Enabling Authorized Encrypted Search for Multi-Authority Medical Databases

SYED FAROOQ T[#1], RAHUL R[#2], SOWMYA S[#3]

[#1], Student, Department of Information Technology, Prince Shri Venketeshwara Padmavathy Engineering College, Ponmar, Chennai

[#2], Student, Department of Information Technology, Prince Shri Venketeshwara Padmavathy Engineering College, Ponmar, Chennai

[#3], Assistant Professor, Department of Information Technology, Prince Shri Venketeshwara Padmavathy Engineering College, Ponmar, Chennai

***ABSTRACT*: E-medical records are sensitive and should be stored in a medical database with encrypted form. However, simply encrypting these records will eliminate data utility and interoperability of the existing medical database system because encrypted records are no longer searchable. Moreover, multiple authorities could be involved in controlling and sharing the private medical records of clients. However, authorizing different clients to search and access records originating from multiple authorities in a secure and scalable manner is a nontrivial matter. To address the above issues, we propose an authorized searchable encryption scheme under a multi-authority setting. Our proposed scheme leverages the MD5 function to enable each authority to limit the search capability of different clients based on clients' privileges. To improve scalability, we utilize multi-authority attribute-based encryption to allow the authorization process to be performed only once even over policies from multiple authorities. We conduct rigorous security and cost analysis, and perform experimental evaluations to demonstrate that the proposed scheme introduces moderate overhead to existing searchable encryption schemes.**

INTRODUCTION

PHP is a server-side scripting language designed for development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP implementation is now produced by The PHP Group. PHP originally stood for Personal Home Page, but it now stands for the recursive acronym PHP: Hypertext Preprocessor. PHP code may be embedded into HTML code, or it can be used in combination with various web template systems, web content management systems, and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.

The standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

The PHP language evolved without a written formal specification or standard until 2014, leaving the canonical PHP interpreter as a fact standard. Since 2014 work has gone on to create a formal PHP specification.

During the 2010s there have been increased efforts towards standardization and code sharing in PHP applications by projects such as PHP-FIG in the form of PSR-initiatives as well as Composer dependency manager and the Packages repository. PHP hosts a diverse array of web frameworks requiring framework-specific knowledge, with Laravel recently emerging as a popular option by incorporating ideas made popular from other competing non-PHP web frameworks, like Ruby on Rails.

RELATED WORKS

[1] Electronic Medical Records Adoption and Use: The aim of this research is to explore the motives behind the adoption or rejection of Electronic Health Records (EHR) systems in the USA by medical offices. The current health care system in the United States suffers from high expenditures and poor quality. The Patient Protection and Affordable Care Act, passed in 2010, attempts to save costs and improve quality of care by offering incentives to use Electronic Health Records systems.

[2] Research of Access Control in Electronic Medical Record Based on UCON: it analyzes the existing drawbacks in traditional access control models firstly and outline the characteristics of next generation access control UCON. Then we apply the idea of UCON to electronic medical record system to meet the challenge of confidentiality, privacy preservation and data integrity.

[3] Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption: Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. they leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file.

[4] An Efficient Cloud-based Personal Health Records System Using Attribute-Based Encryption and Anonymous Multi-Receiver Identity-Based Encryption: As an emerging patient-centric model of health information exchange, cloud-based personal health record (PHR) system holds great promise for empowering patients and ensuring more effective delivery of health care. PHR owners encrypt their PHR data for the public domain using cipher text policy attribute-based encryption scheme, while they encrypt their PHR data for the personal domain using anonymous multi-receiver identity-based encryption scheme. Only authorized users whose credentials satisfy the specified cipher text policy or whose identities belong to dedicated identities can decrypt the encrypted PHR data.

[5] Designing Privacy Information Protection of Electronic Medical Records: interoperability, exchange, privacy, and security of electronic medical records (EMR) across healthcare institution has become an important international issue within medical informatics. Currently Taiwan's electronic medical records exchange center (EEC) system lacks a mechanism for patients to consent to releasing only portions of their EMR. Currently patients must consent to total access when transferring EMR across healthcare institution. This study uses the IHE BPPC profile and HL7 Confidentiality code to develop privacy polices matrices and patient privacy protect mechanism.

PROBLEM DEFINATION

➢ **Creating patient account and assigning patient unique key.**

- Input user name and detail of the patient
- Generate a random key unique to the user.

➢ **Assigning file keys.**

- management upload files onto the system.
  - ➢ Generate random key unique to the file.
  - ➢ Display list of all file with attributes such as:
    - Record number.
    - Date.
    - Medical details.

➢ Share the unique file key in a encrypted form to the patient requesting the file.

SYSTEM ARCHITECTURE

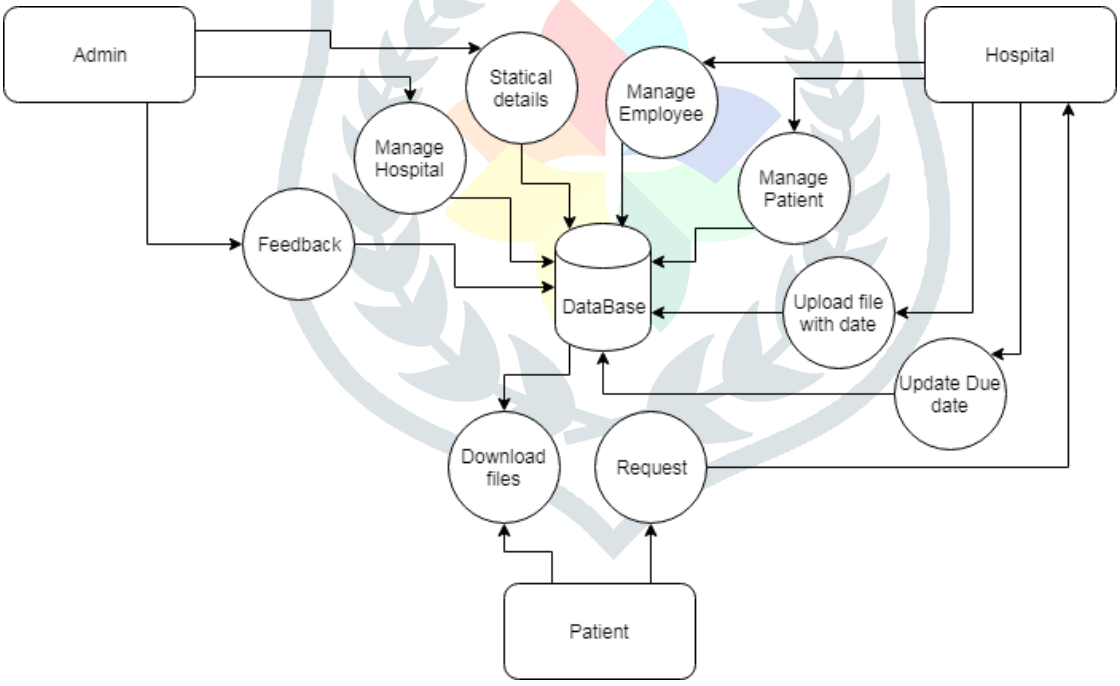

Fig. SYSTEM ARCHTECTURE

PROBLEM DESCRIPTION

METHODOLOGY: To develop the smart attendance management system, some steps are required to be followed. The steps can be defined in the following ways:

•USER INTERFACE DESIGN • REPORT MANAGEMENT UPLOADING

• FILE REQUESTING

USER INTERFACE DESIGN

To connect with server hospital management must give their username and password. If the user already exits, he/she can directly login into the server else user must register their details such as username, password and Email id, into the server. Server will create accounts for every hospital management. Name will be set as user id. Logging in is usually used to enter a specific page.

REPORT MANAGEMENT UPLOADING

Hospital management uploading the medical record or file of the patient into the virtual machines. These constraints serve a dual purpose as they can introduce high-level policies and assist in administration tasks. The user uploads the file/data to the cloud. Given that we rely on network services for our most security-critical data. A source wants to securely send a message to a set of receivers over a cloud network with unit-capacity edges, in the presence of a cloud user.

FILE REQUESTING

The file is only in the viewable format so the file is shared and downloaded purpose. File Request is sent to the patient, the patient checks the request and id user is authorized & accordingly the key is provided to the patient.

RESULTS

We can easily store the patient medical data securely using the patient medical record This will give less time over paperwork's for both the doctors as well as the patient use. This Platform ensures that the patient trust their medical data accesses securely.

CONCLUSION

It will request that clients grow new capacities to utilize CPR frameworks and to change their documentation practices.

FUTURE WORK

- To optimize the work to implement in Artificial Intelligence environment.
- To automate this process by showing the result in desktop application.

REFERENCE PAPER

[1] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attributebased signcryption," Future Generation Comput. Syst., vol. 52, pp. 67–76, 2015.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[3] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. of 25th USENIX Secur. Symp., 2016, pp. 707– 720.

[4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in Proc. of 36th Annu. Symp. on Foundations of Comput. Sci., 1995, pp. 41–50.

[5] X. Yuan, X. Wang, C. Wang, C. Qian, and J. Lin, "Building an encrypted, distributed, and searchable key-value store," in Proc. of the 11th ACM on Asia Conf. on Comput. and Commun. Security, 2016, pp. 547–558.

[6] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, "Result pattern hiding searchable encryption for conjunctive queries," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 745–762.

[7] S.-F. Sun, X. Yuan, J. K. Liu, R. Steinfeld, A. Sakzad, V. Vo, and S. Nepal, "Practical backward-secure searchable encryption from symmetric puncturable encryption," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 763–780.

[8] L. Xu, X. Yuan, C. Wang, Q. Wang, and C. Xu, "Hardening database padding for searchable encryption," in Proc. of the 2019 Conf. on Int. Conf. on Comput. Commun. IEEE, 2018.

[9] S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloudbased secure keyword search," in Proc. of 22nd Aus. Conf. on Inf. Secur. and Privacy, 2017, pp. 227–247.

[10] X. Yang, T. Lee, J. K. Liu, and X. Huang, "Trust enhancement over range search for encrypted data," in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 66–73.