Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Cloud Based Flexible Unified Fine Grained Access Control of Health Records

G. Vinoda Reddy
Professor, Department of CSE (AI & ML),CMR Technical Campus,Hyderabad ,Telangana, India

B Sirisha
Student, Department of CSE (AI & ML),CMR Technical Campus,Hyderabad ,Telangana, India

D Maniteja
Student, Department of CSE (AI & ML),CMR Technical Campus,Hyderabad ,Telangana, India

T Tejas Goud
Student, Department of CSE (AI & ML),CMR Technical Campus,Hyderabad ,Telangana, India

Abstract
Personal health records (PHRs) are important assets that require confidentiality, integrity and access control. ABE is one technology that could secure PHR in a cloud environment. Assembling PHR usually necessitates information from many sources, thus necessitating fine access control. ABE could help in controlling access to PHR. Other users would be able to exchange their PHR without them exposing their private data. This could be done through multi privilege access where key encryptions are generated and allowing the staff to access and store information at certain level, preserving patients' privacy. This paper's results show advances in PHR usability and efficiency and the potential to achieve S/S private requirements. Results show that Private Ciphertext-Policy Attribute Based Encryption Frameworks are capable of providing necessary security guarantees with simulations yielding promising results.

I. INTRODUCTION

Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing' is targeting to configure an effective and versatile access regulation model for the protection of sensitive health data in cloud computing and its applications. By means of context-aware fine-grained permissions, the control framework confirms that only properly cleared individuals can use the designated set of PHRs at any given time. The control framework combines state-of-the-art encryption technologies to safeguard data while in motion and while in storage as well as user authentication mechanisms such as multi-factor authentication (MFA) to give a more controlled and real-time identity verification. The system was developed in a way to be capable of interoperability with the current Healthcare Information Systems, Electronic Health Records and Cloud based health-care application without much hassle and integration issues using designed protocols and APIs.

This project provides for the requirements of scalability and optimization of performance to deal with enormous amounts of data and wide ranges of users while ensuring adherence to healthcare compliance like HIPAA, GDPR, HITECH etc. Compliance with regulations is maintained through regular audits and DA- assessments, data loss prevention technologies, continuous monitoring of the environment and other measures related to security policies. The project also reinforced other educative programs focusing on healthcare providers and patients in order to improve the security perception and make them trusting the PHR systems based on the cloud techniques.

II. RELATED WORK

The idea of unified fine-grained access to personal health records has been explored in various studies and papers, each contributing important methods and insights. Kaelber et al. (2008) [1] Identifies key priorities and challenges for PHR systems, including usability, privacy, and integration with healthcare systems.Abbas and Khan (2014) [2] Discusses the state-of-the-art methodologies, privacy challenges, and potential future research directions in e-health cloud systems. Highlights the trade-offs between data privacy, usability, and scalability. Discusses cryptographic techniques and privacy-aware frameworks.Focuses on challenges such as trust, policy enforcement, and revocation mechanisms.Abukhousa et al. (2012) [3] Identifies challenges like compliance with regulations (e.g., HIPAA), data integrity, and latency. Suggests frameworks to balance performance and privacy.Vilaplana et al. (2013) [4] Explores cloud applications in e-health, including telemedicine and PHR management. Evaluates cost-effectiveness, scalability, and reliability of cloud-based solutions.Wang et al.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

(2016) [5] Proposes a hierarchical ABE scheme for efficient access control over structured data. Improves encryption and decryption efficiency for large file systems. Useful for organizing PHRs with multiple hierarchical access levels.Li et al. (2016) [6] Introduces parallelization in ABE to enhance encryption performance. Targets large-scale datasets in cloud systems, reducing computational delays.Qian et al. (2015) [7] Proposes a multi-authority ABE scheme for better scalability and decentralization.Includes efficient user revocation mechanisms for dynamic access control.Guo et al. (2016) [8] Combines searchable encryption with ABE for secure and precise database queries. Enhances data confidentiality while allowing fine-grained search functionality. Liu et al. (2016) [9] Focuses on hiding sensitive access policies to enhance privacy in EMRs. Balances usability and privacy in cloud-based healthcare systems.These studies and resources form the foundation for our system helps us to design a unified fine grain access to PHRs that is accurate, efficient, and easy to use, all powered by Cloud Computing.

III. PERSONAL HEALTH RECORDS

In this paper, we develop a new Cipher text-Policy Attribute-Based Signcryption Scheme (CP-ABSC) as a novel security mechanism for the access control, data encryption, and message authentication in PHR system. We adopt attribute-based signature (ABS) as the signature part which allows a person to sign his/her PHR with his/her secret key if he/she possesses a set of attributes that satisfy the signing access structure. The concept of cipher text-policy attribute-based encryption (CP-ABE) is used as the encryption construction. CP-ABSC has two properties: signcryption (signature and encryption) and access control. By combining these two properties, CP-ABSC can provide data confidentiality, authenticity, unforge-ability, and collusion resistance required by PHR systems.

IV PROPOSED SYSTEM

A. Unified Framework

- The data access control framework, which yields a structure of multi-root tree. Every single-root sub-tree in the multi-root tree is a access policy. Every node along the sub-tree corresponds to a privilege level for accessing a certain part of the data, as well as the attribute of medical staff that can access the part of data.
- The root corresponds to the highest privilege and the associated attribute. Medical staff equipped with the attribute can access all the data associated with the subtree.

B. ABE Layer

- There are four algorithms in this layer to protect symmetric keys. They are AB-Setup, AB-KeyGen, Symmetric Key Packing and Symmetric Key Unpacking. AB-Setup is an initialization algorithm run by an AA. It takes as input a security parameter and outputs a public key PK and a master secret key MK.
- AB-KeyGen takes as input MK and the set of attributes A of a medical worker, and outputs the personal secret key SK associated with A. Symmetric Key Packing and Symmetric Key Unpacking provide the fine-grained access control of the symmetric keys.

C Cloud Computing Environment:

- Health data is stored off-site in a cloud infrastructure (e.g., AWS, Azure, Google Cloud).
- Access policies must be securely enforced without compromising patient privacy or violating compliance laws like HIPAA or GDPR.

IV.EXPERIMENTAL SETUP

A. Regression Analysis:

Regression analysis is a statistical method that models the relationship between a dependent variable and one or more independent variables. In this study, regression analysis is used to assess the efficiency and scalability of the proposed fine-grained access control framework for PHRs in cloud computing environments. The KPIs include encryption and decryption time, access control policy enforcement time, and system throughput under varying workloads.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

B. Data Collection

Controlled experiments were done to conduct the regression analysis and mimic the PHR management conditions in the real world. Independent variables involved users, the size of the datasets of PHRs, and complexity in access policies. Other dependent variables include the time for encryption, decryption time, and access request latency. To make it more reliable, a systematic variation in independent parameters is carried out for multiple iterations by collecting data points.

C. Dataset Description

The Unified Fine-Grained Access Control system dataset is structured to maintain and secure PHRs in the cloud. The attributes are

1. Users: This includes user IDs, roles, and encrypted password hashes for role-based access control implementation.
2. Health Records: Storing encrypted personal health data such as medical history and test results, ensuring the sensitive information is protected.
3. Access Control: Manages access permissions, monitoring access levels of each record for read/write permission, supporting fine-grained access control.
4. Audit Logs: Maintains audit trail of actions made on health records, including accesses and modifications to ensure regulatory compliance.
   The dataset prioritizes privacy and security with an opmization and encryption. Synthetic data is used during development and testing to validate access control, encryption protocols, and regulatory compliance effectively.

V. RESULTS AND DISCUSSION

Figure 1. Home Page

- This is the homepage interface serves as the gateway for users, offering a seamless login experience. Users input their credentials in designated fields, ensuring secure access to the platform.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

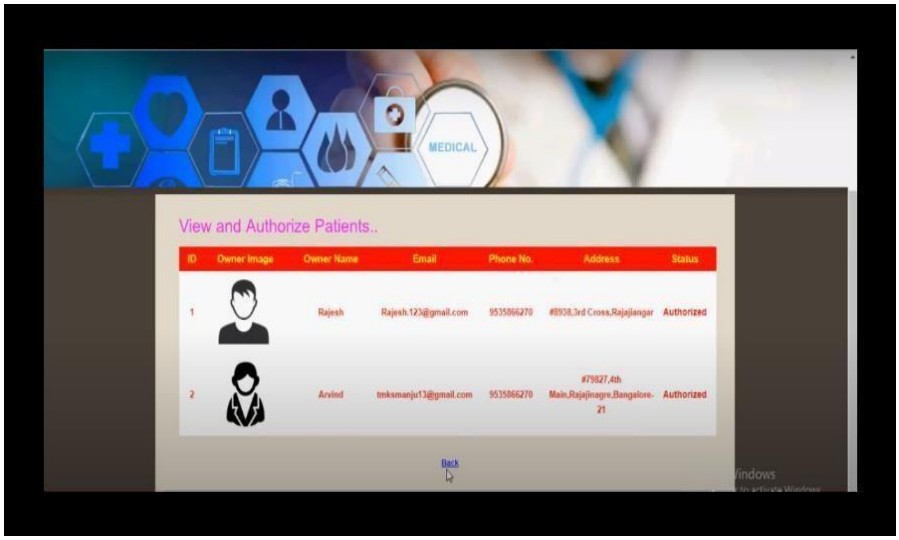

Figure 2. View And Authorize Patients

- The View and Authorize Patients page facilitates secure access for providers using their credentials. Users enter their login details in the designated fields, ensuring a streamlined and authenticated experience. With a focus on security and user-friendly design, the interface enhances the service provider's login process.

Figure 3. Patient register page

- The user registration page allows us to sign up a patient by providing necessary details. Users input their patient's information in the designated fields, ensuring a straightforward and secure registration process. With an emphasis on simplicity and data protection, the interface enhances the user's experience during registration.
- The Profile Datasets Trained and Tested Results page provides insights into the accuracy of the algorithm utilized in our personal health records. It presents the outcomes of training and testing phases, offering a comprehensive view of the algorithm's performance. This page serves as a key analytics tool, empowering users to assess the effectiveness of the employed algorithm in accurately identifying patient's age.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

VI CONCLUSION AND FUTURE SCOPE

The Unified Fine-Grained Access Control system offers the safe and efficient management of PHR in a cloud environment. Role-based access control and proper encryption techniques ensure that data is protected while still being accessible to the proper users which results in Potential improvements and Integration with national health systems. The front end was designed using React and the back end with Node.js and Express to ensure that the user interface is interactive and data is responsive. While the system shows robust functionality, performance, and security

Future development of the system should include the inclusion of machine learning algorithms for health data analysis, thereby making accurate predictions. The inclusion of emerging health technologies, such as wearable devices and telemedicine platforms, would offer a holistic approach to managing patient health. Cloud-native technologies can be utilized to enhance scalability, while multi-factor authentication strengthens security. Another critical aspect will be maintaining compliance with continually changing healthcare regulations, thus driving the system toward a smarter, more integrated, and secure platform for PHR management.

REFERENCES

[1] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds", IEEE J. Biomed. Health Informat., vol. 18, pp. 1431-1441, Jul. 2014.
[2] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton and D. W. Bates, "A research agenda for personal health records (PHRs)", J. Amer. Med. Informat. Assoc., vol. 15, no. 6, pp. 729-736, 2008.
[3] E. Abukhousa, N. Mohamed and J. Aljaroodi, "E-health cloud: Opportunities and challenges", Future Internet, vol. 4, no. 3, pp. 621-645, Jul. 2012.
[4] J. Vilaplana, F. Solsona, F. Abella, R. Filgueira and J. Rius, "The cloud paradigm applied to e-Health", BMC Med. Informat. Decision, vol. 13, no. 1, 2013.
[5] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.
[6] L. Li, X. Chen, H. Jiang, Z. Li and K. C. Li, "P-CP-ABE: Parallelizing ciphertext-policy attribute-based encryption for clouds", Proc. 17th IEEE/ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel Distrib. Comput., pp. 575-580, May. 2016.
[7] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation", Int. J. Inf. Security, vol. 14, no. 6, pp. 487-497, 2015.
[8] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu and K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-healthcare clouds", J. Med. Syst., vol. 40, no. 11, pp. 235, 2016.
[9] L. Liu, J. Lai, R. H. Deng and Y. Li, "Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment", Security Commun. Netw., vol. 9, no. 18, pp. 4897-4913, 2016.

C. Efficiency

Scheme based on the cpabe took-it which uses the Pairing-Based Cryptography library. Then experiments are conducted on a PC. For convenience we have assumed that the common access sub-tree's level is equal to the specific access tree's level. We also have defined the access policy tree depth is the common access sub-tree's level. We conduct the performance analysis between our scheme and conventional scheme under the metrics of running time, communication cost and storage overhead.

F. Results and Discussion

By combining all these techniques, we prove the correctness of the proposed scheme and analyze its security of confidentiality and unforgeability. Then we evaluate its performance in terms of access structure, key size, ciphertext size, and computation complexity.

G. Applications and Conclusion

Unified fine-grained access control for Personal Health Records in cloud computing offers enhanced security, privacy, and flexibility. By allowing users to define specific permissions at a granular level, it protects sensitive health data while enabling efficient and secure sharing among authorized parties. This model is essential in meeting regulatory requirements and maintaining trust between patients and healthcare providers. Additionally, it helps healthcare systems become more interoperable, supporting personalized care and improved patient outcomes.