Phoenix: International Multidisciplinary Research Journal
Vol 1, No. 2, April-June, 2023
ISSN:2583-6897

ATTRIBUTE BASED ENCRYPTION FOR SECURE SHARING OF E-HEALTH DATA

[1]***Rohini,*** *Master of Computer Application BKIT-Bhalki*
[2]***Prof. Sunil Sangme,*** *Master of Computer Application BKIT-Bhalki*

Abstract -In recent years, there has been a tremendous expansion of distributed computing. A lot of data are sent over the internet and stored on open cloud servers that are located in faraway locations. These servers cannot be relied on completely by customers, which is particularly problematic considering that an ever-increasing number of businesses may need to manage their data with the assistance of cloud servers. However, when the data that are re-appropriated in the cloud are unstable, the issues of security and assurance end up constricting the overall game plan for cloud-based frameworks. The purpose of this work is to provide a plan for the secure sharing of data in order to safeguard the safety of data proprietors and address the security concerns associated with information sharing. The examinations of both the set upend plan's security and productivity demonstrate that it is viable and efficient to implement. In the last part of this article, we will discuss its potential applications in electronic health records. Many hospitals and other medical facilities have difficulty adopting cloud-based Electronic Health Record (EHR) systems because of the potential for data breaches and the subsequent loss of patient information that would arise from such a breach. When it comes to the adoption of electronic health records in the healthcare business, the most important barrier to entry is the patient's right to privacy as well as the protection of their information from unauthorized access. As a result, there is an urgent need for the development of an appropriate system for the administration of cloud-based EHR Services that are safe, secure, and simple to use. A secure cloud-based electronic health record storage system is offered in this article as a solution to the aforementioned issues. According to this system, a patient's information will be encrypted and stored on a cloud server in a safe manner using the attribute-based encryption (ABE) method.

***Key Words*:** Attribute based encryption for secure sharing of E-health data

1.INTRODUCTION

The rapid development of technology, particularly in the field of medical sciences, has contributed to the transformation of healthcare organizations into settings that are centered on the needs of patients. These organizations are on a mission to achieve higher standards of excellence. This cannot be accomplished without having access to high-quality information whenever it is needed [1].

According to the International Organization for Standardization (ISO), an Electronic Health Record (EHR) is the storage, secure exchange, and access to patient information in digital format by multiple allowed users. This information is accessed by many authorized users. This data comprises information about the patient's history, present, and potential future. The goal

of electronic health records is to facilitate the upkeep of health care that is both integrated and efficient [2].

An electronic version of a patient's health history that captures all of the pertinent clinical facts over a period of time [3] and is maintained by healthcare practitioners is referred to as an electronic health record, or EHR for short. These electronic health records assist companies in providing better healthcare services by automating the access to and administration of patient information.

When establishing EHR, some of the hurdles that might be faced are those that are technological, organizational, human, financial, and moral-legal in nature [4]. These barriers can be classed as such. As a result of this, the use of modern technologies like cloud computing is an effective method for ensuring that its successful execution is carried out. The term "cloud computing" refers to the processing that was carried out by a network that was comprised of several distant servers. Simply expressed, cloud computing is the practice of acquiring computing resources by means of the Internet [5, 6]. This practice results in the centralized storage of data as well as online access to services and computer resources.

The use of cloud-based electronic health record systems has been hampered by the prevalence of safety and privacy concerns in recent years. In the United States of America, compliance with HIPAA (Health Insurance Portability and Accountability Act) [7] is sometimes stated as the necessity to safeguard the confidentiality of medical data, including EHRs. [Note: HIPAA stands for the Health Insurance Portability and Accountability Act]. Even when access restrictions are in place, cloud service providers cannot be trusted to retain electronic health records (EHRs) without encryption [8, which is why encryption of EHRs must be needed in cloud-based EHR systems.

2. Literature survey:

1)A Patient-Centric Attribute Based Access ControlScheme for Secur..e Sharing of Personal HealthRecords Using Cloud Computing”

AUTHORS: Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk

Personal health records, often known as PHRs, are an emerging paradigm for the interchange of health information. This model makes it possible for owners of PHRs to easily and effectively communicate their private health data with a range of users, such as medical professionals and members of the patient's family and friends. PHRs are often outsourced and kept on the cloud platforms provided by third parties. This frees PHR owners from the responsibility of maintaining the data included inside their PHRs while also increasing the accessibility of health information. Outsourcing confidential health data, on the other hand, creates major privacy issues due to the increased likelihood that confidential health information may be disclosed to third parties who are not authorized to receive it. It has been suggested that personal health record (PHR) owners should use attribute-based encryption (ABE) procedures

to maintain ownership of any PHR data that is outsourced. Nevertheless, such present PHR solutions are hampered by a lack of access flexibility, particularly as a result of the constraints associated with ABE processes. In this article, we present a patient-centered, attribute-based PHR sharing scheme that may allow flexible access not only for professional users like physicians but also for personal users like family and friends. This scheme is patient-centric, and it is based on attributes. In the method that has been presented, each PHR file is encrypted before being uploaded to a cloud storage service for healthcare, and this service also houses an attribute-based access policy that regulates who may see encrypted resources. We utilize an attribute-based authorization method to approve access asking users to access a certain PHR resource based on the associated access policy. At the same time, we employ a proxy re-encryption scheme to make it easier for authorized users to decrypt the necessary PHR files. This allows us to comply with the requirements of the associated access policy. In addition, we have proved that the suggested system is capable of resolving the problems with access inflexibility that are connected with the already existing ABE-based PHR sharing schemes, all while preserving a sufficient degree of security and privacy.

2) "Removing Barriers in Using Personal Health Record Systems"

AUTHORS: Mohammad Alyami, Yeong-Tae Song

A personal health record, often known as a PHR, is regarded as an essential component in the process of improving patient outcomes. However, the rate of adoption by the general population in the United States is still rather low. We conducted a survey of publications from 2008 to 2016 that were connected to personal health record systems (PHRS), and we divided the results of that survey into six distinct categories, including motivation, hurdles, ownerships, interoperability, privacy, security, and portability. Our goal was to determine the factors that prevent people from using PHRs. In this research, we suggest a framework that may assist remove such hurdles and incentivize individuals to use PHRS so that they can manage their health by monitoring and managing their clinical data using PHRS. This would allow them to manage their health more effectively.

3)Dynamic Access Policy in Cloud Based Personal Health Record (PHR) System

AUTHORS Xuhuiliu,Qinliu"

An ever-increasing number of customers are switching to personal health record (PHR) systems that are hosted in the cloud as cloud computing has become more widespread. Existing research suggests encrypting patient health records (PHRs) before outsourcing them because of the intimate connection between the PHR and patient confidentiality. By using the forward and backward derivation functions, comparison-based encryption, also known as CBE, was the first encryption method to incorporate temporal comparison within the context of an attribute-based access control. However, due to the following reasons, CBE cannot be immediately applied to cloud-based PHR environments: To begin, there is a linear relationship between the

amount of characteristics in the access policy and the cost of the encryption. Second, the costs of communication and calculation that are incurred by the owner of the data when the policy is updated are significant. We first present a hierarchical comparison-based encryption (HCBE) scheme that integrates an attribute hierarchy into CBE. This will allow us to quickly construct a dynamic access policy for protected health records (PHRs) in cloud environments. When encrypting a ciphertext, the HCBE method uses a limited number of generic qualities at a higher level rather than a large number of specialized attributes at a lower level. This results in a significant increase in the performance of the encryption. We begin by constructing a dynamic policy updating (DPU) scheme by making use of the proxy re-encryption (PRE) method. This scheme is built on the HCBE scheme, which serves as its basis. By outsourcing policy updating activities to the cloud, the DPU approach is able to prevent the transmission of ciphertexts and decrease the computation burden on the data owner. For the purpose of determining whether or not the strategies that we have presented are effective, a comprehensive set of experiments based on simulated data have been carried out.

4)Distributed clinical data sharing via dynamic access-control policy transformation

AUTHORS: F. Rezaeibagha, Y. Mu

The exchange of information within electronic health record (EHR) systems is essential to the enhancement of the standard of care that is provided. However, the sharing of data has resulted in certain security and privacy issues. This is due to the fact that patient medical records might potentially be accessed by a wide range of users, which could result in patients' privacy being compromised. Without finding a solution to this problem, widespread adoption and sharing of electronic health record data would be impossible. Encryption has often been used as the approach of choice for solving problems of this kind. Encryption may be used for access control, however it cannot be used for sophisticated EHR systems since these systems need many domains (for example, public and private clouds) with varying access requirements.

3. OBJECTIVE:

This study was carried out to address the security and privacy issues of EHR data sharing with our innovative access-control mechanism. This mechanism captures the scenario of the hybrid clouds and the need of access-control policy transformation, and it was designed to provide secure and privacy-preserving data sharing among different healthcare enterprises.

4. SYSTEM ANALYSIS:

Existing System:

"The sender of a message can indicate an identity in the IBE, and only a recipient with a coordinating personality will be able to decrypt the message." The encryptor does not need to provide a separate key to decode each individual figure's data, which distinguishes this method from public-key encryption. When a client enters the IBE framework, the private key—which

includes the holder's identity—is only ever provided to that client a single time. This happens when the client joins the framework.

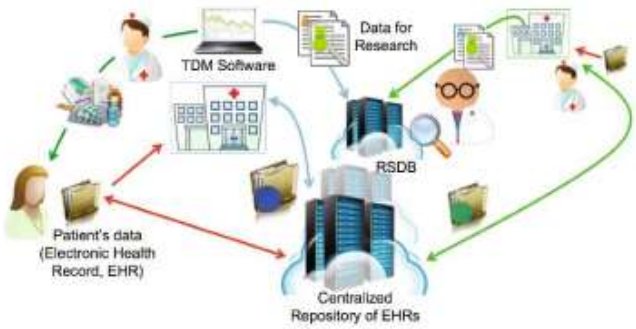
The owner of the information encrypts the information that is stored in the cloud using a certain encryption method, and they provide access to the customers using certain specialized components. There are certain locations of parts, and the clients are confined to those locations; also, each part has its own set of permissions that are allocated to it. Only the customer, equipped with a certain component, will be able to decode the information, which the cloud service provider will not have access to themselves.

The job of a data user is to take encrypted data and, using the private key that was given to him by the authority, decrypt it so that he may access the data that he needs.

Proposed System

The purpose of this work is to provide a plan for the secure sharing of data in order to safeguard the safety of data proprietors and address the security concerns associated with information sharing. The examinations of both the set upend plan's security and productivity demonstrate that it is viable and efficient to implement. In the last part of this discussion, we will examine its use in electronic health records.
Because of this, the person who encrypts data has the highest level of power about the encryption policy. In addition, the private keys that have already been distributed will never be changed, even if the whole system is compromised. In this study, we have presented a multi-authority system, in which each user is assigned an ID, and users are able to communicate with each key generator (authority) using multiple pseudonyms. The security of cloud storage is improved with this multi-authority approach by having the cloud server do proxy re-encryption.

4. ARCHITECTURE



Depending on the information that is stored, several kinds of e-health cloud models may be open, private, hybrid, or community-based. Access control techniques are necessary because EHR information is considered sensitive and because it contains patient data that are stored on servers maintained by a third party. Access control is a security obstacle that maintains data

privacy by limiting the functioning of and access to healthcare documents inside the healthcare system. This is accomplished via the use of confinement. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity-Based Access Control (IBAC) are the three strategies that are used in the access control processes of healthcare information systems. The job of providing responsibilities to clients for the purpose of gaining data access may be accommodated by role-based frameworks (16). ABAC [17], which makes use of cryptographic and non-cryptographic techniques, while IBAC makes use of an identity-based encryption mechanism that use client identification for the purpose of data encryption.
Sharing of information is an important aspect of e-health systems in particular. It is very possible for it to be shared across a variety of stakeholders, such as healthcare providers, emergency clinics, medicinal services groups, and so on.

6. Results and Analysis:

We took into consideration a number of the patients' reports that had been submitted inside the application. And the patients decide who has access to their information by granting authorization to various users. Now you need to determine the amount of time needed by both the current system and the new system.

File Id	File Title	File Size (Bytes)	No of Permissions	Proposed Time (µs)	Existing Time (µs)
121	Blood Report	24860	3	228	686
122	Sugar Report	24860	1	189	189
123	XRay Scans	132139	2	245	491
124	Test Report	666961	2	208	417
125	Citiscan Report	24860	3	182	547

Because it is not user specific, the suggested method takes much less time for the production of attribute keys, as is seen from the graphs that follow. However, with the system that is currently in place, the production of the property takes much more time since it must be updated for each authorization transaction.

Conclusion:

Depending on the information that is stored, several kinds of e-health cloud models may be open, private, hybrid, or community-based. Access control techniques are necessary because EHR information is considered sensitive and because it contains patient data that are stored on servers maintained by a third party. Access control is a security obstacle that maintains data privacy by limiting the functioning of and access to healthcare documents inside the healthcare system. This is accomplished via the use of confinement. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity-Based Access Control (IBAC) are the three strategies that are used in the access control processes of healthcare information systems. The job of providing responsibilities to clients for the purpose of gaining data access may be

accommodated by role-based frameworks (16). ABAC [17], which makes use of cryptographic and non-cryptographic techniques, while IBAC makes use of an identity-based encryption mechanism that use client identification for the purpose of data encryption.
Sharing of information is an important aspect of e-health systems in particular. It is very possible for it to be shared across a variety of stakeholders, such as healthcare providers, emergency clinics, medicinal services groups, and so on.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1] Wing P, Langelier M, Continelli T, and Armstrong D. The HIM workforce and workplace - 2002- member survey data for decisions. 2003 edition published in Chicago by the American Health Information Management Association.
[2] According to Sittig DF and Singh H. Defining health information technology and associated errors: New advancements made after the publication of To Err Is Human. 2011; 171(14):1281–4 from Arch Internal Medicine.
[3] K. Hayrinen, K. Saranto, and P. Nyk'anen, "Definition, structure, content, use, and impacts of electronic health records: a review of the research literature," published in the International journal of medical informatics, volume 77, issue 5, pages 291–304, in the year 2008.
[4] Nima Mirani, Hamid Ayatollahi, and Hamid Haghani. An investigation of the challenges confronting Iran's efforts to create and use electronic health records. Journal of Health Administration, Volume 50, Issue 15 (2017), Page 3.
[5] Buyya R., Yeo C.S., Venugopal S., Broberg J., and Brandic I.
The concept, the hype, and the reality of offering computing as the fifth utility are discussed in relation to cloud computing and developing IT platforms.
Future Generation computer systems, 2009, volume 25, number 6, pages 599-616.
[6] Kanagaraj G, Sumathi AC. [Transcription]. A proposal for an open-source cloud computing system to facilitate the transfer of medical pictures inside a hospital information system. In Trends in Information Sciences and Computing (TISC), IEEE's Third International Conference, 2011, Pages 144–9.
[7] The Department of Health and Human Services of the United States of America.
Privacy of Patient Health Information, 2011.
R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina are referred to in reference number 8. Keeping tabs on your data while it's stored in the cloud requires you to outsource compute but not control. In the Proceedings of the 2009 ACM workshop on Cloud Computing Security, it was abbreviated as CCSW '09 in 2009.
[9] M. Joshi, S. Mittal, K. P. Joshi, and T. Finin wrote an article titled "Semantically rich, oblivious access control using abac for secure cloud storage," which was published in Edge Computing (EDGE), 2017 IEEE International Conference on. IEEE, 2017, pages 142–149.

[10] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," published in the IEEE Internet of Things Journal, volume 3, number 5, pages 637–646, 2016.
[11] In the proceedings of the thirteenth annual ACM conference on computer and communications security is a paper titled "Attribute-based encryption for fine-grained access control of encrypted data." This paper was written by V. Goyal, O. Pandey, A. Sahai, and B. Waters.
The ACM, 2006, pages 89–98.

BIOGRAPHIES (Optional not mandatory)

Description about the author1
(in 5-6 lines)