JOURNAL OF NORTHEASTERN UNIVERSITY
Volume 26 Issue 01, 2023 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

AUTHORITY ACCESS CONTROL ON HEALTH CARE RECORD MANAGEMENT SYSTEM

D.Mobeen[1], Vasundra S[2]

[1]PG Scholar, Jawaharlal Nehru Technological University Anantapur, Ananthapuramu
mubeendariyabhai117@gmail.com
[2]Professor,JNTUA College of Engineering,Anantapuramu,Constituent college of Jawaharlal Nehru Technological University Anantapur, Ananthapuramu
Vasundras.cse@jntua.ac.in

Abstract
A personal health record, also referred to as a PHR system, is a sophisticated medical database that can be accessed by both patients and medical professionals. This type of database is known as a PHR system. On the other hand, there is always the possibility that unauthorized users or semi-trusted third parties will gain access to personally identifiable health information. The purpose of this application is to propose a patient-centered PHR sharing architecture that respects patients' right to privacy while also giving them full authority over their own medical information (PHRs). Under this architecture, all protected health records (PHRs) are encrypted utilizing multi- authority attribute-based encryption prior to being outsourced. This eliminates the need for key hosting and enables access control that is more granular to be applied to PHRs. In addition, a proposal has been made for an anonymous authentication between the cloud and the user. The objective of this proposal is to maintain the integrity of data that is stored on the cloud without revealing the identity of the user at any point during the authentication process. It is possible for encrypted PHRs to withstand attempts at collusion and to not be forged during the entirety of the sharing process, which strengthens the patients' control over their personal health records (PHRs).

Keywords: Anonymous authentication, attribute-based signature, multi-authority attribute-based encryption, personal health record.

I. INTRODUCTION

A new piece of technology called a Personal Health Record (PHR) has emerged in recent years. Data exchange has been greatly facilitated by this technological advancement. A personal health record (PHR) is an electronic health record that both patients and physicians may keep in a central place and access from anywhere. But when PHR is put into practise, it presents extra issues like privacy loss, which is the case anytime data is shared. As a means of protecting patient privacy and giving them more say over their own medical records, attribute- based encryption (ABE) is being pushed as a hot topic in the realm of fine-grained access control for sharing data. Since it is based on attribute-based encryption (ABE), this is the case (PHR).
Attribute sets of users need to be in accordance with ABE's access rules before PHR may be accessed by those users. The characteristics of the private key or cypher text generation procedure determine this policy. PHR is only available to users with conforming attribute sets.

Submitted: 13/01/2023 **Accepted**: 30/01/2023

However, some earlier approaches relied on a centralised authority to both produce keys and confirm user identities, which inevitably led to a system overload. This was a major flaw of the previous approaches. This issue may be remedied by using a multi-authority encryption method. Private keys for users in this system must be generated by a group of authorities working in tandem. We designed a dependable access control system that can function in a setting with many authorities, yet users' sloppy authentication might compromise data privacy. We successfully installed a reliable and safe access control system in an environment with many authorities. To further guarantee the existing strong security of a PHR system, It was suggested that we use a public key encryption method that might be indexed by search engines as an extra. In addition, authentication methods were implemented to link verified healthcare professionals to one another. Both of these enhancements were implemented to further strengthen the system's robust security. There are practical answers to both the issue of patient privacy being breached and the challenge of keeping the scheme's details secret. The same setting provides these answers. The user's privacy is protected using these techniques when they are engaging with the system. The identification of the user and their individual characteristics are two examples of the kinds of data that might be included in this category. New studies are beginning to investigate the feasibility of concealing the access control policy in situations when it must include private user data. In certain cases, the access policy may include sensitive information about individual users. However, they all require some amount of inefficiency in order to be practical. Technology that may be used either online or offline enables users to quickly acquire the decrypted ciphertext. As a result, less processing is required, and customers enjoy a great improvement in convenience. Personal Health Record (PHR) encryption based on several authorities' attributes raises a number of issues, including as the risk of collusion between users and authorities, the difficulty of forging ciphertext, and the potential of anonymous authentication outsourcing. Because of the nature of the PHR, several difficulties arise.

II. LITERATURE REVIEW

[1] X. Yan, H. Ni, Y. Liu and D. Han, (2019), “Privacy-preserving multi- authority attribute-based encryption with dynamic policy updating in PHR,”. PHRs, a new patient-centered health record, may allow users to share their medical history online. The PHR system uses Attribute-Based Encryption (ABE), a unique public key cryptosystem, to fine- tune the release of outsourced encrypted data. PHR created a multi-authority attribute-based encryption system with dynamic policy updating to address privacy and legal issues. Each patient attribute has a name and a value. We'll conceal user attribute values for privacy. LSSS's access structure and policy- updating algorithms allow policy modifications of any structure (based on "and," "or," or "not"). Under the baseline assumption, the approach is safe against a chosen-plaintext attack. The scheme's lower processing cost and smaller secret key and ciphertext are particularly useful for the PHR system, which had previously relied on more cumbersome approaches.

[2] D. Li, J. Liu, Q. Wu and Z. Guan, (2019), "Efficient CCA2 secure flexible and publicly verifiable fine-grained access control in fog computing,". IoT designs reduce latency for real-time devices and applications. Edge computing relieves cloud centre servers with network edge servers. Data access controls still risk IoT security. MA-ABE controls cross- domain encryption access. IoT features and technological requirements shape our fine-grained revocable vast universe multiauthority access control solution. The user's initialization stage now handles the most time-consuming encryption steps by splitting the algorithm into online and offline encryption and adding a reusable ciphertext pool. To decrease decryption's computational strain, many major activities are moved to network-edge servers. Dynamic permission revocation occurs. It also verifies ciphertexts. This reduces system load by keeping and communicating just the proper ciphertext. The chameleon hash function makes the approach CCA2-secure under the q- DPBDHE2 assumption. The performance research shows that the proposed IoT edge computing strategy works.

[3] X. Zhou, J. Liu, Q. Wu, (2018), "Privacy preservation for outsourced medical data with flexible access control,". The significance of electronic medical records (EMRs) in modern healthcare systems is crucial. Privacy protection for the EMR system is essential since patient records usually include a lot of personal information. Commonly used systems nowadays will only provide access to a patient's EMR if the user's job qualifies under the access policy. But with these current techniques, an opponent may easily connect individual patients with their respective physicians. Consequently, illness categories associated with patients are disclosed to opponents without such adversaries having access to patients' EMRs. We provide two anonymous methods of dealing with this issue. Both data privacy and user anonymity may be attained with their help. If an attacker is able to determine potential targets before gaining access to the EMR system, then the first strategy achieves a reasonable level of security. The second method provides perfect safety, with attackers selecting specific EMR nodes to attack in an adaptive fashion. Our schemes have been rigorously shown to be secure and anonymous. We also provide a method for finding EMRs in a hidden system, so that their owners may look for them without revealing their identities. We employ an online/offline strategy to process data more quickly and improve the user experience. The experimental findings demonstrate that key creation and EMR encapsulation might take milliseconds.

[4] M. Yang, T. Zhang, (2018), "Efficient privacy-preserving access control scheme in electronic health records system,". The storage of electronic health records (EHR) on the cloud is a crucial innovation with the potential to revolutionise healthcare delivery. However, there are other worries about the privacy and safety of EHR data. If a malevolent user were to acquire access to the EHR data, not only would it result in a privacy breach for the patient, but it might also have an impact on the doctor's ability to properly diagnose the patient. Maintaining complete privacy while maintaining ownership of one's electronic health records (EHR) is a difficult challenge. In this article, we provide an alternative PPAC strategy for electronic health records. To provide granular control over who may see EHRs, we signcrypt information using

the access policy of linear secret sharing schemes and an attribute-based signcryption (ABSC) method. It is possible that the cuckoo filter might be used to safeguard the EHR owner's private information by concealing the access policy. The security analysis further demonstrates that the proposed system is provably safe under the decisional bilinear Diffie-Hellman exponent assumption and the computational Diffie-Hellman exponent assumption in the standard model. In addition, the performance study shows that the suggested method maintains the privacy of the EHR's owner while having lower communication and computation costs than similar systems. Thus, the suggested technique is more appropriate for EHR.

III. METHODOLOGY

Existing System:

- The currently used authentication comes from a brand-new attribute- based signature that can be accessed both online and offline.
- Encrypted PHRs may be made collusion-resistant and unforgeable during sharing, giving patients more control over their data.

Drawbacks:

- ✓ Expensive
- ✓ It provides less security.
- ✓ When the authorized users increase, the system does not work efficiently.

Proposed System:

Before being outsourced, in this architecture, all PHRs use a multi- authority attribute-based encryption system. This allows for granular control over who may access PHRs and does away with the requirement for key hosting. In addition, a suggestion for anonymous authentication between the cloud and the user has been developed to ensure the security of cloud-based information without revealing the user's identity. This novel attribute-based signature may be utilised online or offline and is the basis for the proposed authentication method. Patients have more control over their PHRs since encrypted PHRs can't be falsified or used in a collusion attack during the sharing period (PHRs). Decryption that is done both online and offline, as well as that which is outsourced, helps to cut costs associated with calculations and boosts operational efficiency.

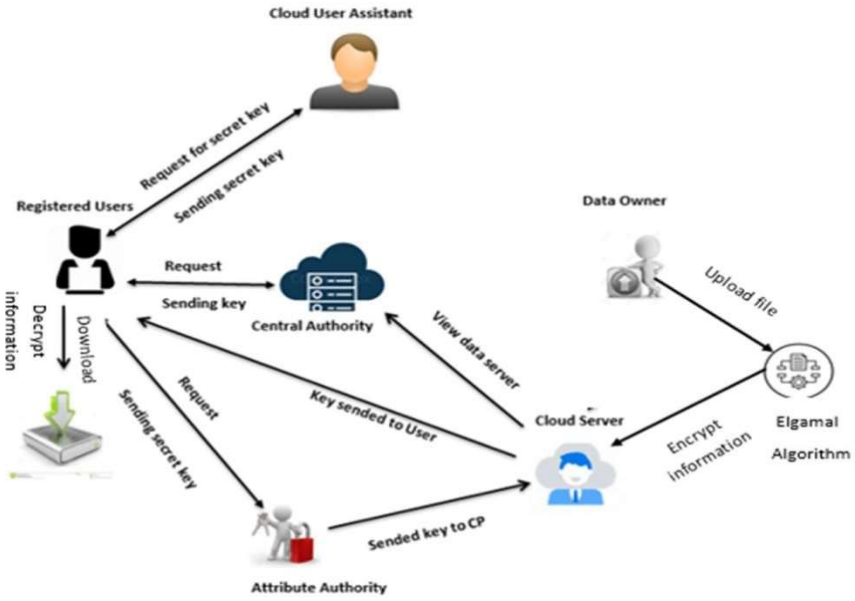

Figure 1: Proposed analysis block diagram

ElGamal

For safe two-way communication between computers, the ElGamal cryptosystem is a widely used cryptographic method based on the ideas of public and private keys. Public and private keys are used in order to encrypt and decode data, making this a kind of asymmetric method. The client employs the public key to encrypt the communication, and the server's private key may be utilised to decode it. To encrypt and decode data, this technique is highly regarded since its keys are so difficult to guess. This approach might successfully safeguard the message transaction against MITM, which is the primary motivation for adding the signature in the first place.

ALGORITHM

Round keys, a specialised kind of key derivation, are used in the encryption process. These, along with other operations, are performed on an array of data consisting of a single block of data (the encrypted data). The name "state array" was coined for this collection of elements.

To encrypt a 128-bit block using aes, you must do the following steps:

- Round keys can be calculated from the cypher key.
- First, load the block information into the state array (plaintext).
- To the initial state array, add the key from the first round.
- Nine iterations of state manipulation are required.
- Complete the tenth and last phase of state control manipulation.
- The encrypted data is a copy of the final state array (ciphertext).
- Because the tenth round requires a little different manipulation than the others, it has been

stated as "nine followed by a final tenth round."

- In this case, the 128-bit encryption key is simply a sequence of bits that make up the block. Given that AES expects numbers to be in bytes, we must first transform the 128 bits to bytes. Yes, we use the word "convert," but in all likelihood it was previously stored in this format. RSN/AES operations are carried out on a byte array with four rows and four columns. Those initial 16 bytes of data at the beginning of the encryption process.

Advantages:

- It provides high security.
- Even with high number of authorized users, the system can work efficiently.
- Cannot know the information about the encrypted data hence data confidentiality is maintained.

Applications:

Used by patients and doctors for better protecting their health data when stored in cloud.

System analysis:

In this stage, As part of our feasibility analysis, we provide a business proposal summarising the big picture of project and preliminary cost estimates. During system analysis, we will examine how feasible it is to implement the proposed system. This safeguard helps to ensure that the proposed system won't put an undue financial strain on the company. In order to do a realistic analysis, it is essential to have a firm grasp of the system's fundamental requirements.

There are primarily three factors to think about while doing a feasibility study:

1.ECONOMICAL FEASIBILITY
2.TECHNICAL FEASIBILITY
3.SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

To calculate how much money the system will cost the business, that's what this study is for. In light of the company's limited resources, it is essential to set priorities in the areas of research and development most critical to the success of the system. The expenditure of funds requires justification. The built system was able to remain within its budgeted limit since the bulk of the technologies employed are open source. Those customised goods were the only ones that could be purchased.

TECHNICAL FEASIBILITY

This research evaluates system technical feasibility. or whether or not it satisfies the system's technical standards. This means that any new system can't put too much stress on the existing network. This will put pressure on our current technical infrastructure. The consumer will have

a lot on their plate because of the high standards being set. The built system should have minimal needs, since its implementation should have minimal adjustments.

SOCIAL FEASIBILITY

The study's aim is to ascertain the level of satisfaction felt by the system's intended users. As part of this process, users will undergo training. A user should not be afraid of the system, but should instead see it as a necessary evil. User adoption is directly proportional to the effort put into familiarizing and training them to utilise the system. To get useful feedback from the system's end user, his confidence must be boosted.

SYSTEM SPECIFICATIONS:

H/W CONFIGURATION:

- Processor : I3/Intel Processor
- Hard Disk : 160GB
- Keyboard : Standard Windows Keyboard
- Mouse : Two or Three Button Mouse
- Monitor : SVGA

S/W CONFIGURATION:

- Operating System : Windows 7/8/10
- IDE : PyCharm
- Server-side scripts : HTML, CSS, Js
- Libraries Used : Numpy, IO, OS,Sklearn, Flask
- Technology : Python 3.6+

IV. RESULTS AND DISCUSSIONS

Functional test

Methodical evidence is provided by functional tests to show that the system operates as specified by the business and technical requirements, the system documentation, and the user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.
Invalid Input : identified classes of invalid input must be rejected.
Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised.

It is necessary to call on systems or processes that work together.

Functional tests are set up and planned with a focus on requirements, key functions, or unique test cases. As part of a full testing strategy, you should think about business process flows, data fields, predetermined procedures, and processes that come after. The effectiveness of existing

tests and the identification of new tests are done before functional testing is considered complete.

System Test: By testing the system as a whole, we can be confident that the final product will be up to par. It puts a setup to the test to guarantee reliable outcomes. The system integration test that focuses on configuration is a kind of system test. System testing relies heavily on detailed descriptions and flows of business processes, with a focus on pre-driven points of linkage and integration.

White Box Testing

When a software tester understands the program's design and purpose, they are said to have "White Box" expertise. The answer lies in a sense of meaning. It is used for the purpose of evaluating regions that can't be reached by a black box.

Black Box Testing

In software testing, "black boxing" means not knowing anything about the code's internals, architecture, or language. A particular source document, such a specification or requirements document, is needed for developing black box tests, as is the case when writing any other kind of test. A programme is said to be "black box tested" if any and all references to the programme itself are disregarded throughout the testing process. The inside is completely opaque. The test only offers inputs and requests replies; it does not consider the underlying logic of the programme in any way.

Unit Testing:

While coding and unit testing are often combined into a single phase of the SDLC, it is not unheard of for them to be treated as two distinct processes. Procedures and methods for conducting tests. Functional tests will be meticulously designed and field-tested.

Test objectives

The data in every field must be valid.

All pages need to be enabled using the specified URL.

There can be no lag time between the user entering their information and receiving a confirmation or a response.

Testable Features

Make sure the entries are formatted properly.

There shouldn't be any room for multiple submissions.

The user should always be sent to the intended destination when clicking a link.

Integration Testing

Testing the interoperability of many software modules inside a single environment is known as software integration testing.

The purpose of an integration test is to ensure proper communication between different parts of a system or different levels of an organization's software.

All the above-mentioned test scenarios were successfully completed. There were no flaws that were discovered.

Acceptance Testing

Compatibility with Users The end user's input is crucial throughout the testing phase of any project. Additionally, this process guarantees that the system is fully functioning.

All the above-mentioned test scenarios were successfully completed. There were no flaws that were discovered.

Figure 2: Request sended to central authority and attribute authority

Figure 3: Request accepted

Figure 4: Request sent to cloud server

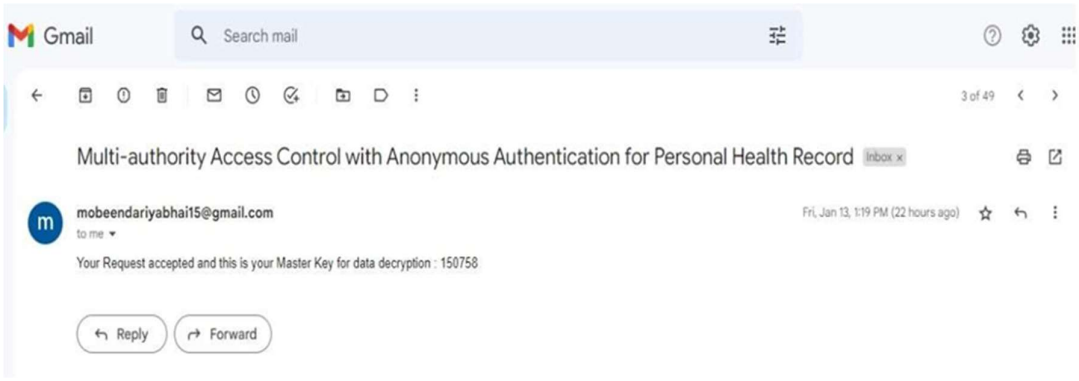

Figure 5: Request accepted and generated master key sended to users mail

Figure 6: File downloaded using master key

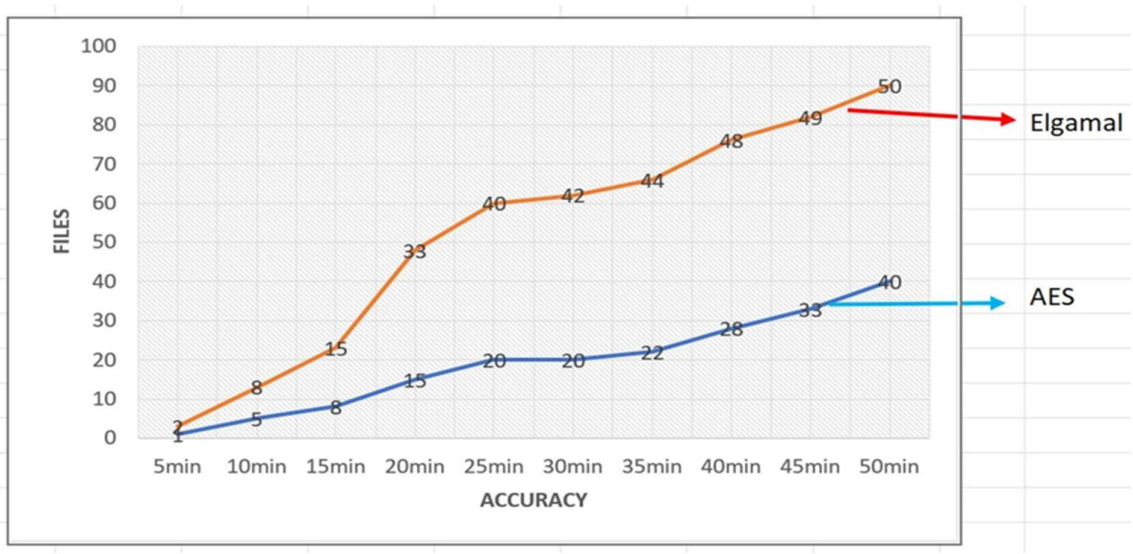

Figure 7: Simulation Results of Data Access Performance

V. CONCLUSIONS

For PHRs, we proposed a framework for secure sharing that relies concerning distributed key management and attribute- based encryption. Here, the user's identity and attributes are hidden from view, with only the central authority having access to them. To stop cloud servers from interfering with ciphertext or fooling end users, an anonymous authentication based on attribute-based signature is suggested.

Only authorised users are able to access and receive messages throughout the entire process of access control. Lightweight computing is accomplished through the use of both online and offline methods, as well as outsourcing activities. The suggested approach not only preserves privacy, which increases patients' control over their PHRs over previous works, but it also retains the encrypted PHRs to resist collusion attempts and not to be forged throughout the duration of sharing.

REFERENCES

[1] Dr. S. Vasundra, CSE, JNTUACEA, Published a paper “A Secure Multi-KeywordSearch Over Encrypted data in Mobile Cloud Computing" IJAEMA- international journal of analytical and experimental modal analysis, ISSN NO: 0886-9367, Vol XI, Isuue VIII,Aug- 2019, (An UGC-CARE Approved Group-A journal) (Scopus indexed).

[2]L. Tbraimi, M. Asim, M. Petkovi, “Secure management of personal health records by applying attribute-based encryption, In Proceeding of the International Workshop on Wearable Micro and Nano Technologies for Personalized Health(pHealth),” in Oslo, Norway, Jun.2009, pp.71– 74.

[3]J. Akinyele, M. Pagano, M. D. Green, “Securing electronic medical records using attribute-based encryption on mobile devices,” in Proceeding of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Oct.2011, pp.75–86.
[4]S. Narayan, M. Gagn´ e, R. Safavi- Naini, “Privacy preserving EHR system using attribute-based infrastructure,” in proceeding of the ACM Cloud Computing Security Workshop, Chicago, Oct.2010, pp.47–52.
[5]J. Lai, R. H. Deng, Y. Li, “Fully secure ciphertext-policy hiding CPABE,” in Proceedings of the International Conference on Information Security Practice and Experience, Jun.2011, pp.24– 39.
[6]J. Sun, Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” in IEEE Trans.Parallel Distrib.Syst., Jun.2009, pp.754–764.
[7]M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” in IEEE Trans.Parallel Distrib.Syst., 2013, pp.131–143.
[8]X. Liang, M. Barua, R. Lu, “HealthShare:Achieving secure and privacypreserving health information sharing through health social networks,” in Comput.Commun., 2012, pp.1910–1920.
[9] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc.13th ACM conference on Computer and Communication Security, 2006, pp.457– 473.
[10] 14. Dr. S. Vasundra, CSE, JNTUACEA, Published a paper “Integrity Checking for StoredData in Mobile Cloud Computing " IJERT-International journal of Engineering Research & Technology, ISSN NO: 2278-0181, Volume. 8 Issues. 8, Aug- 2019
[11] Dr. S.Vasundra et.al, CSE, JNTUACEA, Published a paper “Attribute Based Encryption and Decryption Technique”, International Journal of ComputerApplicationISSN:ISSN:09758887,volume132,No.5December2015.IJCA.