IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303216|

"Strengthening Privacy Measures in Personal Health Records: An Innovative Approach with Multi-Authority Access Control and Anonymous Authentication"

Mrs. S. Venkatalakshmi[1], Ms. C Manasa[2], Mr. Dande Harivardhan[3], Mr. K Sai Ravi Teja[4], Ms. P Sai Ashritha[5]

[1] Assistant professor, Department of CSE, AITS, Tirupati, India

[2, 3, 4, 5] Student, Department of CSE, AITS, Tirupati, India

ABSTRACT: A personal health record (PHR) system is a smart health system that serves patients and doctors. A PHR is usually stored in a cloud and managed by a semi-trusted cloud provider. However, there is still a possibility of the exposure of personal health information to semi-trusted parties and unauthorized users. To protect the privacy of patients and ensure that patients can control their PHRs, a patient centric PHR sharing framework is proposed in this paper. In this framework, all PHRs are protected with multi-authority attribute-based encryption before outsourcing, which solves the key hosting problem and achieves fine-grained access control to PHRs. Furthermore, anonymous authentication between the cloud and the user is proposed to ensure data integrity on the cloud while not exposing the user's identity during authentication. The proposed authentication is issued from a new online-offline attribute-based signature. It can make the encrypted PHRs resist collusion attacks and not be forged during the period of sharing, which enhances patients' control over their PHRs. Online-offline and outsourcing decryption also reduces calculation costs and improves operational efficiency.

KEYWORDS- Anonymous authentication, attribute-based signature, multi-authority attributebased encryption, personal health record.

I.INTRODUCTION

The fine-grained access control system for sharing data based on attribute-based encryption (ABE) is presented and has been a hot issue at the moment in order to safeguard patients' privacy and improve control over their PHR. The private key or ciphertext is generated by ABE using attributes, and only users whose attribute sets match the access policy are allowed to access PHR. But in some earlier designs, user authentication and key generation were handled by a single center, which surely put too much strain on the system.

Such a challenge is solved by multi-authority encryption schemes, which need many authorities to collaborate in order to create private keys for users. This achieved effective and safe access control in a multi-authority setting, but data security is at risk because of the user's hazy authentication. Authentication technology was used to link medical system users to other trusted users, and a searchable public key encryption strategy was added to a PHR system in order to further assure security. Recent studies additionally take into consideration masking the access control policy for access policies that include sensitive user information.

However, using multi-authority attribute- based encryption in a PHR also comes with a few drawbacks, including the outsourcing of anonymous authentication, the unforgeability of the ciphertext, collusion between users and authorities, etc.

II.RELATED WORK

2.1 Attribute based encryption

Sahai and Waters initially recommended attribute-based encryption (ABE) as a solution to the issue of access authorization for data that was outsourced to the cloud. They illustrated how granular access control and encryption policy flexibility may speed up security applications in outsourced data systems. In ABE, a patient creates an encryption access policy for his or her PHR, and the PHR can be successfully accessed when a user's qualities match the access policy. ABE was split into KP-ABE and CP-ABE based on whether the access policy was present in the ciphertext or secret key. This suggested safe and efficient access management in a setting with several privileges. However, fuzzy authentication between users and the cloud is implemented via user access control, endangering the security of user data. To safeguard attribute privacy, it suggested a multi-authority attribute-based encryption method

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303216|

with policy updating. The patient's attributes consist of attribute name and attribute value. In a multicenter setting, made the ciphertext publicly verifiable, enhancing the system's efficiency and security.

2.2 Anonymous Authentication

A cloud sharing scheme can employ the attribute-based signature (ABS) technique to provide an anonymous authentication mechanism. In an attribute-based system, an ABS expands on IBS by representing a signer's identity through a collection of characteristics and offers end-toend safe communication. ABS guarantees the verifier that the supporting message is represented by the attribute set of a signer that fulfills the complex predicate. Unfortunately, there is a significant computational overhead associated with the fact that the complexity of the verified predicate increases the signature time of ABS. A responsible ABS was proposed by Bel Guith et al in 2019 in order to safeguard user privacy. The organization has the option to reveal the identities of anonymous individuals who have authenticated, if needed. However, their techniques' low computational efficiency is also a flaw. Our plan makes use of online-offline technologies to accomplish lightweight authentication, protecting user privacy by concealing the identity and attributes of the user. Moreover, the suggested scheme's computing efficiency is enhanced by outsourcing partial decryption.

III.PROPOSED SYSTEM

The system that is suggested in this publication is a multi-authority attribute-based encryption secure sharing framework for personal health records (PHRs). By giving patients more control over their PHRs and safeguarding their privacy, the system seeks to address these issues. The suggested method has several benefits, such as improved security and privacy, resistance to collusion attacks, prevention of data forgery during sharing, and decreased computing load.

The system uses attribute-based encryption (ABE) to specify access controls for PHR encryption, making sure that the encrypted PHRs are only accessible to users whose attribute sets match the policy. In addition to concealing usernames and characteristics to protect privacy, the suggested solution makes use of online-offline technology to accomplish lightweight authentication.

Several techniques are used in the system's design, such as setup, key generation, and user registration, to provide a foundation for PHRs that is secure and protects privacy. To guarantee the security and operation of the suggested system, it also tackles the computational Diffie-Hellman problem, pseudo-random function, and linear secret-sharing method.

In addition, a performance analysis of the suggested system contrasts its computational overhead with that of current methods, proving how successful it is in cutting computation costs and improving operational efficiency. The system's functioning and security are also assessed, emphasizing its defences against collusion attempts, stopping data forgeries, and protecting user privacy. To sum up, the suggested system seeks to address the issues of data security, privacy leakage, and computational load in PHR systems by offering a safe, private PHR system with finegrained access control.

3.1 Preliminaries

The preliminaries section of the paper provides essential background information and foundational concepts necessary for understanding the proposed scheme.

1. System Model

The suggested scheme's elements and parameters are specified by the system model. It presents the idea of bilinear groups, which are cyclic groups of prime order p and are represented by the notations G_0 and G_T. Additionally defined are the bilinear map e: $G_0 \times G_0 \rightarrow GT$ and the generator g of G_0. With t_a, t_b, t_1, and t_2 being elements of G_0, the bilinear map e possesses the feature of bilinearity, which is represented as $e(t_a, t_b) = e(t_1, t_2)ab$.

2. Bilinear Groups

As cyclic groups of prime order p, the bilinear groups G_0 and G_T are defined, and for G_0, the generator g is given. We introduce the bilinear map e, which possesses the bilinearity feature.

3. Computational Diffie-Hellman Problem (CDH)

The difficulty of creating gab from g_a and g_b, where a and b are two secrets, is known as the CDH issue. The importance of the CDH problem to the security analysis is shown as the study addresses it within the framework of the suggested scheme.

Pseudo-Random Function (PRF)

The idea of a pseudo-random function (PRF), or a function that may perform an operation to produce secure pseudo-random numbers, is presented. The PRF is a safe pseudo-random number generator whose distributions, when subjected to all polynomial constrained black box assaults, are indistinguishable from uniform distributions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303216|

Overview

1. Central authority (CA)

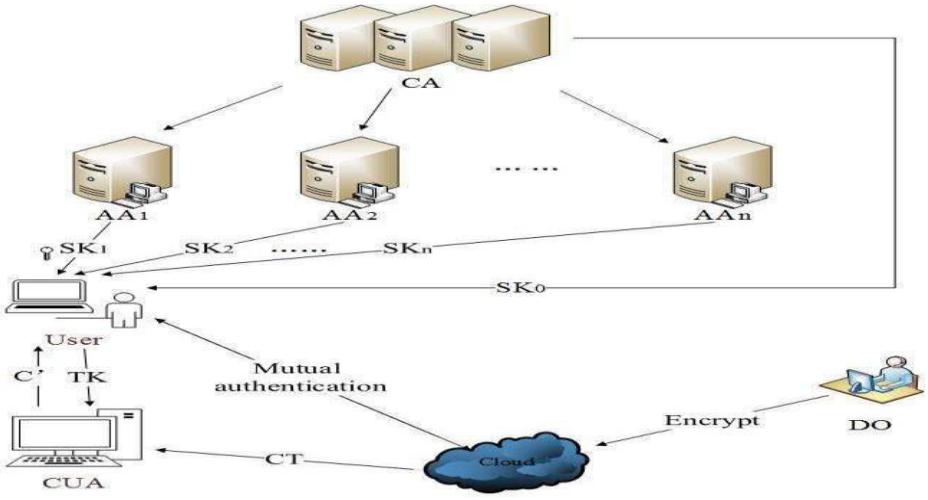
In order to maintain the integrity and dependability of the multi-authority access control with anonymous authentication for personal health records, CA is in charge of overseeing the entire system infrastructure, which includes user authentication, key distribution, and policy enforcement.

2. Attribute authority (AA)

In order to apply access control policies based on user characteristics or roles, attribute authorities are in charge of maintaining and issuing user attributes.

3. User (U)

Through the authentication procedure, users maintain their anonymity while securely accessing their personal health records through interaction with the system.



4. Data owner (DO)

Retaining control over the data and having the ability to create access controls for permitted parties are the rights of the data owner, usually the person or organization whose personal health records are being accessed.

5. Cloud Server (CS)

Personal health records are safely stored and managed by a cloud server that protects user privacy and confidentiality while guaranteeing data integrity and accessibility for authorized users.

6. Cloud user assistant (CUA)

Ensuring security and privacy while facilitating user interactions with the cloud server, the cloud user assistant helps users access, manage, and retrieve personal health records.

IV.RESULTS AND DISCUSSIONS

4.1 Performance analysis

The multi-authority attribute-based encryption (MA-ABE) method for personal health records (PHRs) is the subject of a performance analysis that compares the computing costs associated with decryption, verification, and signing. The proposed scheme's computational overhead and storage costs are compared to those of existing schemes in detail as part of the research. The amount of characteristics and computational cost in signing (ms)indicate that the suggested scheme has less calculation overhead than other schemes. A comparison is also made between the user-side calculation costs of verification and decryption; in both scenarios, the suggested technique demonstrates reduced costs. Finally, the performance study of the suggested MA-ABE scheme for PHRs demonstrates the system's efficiency with respect to the computational expenses associated with signing, verifying, and decryption.

4.2 Security analysis

The security analysis of the proposed multi-authority attribute-based encryption (MAABE) scheme for personal health records (PHRs) addresses several key aspects, such as safeguarding user privacy, preventing replay attacks, utilizing a selective access structure model, and preventing collusion. The proposed MA-ABE approach for PHRs' security analysis concludes by demonstrating how well it protects user privacy during authentication and how

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303216|

resistant it is to replay attacks, unauthorized access, and collusion. By contrasting the security features of the scheme with those of previous works, it is possible to see how reliable and effective it is at granting secure, private access control for individual health records.

4.3 Algorithm definition

In this context, the term "algorithm definition" refers to the particular processes and actions that make up the suggested multi-authority attribute-based encryption (MA-ABE) scheme for personal health records (PHRs) that features anonymous authentication. The setup, key generation, user registration, and encryption procedures are all included in the algorithm definition and are all essential to the safe sharing architecture.

1. **Setup Algorithm:** It entails the creation of public-secret key pairs, hash functions, and group element selection.
2. **Key Generation Algorithm:** The algorithm makes sure users get the keys and login information they need to access and unlock the PHRs that are encrypted.
3. **User Registration Algorithm:** It entails the creation of anonymous identification credentials, pseudonyms, and signatures, which are subsequently sent to the users by the central authority.
4. **Encryption Algorithm:** Public keys, messages, and access controls are used in the encryption method to encrypt the PHRs. It guarantees that the information is safely encrypted and that only authorized users who meet the requirements of the access policy will be able to access it.

V. CONCLUSION

For PHRs systems, we suggested a safe sharing framework based on multiauthority attribute-based encryption. Only the reliable central authority is aware of the user's identity and characteristics under this method. An anonymous authentication method based on attribute-based signature is suggested to stop cloud servers from altering ciphertext or tricking end users. Only authorized users are able to access and obtain communications during the entire access-control process. In contrast to previous efforts, the suggested strategy maintains patients' authority over their PHRs by protecting them from collusion attacks and forgeries during the sharing phase while also achieving privacy preservation. The following two components of this approach can be expanded upon to fulfill the higher security and efficiency requirements of real-world application scenarios.

Anonymous authentication between the authority and the user: It is worthwhile to look into the authenticity between the user and the authority because it was previously believed that they were dishonest.
Traceability: Taking the scheme's practicality into account, the system uses traceable technology to determine the identity of the current user in the event that an unauthorized user is unable to verify.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,” in IEEE Trans.Parallel Distrib.Syst., 2013, pp.131–143.
[2] K. Yang, Q. Han, and H. Li, “An efficient and fine-grained big data access control scheme with privacy-preserving policy,” in IEEE Internet Things., 2017, pp.563–571.
[3] M. Yang, T. Zhang, “Efficient privacy-preserving access control scheme in electronic health records system,” in Sensors., 2018, pp.3520–3525.
[4] Y. Liu, Y. Zhang, and J. Ling, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing,” in Future Gener. Comp.Sy., 2018, pp.1020–1026.
[5] 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. [6] J. Wei, W. Liu and X. Hu, “Secure and efficient attribute-based access control for multiauthority cloud storage,” in IEEE SYSTEM JOURNAL, June.2018, pp.1731–1742.
[7] Y. S. Rao, “A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing,” in FutureGener.Comput.Syst., vol.67, 2017, pp.133–151.
[8] X. Yan, H. Ni, Y. Liu and D. Han, “Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR,” in Computer Science and Information Systems., 2019, pp.831-847.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details