OPEN ACCESS

Volume: 11

Special Issue: 1

Month: July

Year: 2023

E-ISSN: 2582-0397

P-ISSN: 2321-788X

Impact Factor: 3.025

Received: 08.05.2023

Accepted:13.06.2023

Published: 01.07.2023

Citation:
Sreedhar, and GB Vinay. “Controlling Access with Multi-Authority and Identification for Individual Personal Medical Records.” *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. S1, 2023, pp. 213–17.

DOI:
https://doi.org/10.34293/sijash.v11iS1-July.6341

Controlling Access with Multi-Authority and Identification for Individual Personal Medical Records

Prof. Sreedhar
Department of Master of Computer Applications
Raja Rajeswari College of Engineering

Vinay GB
Department of Master of Computer Applications
Raja Rajeswari College of Engineering

Abstract

A useful health tool that helps both patients and doctors is the personal healthcare record (PHR) system. A semi-trusted provider of cloud services frequently manages and stores a PHR. Confidential health information could still be viewed by unauthorized people and unscrupulous parties, though this possibility is still present. By providing a client-centric PHR sharing framework, this technique safeguards patient privacy and guarantees that patients retain control over their PHRs. Prior The PHRs in this architecture have been multi-authority protected against outsourcing. attribute-based encryption, which solves the issue of key hosting and provides PHRs with fine-grained access control.

Introduction

PHR has played an important part in data exchange in recent years as an emerging technology. PHR may keep medical records online so that patients and doctors can access them from anywhere at any time any location. However, after data allocation is done, PHR introduces other issues, such as privacy leaking. To preserve patients’ privacy and improve control over their PHR, a fine-grained access switch approach based on attribute-based encryption (ABE) is proposed and is now a hot issue. ABE specifies an access policy using characteristics linked with producing the private key or ciphertext, and only users with matching attribute sets may access PHR.

Some prior approaches, on the other hand, relied on a single centre to create keys and verify users, which surely overwhelmed the system. A multi-authority encryption technique, which requires many authorities.

Literature Survey

Sana Belguith has suggested In this research, we offer the InsPAbAC framework, which combines attribute-based encryption and attribute-based signature approaches for securely sharing outsourced data contents over public cloud servers. There are various advantages to the suggested architecture. First, it provides an encrypted access control feature that is enforced at the data owner's end, while also allowing access control policies to be as expressive as required. Second, Ins-PAbAC protects users' privacy by employing an anonymous authentication technique developed from a privacy-preserving attribute-based signature system that conceals users' identifying information.

Daweili presented Fog Computing, which offers compute, storage, applications, and network services between Internet of Things (IoT) and cloud servers by extending the Cloud Computing paradigm to the network's edge. Because of the large number of nodes, enhanced security with low latency, widespread geographical distribution support, and high flexibility should be prioritised while safeguarding information security in Fog Computing. To accomplish flexible fine-grained admittance regulator in Fog Figuring, we suggest a new cryptographic primitive called CCA2 Secure Publicly-Verifiable Revocable Large-Universe Multi-Authority Attribute-Based Encryption (CCA2- PV-R-LU-MA-ABE).

End nodes in fogs create private keys from numerous authorities in this primitive, which may be distinguished by their geographical locations or functions, and their characteristics can be represented by any strings in the huge universe, which satisfies a variety of purposes in actual Fog applications. Furthermore, node access may be cancelled efficiently even by devices with minimal resources. This primitive provides public verification to assure ciphertext correctness, and only valid ciphertext can be saved or communicated. We build a tangible CCA2-PV-RLU-MA-ABE strategy based on the primitive and fog computing feature. We define the primitive's security model, which is far more secure than the CPA-secure approach.

Finally, we evaluate the productivity of the suggested practical method to that of the current CPA-secure method using both theoretical and experimental analysis, and the findings demonstrate that the extra consumption of efficiency to improve CPA to CCA2 is quite little. The suggested approach is sufficiently safe, versatile, and efficient to be used in practical fog computing.

Yang Ming has talked about The collaboration of electronic health information, or EHR, in cloud servers is a growing trend that has the potential toward recover the competence of medical systems. However, there are various concerns about the security and privacy of EHR systems. The EHR data covers subtle personal information about the EHR owner; if these data are gained by a hostile user, it would not only result in the leaking of the patient's privacy, but it will also influence the doctor's diagnosis. It is a difficult dilemma for the EHR owner toward have whole regulator finished his or her own EHR data while also protecting his or her own privacy.

According to Xiaoyanzhu, mobile healthcare social networks have emerged as a viable next-generation healthcare system that will significantly advance people's quality of life. But, there are some safety and privacy considerations that must be addressed before distribution subtle health material with third parties. We present a fine-grained and scalable data access control approach based on attribute-based encryption to ensure patients have whole controller completed their PHI. Furthermore, PHI sharing policies themselves may be sensitive, revealing information about underlying PHI or data owners or receivers. Fashionable our system, each attribute has a name and a value, and we usage the Blossom strainer to effectively examine attributes before decryption. Thus, in our suggested method, data privacy and policy privacy may be guaranteed.

Furthermore, given that computational charge escalates through the intricacy of the admission policy, by way of the limitations of a smart phone's resources and energy, we outsource ABE decryption towards the fog while preventing the cloud from knowing anything about the content and access policy. The security besides recital studies display that our planned method can establish fine-grained access controls for PHI sharing in MHSNs.

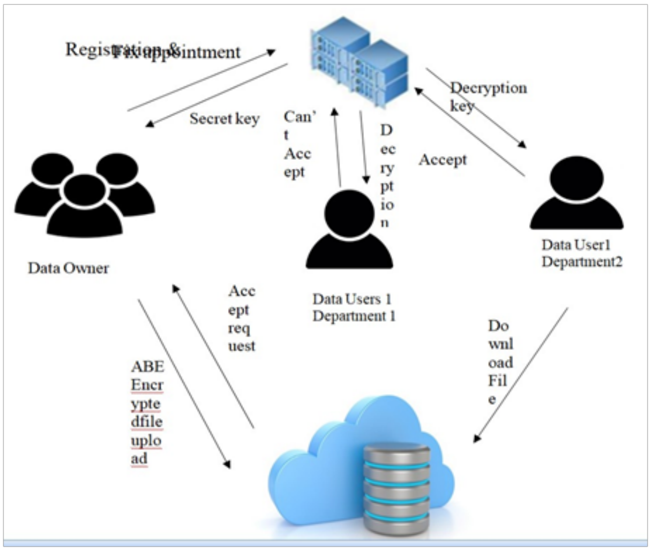

Figure 1 PHI Sharing in MHSNs

Proposed Methodology

A can facilitate statistics stowage and exchange. However, sensitive consumers' data stored on mist strategies could be taken by unauthorised users, resulting in major privacy problems. It is dangerous to create a safe, private PHR a system with precise access control. For instance, before encoding a PHR and uploading its encrypted text to the cloud, a data owners may define an access policy. To protect security and privacy, it is possible to encrypt patient personal data before uploading it to the cloud. It is crucial to note that patients ought to be able to decided by who is privy to their PHRs.

A private medical file is a collection of data about a patient's health that allows for the efficient, consistent, and universal sharing of health information. Because of the sensitivity of health-related information, the key difficulty in today's PHR systems is providing safe storage and access to PHR. Personal information protection and electronic documents act for health data are aimed at ensuring enough care is taken to managing such data.

The following are the primary contributions of this paper:

- To assist with verification and partial decryption, we use the offlineonline strategy and outsource decryption processes. to achieve lightweight computation.
- It will provide a solution to issues such as employing multi-authority attribute-based security in a PHR, including user and authority collusion, anonymous authentication outsourcing, and cypher text enforceability.
- When compared to the previous system, the experimental outcome is excellent.
- It will be more secure than the current system.

Implementations

Data Owner and Data User Login

- The information landlord in care of the total patient records.
- If the login information and Passcode entered data owner are accurate, they will be transferred onto a different form.
- All patient information will be manageddata owner.

- The data user will then look for a record to download. The data user will download the records after receiving authorization from the server.

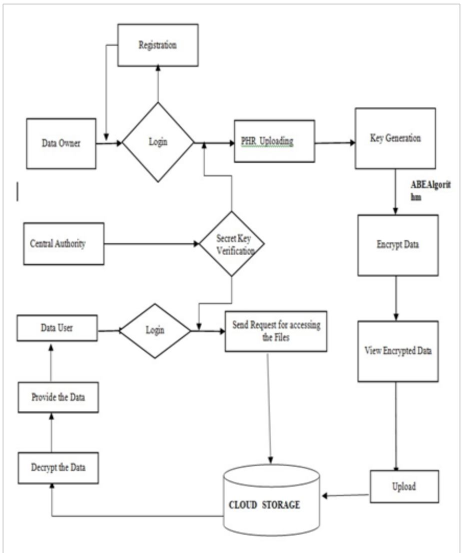

Figure 2 PHR Data Implementation

PHR Data Uploading

- PHR data uploading entails the owner submitting their health information.
- After uploading, the data is saved in text format, and the details are saved in the database.
- The file will at that time uploaded to t ABE encryption.
- The key-based encryption procedure. Central authority will produce that key.

Conclusions

In this Procedure, we suggested a safe sharing architecture for PHRs systems based on multiauthority attribute-based encryption. In this structure, the user's identity and characteristics are concealed and only known by the dependable central authority. To prevent cloud servers from tampering with ciphertext or deceiving end users, an anonymous verification based on attribute-based signature is recommended. During the access-control method, only approved users are permitted to access and obtain messages.Additionally, the data owners will save their personal health record (PHR) data on the cloud securely.the information utilised to encode ABE Algorithm and the data user who wishes to receive this file must be confirmed by the central authority and CSP before they may decrypt the file. • As a future project, it would be fascinating to improve or develop the algorithms used to encrypt data and store it more securely on the cloud.

- In the future, we'd like to mix multiple algorithms and evaluate the process one after the other, such as comparing the accuracy and safety of such methods.
- The suggested model will be extended in the future to incorporate additional and wellorganized processes to implement online, by way of a real-time procedure.

References

1. L. Tbraimi, M. Asim, M. Petkovi, "Secure management of personal By using attributebased encryption, health records may be protected. This is described in the proceedings of the worldwide workshops on practical micro and nanoscale technologies for personalised health (pHealth), which was held in Oslo, Norway, in June 2009.

2. J. Akindele, M. Pagwano, M. D. Green, a man “Securing digital medical records utilising encryption based on attributes on mobile devices,” Session of the Ieee Conference on Privacy and Security in Mobile and Portable Devices, October 2011, pp. 75–86..
3. S. Navrayan, M. Gafgne´, R. Saravanan, “Privacy preserving electronic health record (EHR) systems using attribute-based infrastructure,” in proceedings of the ACM Internet of Things Security Workshop, Chicago, October 2010, pages 47–52.
4. J. Lafi, R. H. Deeng, Y. Lif, “Fully secure ciphertext-policy hiding CPABE,” Papers of the International Seminar on Information Security Practise and Experience, June 2011, pp. 24–39 .
5. J. Sun, Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” in IEEE Trans.ParallelDistrib.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.Parallel Distrib.Syst., 2013, pp.614–624.
9. X. Zhou, J. Liu, Q. Wu, “Privacy preservation for outsourced medical data with flexible access control,” in IEEE Access., Jun.2018, pp.14827– 14841.
10. 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.