQUL ISLAM , NURUL FADZLIN HASBULLAH AND SURIZA AHMAD ZABIDI.., "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems.," VOLUME 10, September 2022

[6]P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, ‘‘BinDaaS, ‘‘Blockchain-based deep-learning as-a-service in healthcare 4.0 applications,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[7]A. AwadAbdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O’Connor, and J. Laughton, ‘‘MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchang,’’ IEEE Internet Things J., vol. 8, no. 21, pp. 15762–15775, Nov. 2021.