Hidden Cipher text Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System

Sowmya J

Associate Professor

Department of Computer Applications

The Oxford College of Engineering

sowmyaj@theoxford.edu

NAVYA SHREE B A

PG Student

Department of Computer Applications

The Oxford College of Engineering

navyareddy087@gmail.com

ABSTRACT

The presence of adequate protection of data confidentiality and efficient access control in a PHR system is of the essence. Hidden cipher text policy is one of the techniques that conceals this access control policy within the encrypted data, thus adding privacy and security to the data, making it invisible to those not authorized as it is decrypted. Attribute-Based Encryption is a methodology whereby the user's secret key and the ciphertext are functions of specific attributes, and access is granted only if the user's attributes match up with an access policy which is encoded in the ciphertext. Personal Health Records represent the electronic systems that manage and share health information of individuals in a secure and private way. Decryption Efficiency: the process in which decryption receives the optimization to recover a ciphertext into plain text with lesser consumption of time and computational resources. Data Confidentiality: a certain assurance that access to information of a sensitive nature is restricted only to those persons who have the necessary authorizations, hence protecting it against unauthorized access and disclosure. Access Control: about mechanisms for identifying users and granting or denying permissions against rules predefined and agreed upon, so that access to information becomes available only to authorized persons. Finally, cryptographic security refers to the technology used in protecting data integrity, confidentiality, and authenticity using encryption and decryption methods to protect information from unauthorized access and detecting its actual sources.

Keywords: Python, Django, MySQL, Angular

INTRODUCTION

Given the digitized health records today, the confidentiality and security of PHR are very critical to maintain. Traditionally, although encryption mechanisms have proved really effective, it often falters on access control management and decrypting efficiency in dynamic environments. One such promising solution is Hidden Cipher Text Policy ABE: an enhancement of security and performance. This encryption scheme involves advanced cryptographic techniques securing health data and ensuring efficient decryption processes for any user who needs access.

HCP-ABE is an extension of ABE, which involves a hidden cipher text policy, greatly enhancing the security in the data. In traditional ABE systems, the access control policies are always embedded within the cipher text; this may leak some sensitive information regarding the policies. This risk is mitigated by HCP-ABE, which conceals the policies in the cipher text to reduce the chance of unauthorized inference, hence improving security. That will ensure that only users with appropriate attributes would have the capability for decrypting the data without exposure of policy details to probable attackers.

Decryption efficiency is also important in PHR systems, where timely access is critical to health records in healthcare. In conventional ABE schemes, the decryption time is slow due to complex cryptographic operations. HCP-ABE provides optimizations that make the decryption process clear, faster, and fit for real-time applications. HCP-ABE makes use of advanced techniques, such as precomputation and efficient data structures, reducing computational overhead with regards to decryption to near minimal, hence improving responsiveness in terms of user experience.

Implementing HCP-ABE in PHR systems will require its integration with existing health information systems, which have to fulfil a myriad of access control requirements. To ensure smooth integration and operation, HCP-ABE requires proper policy design, key management, and system architecture. It further requires the stakeholders to consider issues of the scalability of the system, user management, and interoperability of other health information technologies. Even with such flaws, the improved security and fast decryption offered by HCP-ABE present it as an attractive system for modern PHR systems.

It improves the cryptographic security for Personal Health Records through defending access by concealed policies and optimizations in decryption. In this way, a strong protection mechanism will definitely help in protecting sensitive health information and efficiently managing access. In other words, while the PHR system keeps evolving further, adoption of HCP-ABE would form a critical part for enhancing the security and functionality of digital health record management.

LITERATURESURVEY

[1] In their ground-breaking 2010 paper, "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data," S. Yu, C. Wang, and W. Lou presented a solid framework for Attribute-Based Encryption (ABE) that has significantly influenced subsequent advancements in the field. Their approach was designed to provide fine-grained access control over encrypted data, a feature that is particularly essential for Personal Health Record (PHR) systems, where it is necessary to manage different levels of access effectively. This pioneering work underscored the critical role of using attribute-based policies to safeguard sensitive health information.

[2] On top of that foundation, A. Sahai and B. Waters laid the groundwork with Ciphertext-Policy Attribute-Based Encryption through their very influential 2005 paper entitled "Fuzzy Identity-Based Encryption." They gave a scheme that provided a way for encrypting data based on a set of policy defined by attributes, which PHR systems would find very useful. Their work is notable in that it has brought flexibility to attribute-based encryption and introduced the really original idea of policies that are dynamic regarding different user roles and permissions.

[3] G. Ateniese, K. B. Frikken, and R. H. Greenstadt performed further work in 2007 with the paper entitled "Attribute-Based Encryption for Cloud Storage and Services". It further extends the applicability of CP-ABE in more practical settings of cloud storage environments, such as PHR systems where health records are maintained and accessed via cloudbased settings. Their work was oriented towards the refinement of methods of encryption in

EXISTING SYSTEM

Traditional applications in the PHR system face problems managing health data in an effective way. Less control over data, insufficient features for interaction between the healthcare service provider and user, and difficulties in correcting medical errors are some of the issues reflecting a flaw in current systems. Specifically, these PHR systems can be inefficient in access control management and privacy protection, which may bring about a potential loss of data, and the key generation processes are really slow. Hidden Cipher Text Policy Attribute Based Encryption with Fast Decryption will make a system for handling sensitive health information safer and more efficient if integrated.

Merits of the Current System:

Patient-Centric Health Management: It provides patients with more information about their health and various conditions so that they may attract more personalized attention for their problems.

Improved Safety of Patients: The system would improve patient safety and provide quality healthcare through proper recordkeeping and management.

Disadvantages of the Current System:

- **Challenges of Error Correction:** Most of the available systems completely miss medical errors and cannot correct them; the inaccuracies remain uncorrected.
- **Problems with Accessibility:** PHRs are modestly accessible to patients for the purpose of health data management. ✞ **Little Support for Health Literacy:** Fewer resources are available to help patients understand and use records of their health data, leaving an open door for health literacy gaps.

PROPOSED SYSTEM

In the proposed PHR system, the public parameters are fixed, but the attribute universe is enormously large. In this system, a large array of messages can be managed and validated efficiently by an optimized decryption mechanism.

Management of these attributes by this decryption key is very important for secure processing and access based on predefined policies.

It provides robust security through a dual encryption framework with static supposing. The data is stored in an encrypted form that ensures concerns regarding the integrity of the data are very minimal and the chances of loss of information are reduced. The design of the system incorporates a mechanism that dynamically modifies the accuracy of the data structures; each format is being processed by the method of encryption to ensure appropriate access control. This design embeds the access structure within the private key to provide much-needed security and functionality.

This is certainly true, with a rewording of the benefits of the proposed PHR system as follows:

Benefits of Proposed System

1. Improved Accuracy: The system refines data management accuracy and thus maintains health records more effectively.

2.Better Patient-to-Provider Relationships: By providing better data handling and access control features, the system promotes better communication and thus relations between patients and their healthcare providers.

3. Improved Quality of Care: Enhanced data security and better accessibility, thereby promoting quality care through better decision-making.

4. Reduced Costs: Flexibility in architecture and efficient management features in handling health information, especially handling huge data volumes.

METHODOLOGY

1. System Design and Framework:

- **Fixing Public Parameters:** Set, in the first place, fixed public parameters to be used in the whole system. These parameters shall be used to lay a base for the processes of encryption and decryption.
- **Define Attribute Universe:** Develop an all-inclusive attribute universe to handle the wide range of health data attributes. This ensures that the system is managing and validating a large number of attributes effectively.

2. Encryption and Decryption Process:

- **Dual Encryption Approach:** Incorporate a dual encryption framework to improvise data security. The information would be encrypted twice to make it very secure from unauthorized access.
- **Optimization of Decryption Mechanism:** An optimized decryption mechanism shall be designed to manage and validate effectively the encrypted message. Optimization is necessary due to bulk health data.

3. Data Management and Accuracy:

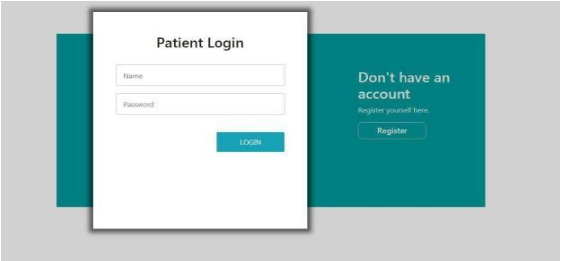
- **Dynamic Adjustment of Data Structure Accuracy:** A mechanism

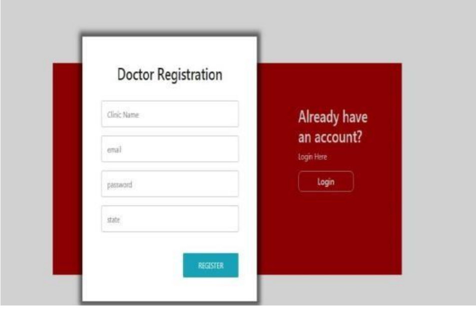
- shall be developed that will adjust dynamically according to the methods used for its encryption, the accuracy of the data structures. This will ensure that data remains accurate and accessible under different conditions.

4. System Implementation and Integration:

- **Hidden Cipher Text Policy Attribute-Based Encryption:** Hidden Cipher Text Policy Attribute-Based Encryption shall be implemented to enhance personal health records' security and management. This technique has a significant share in solving some of the prevalent security issues.
- **Fast Decryption Techniques:** Fast decryption techniques should be adopted so that the accessed data in the ciphertext form may be decrypted quickly, hence improving the system's performance.

RESULTS





CONCLUSION

The development of robust features in scenarios in which secure and adaptive management of PHRs is required must be coupled with access control mechanisms to enhance the protection of personal health information through the regulation of 'view' and 'modify' authors of records. The information present in PHRs is very private, hence, unauthorized access is a major concern in this regard. "Indeed, individuals need to take care, since their control of access to health records significantly affects security. In addition, it is difficult for the users to correct errors inside PHR records, which clearly calls for a dependable and safe system. Changes in security policies may defeat the assurances given for PHR data, which further underlines the requirement for robust and adaptable security measures.".

PHR systems have numerous benefits, such as sharing health-related information, managing medications, and integration of medical history. The system is effective in improving and further empowering and informing the patient with very important information regarding their health and the options to be taken regarding treatment. Community-based implementations of PHR systems could have the ability to use computer cloud storage and the web in managing and handling health information effectively and securely. This development ensures access to the health data, management of them across different platforms securely, and general improvement on the delivery of health care.

Besides, through the PHR systems being able to monitor and analyse the real health behaviour, it aids in justifying the health expenditure and improving system efficiency. It also improves data management and transparency, and, therefore, this supports better decision making and consequently, the development of strategies on matters concerning health. Continued improvement and development of applications of PHR underscore its significance in the growth of health practices so that the users can benefit from a coordinated and secure health information network.

FUTURE ENHANCEMENT

One can enhance digital security and privacy through the integration of new technologies with the electronic health systems. The advanced techniques of encryption and decryption can offer users more control over their personal health data. Such technologies ought to be implemented and integrated properly, validation carried out as rigorously as possible, to ensure high standards. The developed products require standardization of data formats at all times to reduce the effort and make them more effective during software development. The proposal will take care of the refinement of the project, its compatibility with existing systems, and data integrity and security.

The primary motivation of this exercise is to deal once and for all with security issues related to management of the keys and procedural complexities. Since personal health information is very sensitive, effective security measures are hence much needed for the protection of privacy. The security framework can be enhanced by assessing the needs for health resources and by employing standardized techniques for encryption and decryption. These strategies will reduce probable vulnerabilities and thus will be helpful in protecting the privacy of health information. Further work in this regard will be done through continuous improvement of these security measures, since both threats and technology evolve over time, with consequent improvement of the protection and security of personal health data.

REFERENCES

1.M. Qutaibah, S. Abdullatif, „„„ciphertext -policy attribute based encryption ciphertext size and fast decryption,‟‟‟ ACM Asia Conf. CS, Communication, Apr. 2017

2.Bethencourt, Sahai, and Waters,„„„Cipher text-policy attribute based encryption,‟‟‟ IEEESymp, Security, Privacy,May.2007

3.Goyal, Pandey, Sahai, „„„Attribute-based encryption with grained access control of encrypted data,‟‟‟13thACMConf. CS, Communication, Nov. 2006

4.www.strokeback.eu/deliverables/StrokeBack

5.www.researchgate.net/figure/Cloudbased-PHR-system