Grenze International Journal of Engineering and Technology, June Issue

Crypto Care: Secure Health Vault in the Cloud

Hemanth Kumar R[1] and E. Sujatha[2]
[1]Department of Computer Science and Engineering, Saveetha Engineering College (Autonomous), Chennai, India
Email: Kingonly2511@gmail.com
[2]Professor, Department of Computer Science and Engineering, Saveetha Engineering College (Autonomous), Chennai, India
Email: sujathae@saveetha.ac.in

***Abstract*— The Personal Health Record (PHR) acts as a central repository for health information, often managed by third-party cloud providers. However, this raises privacy concerns as sensitive personal health data could be exposed. To address this, we propose innovative data control mechanisms specifically designed for PHRs hosted on semi-trusted servers. Utilizing Attribute-Based Encryption (ABE) techniques, we encrypt eachpatient's PHR file, drawing from previous research on secure data outsourcing. Unlike existing methods, our focus lies in streamlining core management for PHR users and owners across different scenarios. By employing Multi-Authorization ABE, we ensure robust patient privacy while facilitating access policies, dynamic attribute adjustments, user/attribute overrides upon request, and emergency mirror access. Our studyincludes comprehensive analytical and experimental assessments to validate the safety, scalability, andeffectiveness of our proposed approach.**

***Index Terms*— PHR, ABE, Personal Health**

I. INTRODUCTION

In recent years, personal health records (PHRs) have become increasingly prevalent as a patient-centeredapproach to managing health high information. PHR services offer patients the ability to consolidate, organize, and monitor their personal health data through online platforms, simplifying the storage, retrieval, and sharing ofmedical information. A fundamental aspect of PHR services is the empowerment of patients, granting them full control over their health records and the ability to share this information with various parties, including healthcareproviders, family members, and friends. However, alongside the potential benefits, the implementation of PHR services encounters significant challenges related to security and privacy. A primary concern revolves around ensuring patients' control over the storage and dissemination of their sensitive personal health information (PHI)on third-party servers, which may not always be fully trusted. Additionally, given the sensitivity of PHI, third- party storage servers are susceptible to malicious activities, posing risks of data breaches and exposure. For example, the theft of the Veterans Affairs Database, containing data on millions of military veterans, underscores the severity of such security breaches. To mitigate these challenges and maintain centralized privacy control overpatients' PHRs, it is crucial to implement fine-grained data control mechanisms that operate effectively with semi-trusted servers. An effective approach involves encrypting PHR data before outsourcing, allowing PHR owners to define encryption methods and access privileges for each file. Access to PHR files is then restricted to authorized users who possess the appropriate decryption keys, thereby safeguarding privacy against unauthorizedaccess. To enhance the protection of PHI stored on semi-trusted servers, we propose the adoption of attribute-based encryption (ABE) as the primary encryption technique. ABE enables the implementation of access policies based on user or data attributes, allowing

Grenze ID: 01.GIJET.10.2.223

patients to specify access privileges for PHR files using predefined attribute sets, rather than specifying individual users explicitly. Importantly, the computational complexity of encryption, key generation, and decryption in ABE scales linearly with the number of attributes involved, ensuring efficiencyand scalability. In our comprehensive analysis, we thoroughly evaluate the complexity and scalability of the proposed secure PHR sharing solution across various metrics, including computing resources, communication overhead, storage requirements, and key management. Furthermore, we conduct comparative assessments with existing approaches, considering factors such as complexity, scalability, and security. Finally, we validate the effectiveness of our scheme through implementation and experimentation/simulation on modern computing platforms.

II. Related Work

Author introduced Predicate Based Encryption (PBE) in 2011, merging Attribute Based Access Control (ABAC) with asymmetric encryption. This technique ensures secure cloud data handling by allowing a single encryptor/multiple decryptors setup. Author identified 43 security challenges and corresponding techniques, with confidentiality being the most emphasized aspect.

In the same year, author proposed a security framework called Parity Based Partially Distributed File System (PDFSP) to enhance confidentiality, integrity, and availability in cloud storage. Author suggested a Data Centric Security approach based on the Chinese Remainder Theorem, focusing on data-level security management.

Author outlined five techniques for cloud data security, including innovative key management and privacy-enhanced keyword search. Author suggested using RSA encryption and MD5 algorithm to enhance data security in cloud computing.author proposed an Advanced Secret Sharing Key Management Scheme for decentralized key management.

Author discussed ID-Based Cryptography and CloudaSec as cryptographic mechanisms for securing cloud data. Author introduced Access Control and Data Confidentiality (ACDC) for enforcing access control policies. author (2016) presented Enhanced Mutual Trusted Access Control Algorithm (EMTACA) to ensure mutual trust between cloud users and service providers.

Author focused on security policies for cloud computing, aiming to protect users and data, minimize risks, and ensure compliance with regulations.

III. System Analysis

To safeguard personal health information stored on semi-trusted servers, our strategy revolves around implementing attribute-based encryption (ABE) as the primary encryption technique. This method enables access policies based on user or data attributes, empowering patients to designate specific PHRs among users by encrypting files using attribute sets. This obviates the necessity for a complete user list. Notably, the complexity associated with encryption, key generation, and decryption scales linearly with the number of attributes involved. However, integrating ABE into large-scale PHR systems poses challenges, particularly in terms of basic management capabilities, such as dynamic policy updates and effective revocations. We conduct a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution across various metrics, including computing resources, communication overhead, storage requirements, and key management. Furthermore, we compare our approach with previous methodologies in terms of complexity, scalability, and security. Subsequently, we validate the efficacy of our scheme through implementation and experimental simulation on a contemporary workstation, demonstrating its suitability for real-world scenarios.

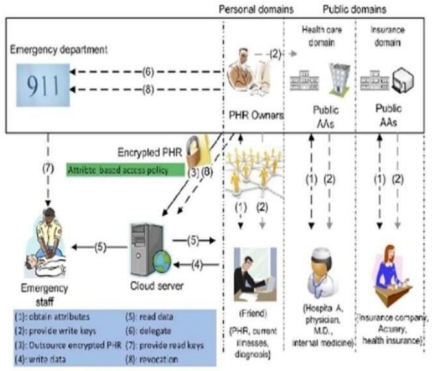

Fig.1. Architectural Diagram

IV. Existing System

The trend towards outsourcing or providing Personal Health Record (PHR) services via third-party providers, such as Microsoft Health Vault, often stems from the substantial expenses associated with constructing and maintaining dedicated data centers. While achieving universal access to PHR services is a commendable goal, various security and privacy concerns pose significant obstacles to their widespread adoption. A notable challenge lies in the limited control patients have over the sharing and storage of their Personal Health Information (PHI) on third-party servers, which may lack complete trustworthiness. The inability of patients to actively manage their PHI represents a significant barrier to the widespread uptake of PHR services. Worries regarding the confidentiality and integrity of sensitive health data stored on third-party servers contribute to user apprehension. The absence of guarantees that their PHI will be handled securely and accessed solely by authorized parties may lead individuals to hesitate in entrusting their health information to external service providers. Moreover, navigating the landscape of regulatory compliance and legal frameworks governing PHI handling further complicates the adoption of PHR services. Compliance with stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, imposes intricate requirements and obligations on both service providers and users. The risk of non-compliance with these regulations carries severe penalties and legal ramifications, dissuading users from embracing PHR services offered by third-party entities. To overcome these barriers to adoption, a paramount focus must be placed on implementing robust security measures and transparent privacy policies that empower users with greater autonomy over their PHI. The deployment of advanced encryption protocols, stringent access controls, and comprehensive audit trails can significantly enhance data security and instill user confidence in the safeguarding of their sensitive health information. Additionally, building trust through transparent communication and unwavering adherence to regulatory standards can play a pivotal role in assuaging concerns and fostering widespread acceptance of PHR services.

A. Disadvantages of existing system

Privacy concerns arise due to the potential exposure of personal health information (PHI) to third-party servers and unauthorized parties. Incidents like the theft of a database from the Department of Veterans Affairs, containing PHI of 26.5 million military veterans, highlight the risks associated with centralized systems. This incident occurred when an employee took the data home without authorization. The reliance on a single trusted authority (TA) in existing systems poses significant drawbacks. This approach not only creates a bottleneck but also raises privacy concerns as the TA has access to all encrypted files, compromising privacy. Additionally, assigning all attribute management tasks to a single TA is impractical and inefficient.

V. Proposed Work

To address these challenges and control patient access to their Personal Health Records (PHRs), we propose a new patient-centric framework and a set of data control mechanisms for PHRs stored on semi-trusted servers. Our approach utilizes attribute-based encryption (ABE) to encrypt each patient's PHR file, ensuring fine-grained data control. By leveraging ABE, access policies are based on user or data attributes, allowing patients to select PHRs among users without needing the full user list.

A. Advantages of proposed system

Our focus is on scenarios involving multiple data owners and dividing users in the PHR system into several security domains. This significantly reduces the complexity of basic management for owners and users. We address the shortcomings of existing systems by proposing a unified security framework for sharing PHRs with patients in a multi-user, multi-domain, multi-authority PHR system. Our framework captures application- level requirements for both public and private use of a patient's PHR and distributes user beliefs to multiple entities, reflecting reality more accurately. Each PHR file is encoded with a special fine-grained and role-based access policy for Potential Utility Density (PUD) users and a set of selected data attributes allowing access to Potential Security Density (PSD) users. Only authorized users can open the PHR file without logging into the server.

VI. Testing Analysis

System testing is a pivotal phase in ensuring the success of a system. It involves the practical testing of the system within an organizational context to pinpoint and rectify errors, thereby ensuring that the system functions seamlessly as intended. Through meticulous examination of all connections and functionalities, system testing validates the accuracy and efficiency of the new system. Its primary aim is error detection, underscoring the importance of providing valid login credentials for unlocking processes to facilitate successful testing.

Each module undergoes thorough testing, followed by integration to assess the final system using specially designed test data. This exhaustive testing procedure aims to showcase the system's ability to operate successfully under diverse conditions. Inadequate testing or its absence may lead to latent errors surfacing months later, potentially causing delays and compromising the integrity of system files and records.

VII. ALGORITHM

Attribute-based encryption (ABE) is a widely used encryption method where the user's secret key and ciphertext are determined by attributes such as country of residence or subscription type. However, a notable security aspect of ABE is combination resistance, where an adversary holding multiple keys can access data if at least one key permits it. In our context, encryption should intelligently regulate access to encrypted data, necessitating a novel approach as conventional ABE lacks this capability.

VII. FUTURE ENHANCEMENTS

Our framework aims to streamline the management and access of Personal Health Records (PHRs) at the patient's center. By segregating the system into multiple security domains (public and private), we cater to diverse user data access requirements. Professional User Domains (PUDs) comprise users logging in based on their professional roles, while Potential Security Density (PSD) users are linked with data owners and access PHRs based on access rights assigned by the owner.
We employ ABE in our approach to implement cryptographically secure, patient-centric PHR access for both PUDs and PSDs. PUDs utilize multi-authority ABE, whereas PSDs utilize key-policy ABE. This multidisciplinary approach effectively models different user types and access requirements, ensuring encrypted PHRs remain secure even when stored on semi-secure servers. Our enhancements to ABE facilitate efficient user engagement and access control.

IX. CONCLUSION

Our project introduces a novel framework for the secure sharing of Personal Health Records in cloud computing. By harnessing encryption techniques, particularly ABE, patients can assert full control over their privacy, ensuring patient-centricity. Addressing challenges encountered by PHR owners and users, our framework significantly reduces management complexity while enhancing privacy assurance. Through implementation and simulation, we showcase the scalability and efficiency of our solution.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient- Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] "TheHealth InsurancePortability and AccountabilityAct,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283- 287, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.