Revocable Cloud Assisted Attributes Based Signcryption Using PHR

M, Mohamed Rafi, V.Abdul kadar
Head of the Department, Mohamed Sathak Engineering College. Kilakarai
Final MCA, Mohamed Sathak Engineering College. Kilakarai

Abstract- **In cloud-assisted personal health record (PHR) systems, managing access control securely and efficiently is a crucial challenge. This project introduces a Revocable Cloud-Assisted Attribute-Based Signcryption (RCA-ABSC) scheme that combines Attribute-Based Encryption (ABE) and Signcryption. The system ensures data confidentiality, integrity, and fine-grained access control. A key feature is the revocation mechanism, allowing for dynamic user revocation without re-encrypting the entire dataset. The design supports lightweight policy updates, leveraging cloud infrastructure to reduce computational burden while maintaining high security standards, making it suitable for real-time, scalable health data sharing applications.**

I. INTRODUCTION

The exponential growth in digital healthcare systems has necessitated secure and efficient management of sensitive personal health information. PHR systems allow individuals to manage and share their medical data with authorized entities. However, traditional security mechanisms often fall short in providing flexible and scalable access control. To overcome this, our system integrates a lightweight policy update scheme and ABE-based signcryption that supports user revocation. This ensures dynamic access control with reduced computational overhead, enhancing data privacy and integrity in cloud-based healthcare environments

II. LITERATURE SURVEY

1.Title: A Systematic Literature Review of Attribute-Based Encryption in Health Services
Author: Raza, S., et al.
Year: 2022
Explanation:
This comprehensive review provides an in-depth analysis of the utilization of Attribute-Based Encryption (ABE) in the context of healthcare services, a sector where the protection of sensitive data is paramount. The paper begins by outlining the fundamental principles of ABE, emphasizing its ability to enforce fine-grained access control—a crucial requirement in healthcare environments where different users (e.g., doctors, nurses, insurance providers) need varying levels of access to electronic health records (EHRs).

The review categorizes and compares different types of ABE schemes, including Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), explaining how each can be leveraged to achieve controlled data sharing. Special attention is given to their implementation in real-world healthcare applications, where issues such as computational efficiency, scalability, and ease of policy management play a critical role.

2.Title: Survey on Secured Health Care Data Sharing on Cloud Using Revocable Attribute-Based Encryption Schemes
Author: Pavani, S., & Sahayadhas, A
Year:2021
Explanation:
This survey provides a focused exploration of revocable Attribute-Based Encryption (ABE) techniques specifically designed for the secure sharing of healthcare data within cloud-based environments. As healthcare systems increasingly migrate to the cloud to enhance accessibility and reduce infrastructure costs, the need for robust and flexible access control mechanisms becomes critical. A core challenge in this domain is the revocation of user access rights—particularly ensuring that users who no longer have authorization (such as former employees or withdrawn third-party partners) cannot continue to access sensitive health records.

The paper delves into this issue by examining the limitations of traditional ABE schemes, which often lack efficient mechanisms for revoking access without re-encrypting the entire dataset or redistributing keys to all users. Such approaches can

be both computationally intensive and administratively burdensome, especially in large-scale healthcare systems where policy updates and user access changes are frequent.

3. A Survey on Ciphertext Policy Attribute-Based Encryption Scheme Based Cloud E-Healthcare Secure Framework
Author: VGurupriya, K. G., & Aneeshkumar, A. S.
Year:2023
Explanation
This paper provides a comprehensive examination of the role of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in enhancing security within cloud-based e-healthcare systems. CP-ABE is particularly well-suited to healthcare environments because it allows data owners to define and enforce access control policies directly within the encrypted data itself. This capability ensures that only users possessing a matching set of attributes—such as role, department, or specialization—can decrypt and access specific medical information.

The study highlights the critical need for fine-grained access control in electronic healthcare systems, where different users—doctors, nurses, administrators, and insurance providers—require different levels of access to patient data. Traditional encryption methods often lack the flexibility to accommodate these nuanced access requirements, whereas CP-ABE offers a more dynamic and scalable solution. By embedding access policies into the ciphertext, CP-ABE minimizes reliance on centralized access control lists, thereby reducing the risk of data leaks and unauthorized access.

In addition to outlining the theoretical framework of CP-ABE, the paper explores its practical implications and current limitations. Key challenges discussed include policy update management, scalability, and computational overhead on resource-constrained devices. The authors propose several enhancements to the CP-ABE model to address these concerns, such as incorporating lightweight cryptographic operations, policy versioning, and hierarchical access structures that reflect real-world healthcare workflows.

2.1 EXISTING SYSTEM

In current healthcare data security systems hosted on the cloud, conventional encryption techniques—namely symmetric and asymmetric cryptography—are frequently used to protect sensitive information However, these traditional approaches are not well-suited for environments that require fine-grained access control, dynamic user management, and scalability. Most systems rely on role-based or identity-based encryption methods, which lack the flexibility to accommodate changing access policies for diverse users. A major limitation arises during user revocation; when a user's access rights need to be removed, the system typically demands that the entire dataset be re-encrypted or that new keys be redistributed to all remaining users. This process is resource-intensive, both computationally and in terms of communication overhead.

In addition, authentication is often handled separately through digital signatures, which increases system complexity and makes integration more cumbersome. Many cloud-based healthcare platforms also rely heavily on centralized key management, creating a single point of failure and raising the risk of security breaches. Without a unified mechanism that seamlessly integrates encryption, access control, and authentication, these systems struggle to provide both efficiency and robust protection for sensitive health information.

2.2 PURPOSE OF WORK

The primary objective of this project is to design a robust and efficient framework for sharing Personal Health Records (PHRs) within a cloud computing environment. This system is intended to overcome common challenges such as ensuring that access to sensitive medical data is both secure and flexible, allowing permissions to be updated dynamically as user roles change. By incorporating a unified signcryption technique—combining encryption and digital signature into a single process—the model enhances both data confidentiality and authentication. Additionally, it introduces mechanisms for revoking access rights without the need to re-encrypt the entire dataset, thereby minimizing administrative overhead. This integrated approach aims to simplify the system's architecture while significantly reducing the computational resources required, making it suitable for real-world healthcare applications where performance, security, and scalability are critical.

III. PROPOSED SYSTEM

The proposed solution introduces a streamlined and secure approach to updating access control policies for Personal Health Records (PHRs) stored on cloud platforms. As users increasingly rely on third-party cloud services to store and share their medical data, safeguarding privacy and maintaining control over who can access this information becomes a major concern. This model addresses these issues by using lightweight cryptographic techniques that enable policy updates—such as granting or revoking access—without needing to re-encrypt the entire dataset. This not only preserves the confidentiality and accuracy of health information but also reduces the computational load on the system.

Designed with adaptability and scalability in mind, the system is particularly suitable for environments where access rules change frequently. It leverages proxy re-encryption, allowing cloud servers to update encrypted data in line with new access policies without exposing the actual content. This method reduces dependency on the data owner while supporting efficient and secure data management across large user groups. Furthermore, the system integrates auditing and tracking capabilities, enabling users to monitor access logs and policy modifications. These features improve transparency and reinforce trust, making the platform more reliable for managing sensitive healthcare data in distributed cloud environments.

IV. TEMPORAL PATTERN LEARNING MODULE

The Temporal Pattern Learning Module plays a vital role in identifying irregular events in video streams by analyzing both spatial and temporal data patterns. This module is particularly effective in healthcare monitoring systems, where continuous observation of patients is essential. Initially, the system preprocesses raw video inputs by extracting frames, resizing them for uniformity, and normalizing pixel values to remove noise. These preprocessed frames are then arranged sequentially to retain the time-based structure of the events.

To extract meaningful features, Convolutional Neural Networks (CNNs) are employed to analyze spatial information within individual frames, while Long Short-Term Memory (LSTM) networks capture the temporal dependencies between consecutive frames. This combination allows the system to learn typical behavior patterns over time, making it capable of identifying deviations that signify potential anomalies, such as sudden movements, falls, or unusual patient activity.

Once the features are learned, the anomaly detection engine computes an anomaly score for each sequence, comparing current observations to the expected normal behavior. If the score exceeds a defined threshold, the system flags the event as abnormal. This scoring mechanism relies on reconstruction errors or discrepancies in sequence prediction, ensuring accurate detection.

V. MODULES

1. Administrator:
The administrator manages doctor accounts by adding, viewing, or deleting their records,including personal and professional details.
2. Doctor Login:
The doctor logs in to create patient profiles and upload medical and prescription details.
3. New Patient:
In this module, the doctor enters new patient details such as name, blood group, gender, address, contact number, username, and password. Once the patient approves the upload, the data is encrypted using a user-generated key and stored on the server.
4. Upload Status:
In this module, the doctor checks whether patient records have been encrypted and uploaded based on the user-generated key. It also allows viewing encrypted data and removing unnecessary patient entries.
5. Accept Request:
In this module, users can approve a doctor's access request, allowing the doctor to add health and prescription details, which are then encrypted with the user’s key and stored on the server.
6. Revoke Doctor:
This module enables users to revoke access, preventing the doctor from viewing or updating their records on the server.previously granted

VI. RESULT AND CONCLUSION

In summary, the proposed Lightweight Policy Update Scheme for managing Outsourced Personal Health Records (PHRs) in the cloud offers an effective approach to secure and flexible data sharing. It incorporates strong encryption techniques, real-time

policy updates, and robust user authentication to safeguard sensitive health information while allowing access based on specific user roles. This dynamic access control mechanism helps reduce processing overhead, improving both system performance and user experience. As a result, healthcare professionals can retrieve important patient data quickly, supporting timely and accurate medical decisions.

Additionally, the system aligns with privacy regulations such as HIPAA and GDPR, reinforcing its commitment to data protection. Utilizing JavaScript for the frontend ensures a smooth and user-friendly interface that can easily integrate with existing web platforms. Altogether, this solution provides a practical and secure method for managing PHRs in cloud environments, representing a valuable step forward in digital health information systems

VII. FUTURE ENHANCEMENTS

Future research on the Lightweight Policy Update Scheme for Outsourced Personal Health Records (PHRs) Sharing will prioritize improving the system's scalability and flexibility to effectively manage an expanding user base and growing data volumes. This could involve investigating the application of distributed ledger technologies like blockchain, which offer enhanced data integrity, security, and transparency for access control mechanisms. Moreover, incorporating machine learning techniques may enable the system to analyze and predict user access patterns, facilitating more adaptive and intelligent updates to access policies tailored to user behavior and specific needs. Additionally, ongoing work will focus on optimizing the user interface and overall user experience, striking a balance between maintaining simplicity and incorporating sophisticated functionalities to ensure the system remains user-friendly as it evolves.

REFERENCES

[1] Haifeng Li (2020) proposes a secure and efficient data sharing scheme specifically designed for mobile cloud computing environments. The scheme emphasizes fine-grained access control, allowing data owners to precisely define who can access specific parts of their data. By focusing on lightweight cryptographic techniques, the approach ensures that security measures do not overly burden mobile devices, which typically have limited computational resources. This balance between strong security and low resource consumption makes the solution particularly well-suited for mobile users who rely on cloud services to store and share sensitive information.

[2] In the 2024 study published in the International Journal of Research Publication and Reviews (IJRPR), Arjumand Afroze presents a novel approach for securely sharing data and enabling authorized searches within e-Health systems. The research addresses the critical need for protecting sensitive medical information by designing a secure framework that restricts data access to verified users only. This method ensures that healthcare data can be shared efficiently while maintaining strict privacy controls and preventing unauthorized retrieval, thereby improving the overall security and reliability of digital health services.

[3] In his 2022 study published in HCIN, Arvind Panwar proposes a blockchain-based framework designed to enhance the security of Personal Health Records (PHR) stored within an IBM Cloud-based data lake. This approach leverages the decentralized and tamper-resistant features of blockchain technology to ensure data integrity, privacy, and controlled access to sensitive health information in cloud environments.

[4] In a 2024 systematic literature review published by MDPI, Parisasadat Shojaei examines the various security and privacy challenges associated with technologies used in health information systems. The study provides a comprehensive analysis of existing methods and frameworks aimed at protecting sensitive health data, highlighting key vulnerabilities and proposing strategies to enhance the confidentiality and integrity of healthcare technologies.

[5] In the 2021 article published by MDPI, Remya Sivan explores the critical issues of security and privacy in cloud-based e-health systems, emphasizing the importance of protecting sensitive patient data from unauthorized access and ensuring secure data storage and transmission in cloud environments

[6] In her 2020 article published in *Frontiers*, Nina Schwalbe discusses the concept of data sharing within the context of global public health, aiming

to clarify the meaning and scope of “data” to improve collaboration and decision-making in health initiatives worldwide.

[7] Teng Cao, "Enhancing the Functionalities of Personal Health Record Systems: Empirical Study Based on the HL7 Personal Health Record System Functional Model Release 1 ", JMIR, 2024.

[8] Sugantha Lakshmi, "secure health record sharing using collaboration based multi user access with revocation", IRJMETS, 2024.

[9] José A. García-Berná, " Automated Workflow for Usability Audits in the PHR Realm", MDPI, 2022.