IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005296 |

Multi-Authority Access Control for Personal Health Records with Anonymous Authentication

Vakka Srivalli, Shaik Mohammad Kashif, Shaik Sharmila, Vuyyala Syam Gopal,

Pinnamaneni Siva Prasad

UG Student, Dept. of Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

Assistant Professor, Dept. of Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

ABSTRACT: Patients and doctors benefit from a PHR system, which is a smart health system. It's possible that semi-trusted parties and unauthorised individuals could still access personal health information. This application proposes a patient-centric PHR sharing framework to preserve patients' privacy and provide them control over their PHRs. Multi-authority attribute-based encryption is used to encrypt all PHRs before outsourcing, which eliminates the key hosting issue and provides fine-grained access control to PHRs in this framework It is also suggested that the cloud and the user employ anonymous authentication to secure the integrity of cloud data without disclosing the identity of either party. It has the ability to make encrypted PHRs resistant to collusion assaults and forged over the period of sharing, which strengthens patients' control over their PHRs and their ability to access their records. This application proposes a patient-centric PHR sharing architecture with the primary objective of protecting patients' privacy and ensuring patients have control over their PHRs. As a result of this design, the key hosting issue is eliminated, and PHRs can have fine-grained access control thanks to multi-authority attribute-based encryption.

I. INTRODUCTION

PHR, a developing technology, has played an important role in data exchange in recent years. PHR allows patients and clinicians to maintain medical records online and access them at any time and from any location. However, when PHR is used to share data, it might cause issues like privacy leaking. It has become a popular subject in recent years to preserve the privacy of patients and strengthen their control over their Personal Health Records (PHRs) through the use of a fine-grained access control method based on attribute-based encryption (ABE).

Users can only access PHR if their attribute sets satisfy an ABE-defined access policy connected with the generation of the private key or cypher text. Certain prior methods relied on a single location to produce keys and verify the identity of the people using them. An encryption technique that requires multiple authorities to jointly produce private keys for users is a solution. In a multi-authority context, we achieved secure and efficient access control, but the user's fuzzy authentication poses a risk to data security. A searchable public key encryption strategy was proposed for a PHR system, and authentication technology was used to link users of the medical system with other trusted users in order to further enhance security. There are also a number of practical ways to deal with the issue of patient privacy and scheme confidentiality. A user's identity and other personal information are kept private when interacting with the system using these techniques. In recent research, masking access control policies including sensitive user information is also considered. All of them, however, are dependent on sacrificing productivity. The final ciphertext can be instantly obtained using online and offline technology, reducing calculation time and enhancing user comfort. Multi-authority attribute-based encryption in a Personal Health Record (PHR) also has many drawbacks, including anonymous authentication outsourcing and ciphertext unforgeability, as well as collusion between users and authorities.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005296 |

II. RELATED WORK

[1] 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.

Personal health records (PHR) are a new type of patient-centered health-records approach that can help patients share their health information online. The PHR system was built using Attribute-Based Encryption (ABE), a revolutionary public key cryptosystem that ensures fine-grained management over outsourced encrypted data. A privacy-preserving multi-authority attribute-based encryption system with dynamic policy updating in PHR has been presented to address the main issues of PHR. Attribute name and value make up the first half of the model for each patient. To prevent unauthorised access, the user's attribute values will be obscured. It is also possible to update policies based on "and," "or," and "not" operations using the Linear Secret Sharing Scheme (LSSS) access structure and policy-updating algorithms. Finally, the standard model shows that the method is safe from a chosen-plaintext attack. User's secret key and ciphertext are lowered in size, and the lower computing cost makes it more effective in a PHR system.

[2] D. Li, J. Liu, Q. Wu and Z. Guan, "Efficient CCA2 secure flexible and publicly-verifiable fine-grained access control in fog computing," in IEEE Access., 2019, pp.11688-11697.

The Internet of Things (IoTs) designs provide low latency for real-time devices and applications with the help of edge computing, which decreases the heavy burden of the cloud centre server by employing the network edge servers. Data access control for the Internet of Things (IoT) still faces security concerns. Access control for encrypted data in cross-domain applications is made possible through the use of multiauthority attribute-based encryption (MA-ABE). We present an efficient fine-grained revocable large-universe multiauthority access control mechanism based on the IoT's characteristics and technical constraints. Additionally, it has been proposed to add a reusable ciphertext pool in order to speed up the user's configuration step and to split the encryption method into online and offline encryption. In order to reduce the computational burden of decryption, large decryption activities are outsourced to the near-edge servers. Access privileges can be dynamically altered by an effective revocation mechanism. Furthermore, ciphertext verification is supported by the system. To conserve system resources, only valid ciphertext can be stored and communicated. The suggested technique is CCA2-secure under the q-DPBDHE2 assumption thanks to the chameleon hash function. This approach's efficiency and suitability for IoT edge computing have been determined through performance analysis.

[3] X. Zhou, J. Liu, Q. Wu, "Privacy preservation for outsourced medical data with flexible access control," in IEEE Access., Jun.2018, pp.14827– 14841.

Healthcare networks rely heavily on electronic medical records (EMRs). The EMR system must be able to protect the privacy of patients' medical records because they are always full of sensitive information. Currently, most systems only allow a user to access an EMR if and only if his or her role matches the access policy that has been specified. Patients' identities can be linked to their doctors through these existing schemes, though. Without access to patients' electronic medical records, classifications of patients' ailments can be disclosed. We propose two anonymous approaches to solve this issue. They are able to maintain data secrecy while simultaneously providing individuals with a sense of anonymity. Using the first method, attackers select their targets prior to getting information from the EMR. When an adversary interacts with the EMR system, he or she can adaptively select an attack target. Our schemes are shown to be secure and anonymous through thorough testing. Additional to this, we suggest a method for EMR owners to search for their EMRs in an anonymous environment. We adopt an online/offline method to speed up data processing in order to provide a better experience for our customers. Key generation and EMR encapsulation can be completed in milliseconds, according to the findings of recent experiments, demonstrating this claim.

III. PROPOSED ALGORITHM

As a result of this design, the key hosting issue is eliminated, and PHRs can have fine-grained access control thanks to multi-authority attribute-based encryption. It is also suggested that the cloud and the user employ anonymous authentication to secure the integrity of cloud data without disclosing the identity of either party. In the proposed authentication, a new attribute-based signature is used. It has the ability to make encrypted PHRs resistant to collusion assaults and forged over the period of sharing, which strengthens patients' control over their PHRs and their ability to access their records. Offline and online decryption also decreases calculating expenses and enhances operational efficiency

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005296 |

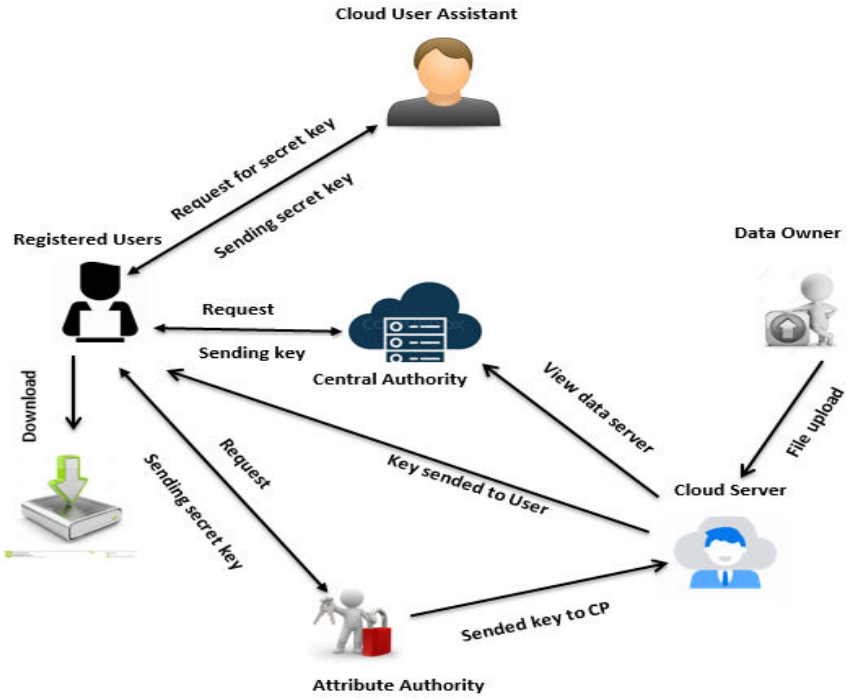

Figure 1: Architecture

. **1. Central authority (CA):**
CA is a trust entity that generates the system public parameters and master secret key. It also generates partial secret keys and anonymous identity credentials for users, along with the public signing key and corresponding private key. Then CA sends anonymous identity credentials and partial secret keys to users, and the signing private key to the data owner.

2.Attribute authority (AA):
Each AA is responsible for managing attributes that are disjoint from other AAs, and publishing attributes to data owner to generate access policies to encrypted data. AAs produce local public parameters and secret keys. They are responsible for users to generate attribute secret keys.

3.User (U):
U obtains the AIC and partial secret key from the CA and sends it to the AA. After authentication, the AA generates the attribute private key for U. If the U's identity and the ciphertext are not tampered with, then U sends the signing secret key and transformation key to cloud user assistant and decrypts the ciphertext by getting retrieving keys.

4.Data owner (DO):
The DO owns the data and shares them by outsourcing them to the cloud server. The DO first defines the expected access policy on the attributes and then encrypts the data by calling the proposed scheme. Then the ciphertext is signed by using ABS and uploaded to the cloud.

5. Cloud Server (CS):
The CS stores ciphertext signed by the DO. We assume that it is not trusted, i.e, CS may replace or tamper with ciphertext generated by the DO with fake conversions, and it may deceive U by returning a terminator.

6. **Cloud user assistant (CUA):**
CUA running on the cloud checks the unforgeability of ciphertext and realizes its partial decryption for the user. Most computation is transferred to the CUA, which reduces the computation cost on the user side.

IV. PSEUDO CODE

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data?the data to be encrypted. This array we call the state array.

You take the following aes steps of encryption for a 128-bit block:

Derive the set of round keys from the cipher key.

Initialize the state array with the block data (plaintext).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005296 |

Add the initial round key to the starting state array.
Perform nine rounds of state manipulation.
Perform the tenth and final round of state manipulation.
Copy the final state array out as the encrypted data (ciphertext).
The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.
The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data.

V. RESULTS

HOME PAGE:

Figure 2: Output Screenshot 1

DECRYPTED DATA:

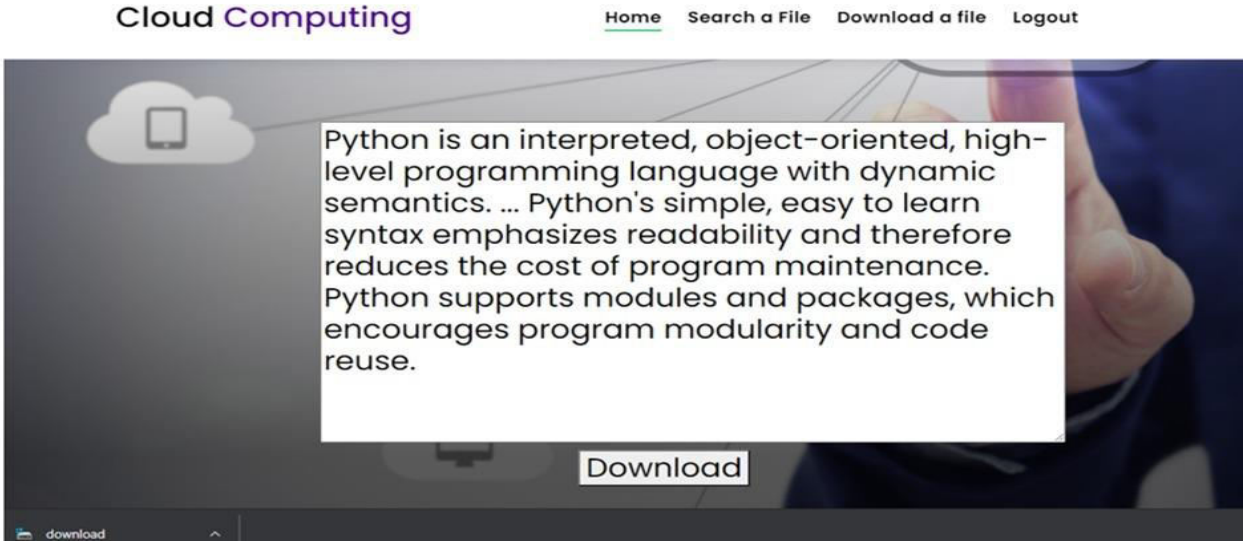

Figure 3: Output Screenshot 2

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005296 |

V. CONCLUSION AND FUTURE WORK

.

A multiauthority attribute-based encryption architecture for PHRs-based safe sharing was proposed by us. The user's identity and attributes are only known to a trusted central authority in this model. An anonymous authentication based on attribute-based signature is proposed to prevent cloud servers from interfering with ciphertext or fooling end users. Messages can only be accessed and obtained by authorised users in the entire access-control process. Online and offline techniques, as well as outsourcing processes, are employed to achieve light computation. With the proposed approach, people have more control over their personal health records because they are protected from collusion assaults and cannot be forged while they are being shared. From the following two features, this solution can be expanded to fulfil better security and efficiency requirements in practical application scenarios.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," in IEEE Trans.ParallelDistrib.Syst., 2013, pp.131–143.
7. 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. [8] R. Lu, X. Lin, X. Shen, "SPOC: A secure and privacy-preserving oppotunistic computing framework for mobile-healthcare emergency," in IEEE Trans.ParallelDistrib.Syst., 2013, pp.614–624.
8. X. Zhou, J. Liu, Q. Wu, "Privacy preservation for outsourced medical data with flexible access control," in IEEE Access., Jun.2018, pp.14827– 14841.
9. S. Jiang, X. Zhu, and L. Wang, "EPPS:Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks," in Sensors., 2015, pp.22419–22438. [11] K. Yang, Q. Han, and H. Li, "An efficient and fine-grained big data access control scheme with privacy-peserving policy," in IEEE Internet Things., 2017, pp.563–571.
10. M. Yang, T. Zhang, "Efficient privacy-preserving access control scheme in electronic health records system," in Sensors., 2018, pp.3520–3525.
11. 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.
12.A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption," in Proc.EUROCRYPT,vol.LNCS 3494, May.2005, pp.457–473.
13.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

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details