IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 7.918 ⁙ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12259

Privacy-preserving Search over Encrypted Personal Health Records in Multi-Source Cloud

Mrs. Pallavi K N[1], Yashwanth S R[2], Varsha Bai R[3], Thanushree S[4], Tejas P[5]

Asst Professor, Dept of Computer Science, K S Institute of Technology, Raghuvanahalli, Bengaluru[1]

Computer Science and Engineering, Dept of Computer Science, K S Institute

of Technology, Raghuvanahalli, Bengaluru[2-5]

Abstract: Cloud-based Personal Health Record systems (CB-PHR) have great potential in facilitating the management of individual health records. Security and privacy concerns are among the main obstacles to the wide adoption of CB-PHR systems. Multi-source CB-PHR system in which multiple data providers such as hospitals and physicians are authorized by individual data owners to upload their personal health data to an untrusted public cloud. The health data are submitted in an encrypted form to ensure data security, and each data provider also submits encrypted data indexes to enable queries over the encrypted data. We propose a novel Multi-Source Order-Preserving Symmetric Encryption (MOPSE) scheme whereby the cloud can merge the encrypted data indexes from multiple data providers without knowing the index content. MOPSE enables efficient and privacy-preserving query processing in that a data user can submit a single data query the cloud can process over the encrypted data from all related data providers without knowing the query content. We also propose an enhanced scheme, MOPSE+, to more efficiently support the data queries by hierarchical data providers. Extensive analysis and experiments over real datasets demonstrate the efficacy.

Keywords: Security, SMS (Short Message Service), Cloud, Authentication, Cryptography, Confidentiality.

I. INTRODUCTION

Cloud-based Patient Health Record System (CB-PHR) is an electronic medical record that offers advantages for storing and accessing patient health information in a multi-source cloud. Patient recording management is an integral component of the modern-day health care management system.

Technology is always been the savior that workaround for over coming major health care industry challenges, which may improve the management of patient care. However, the features that make electronic records desirable are accessibility, transferability and portability of patient health information, cloud computing is transforming the health care industry.

Different levels with features like collaboration, scalability, efficiency, reachability and security.Health care sector is one such that has been at the forefront of adopting cloud technology. Health care in many other countries is confronted with growing demand for medical treatment and services. The medical records must appropriately have all the patient's medical history. In this paper we propose such a system where the patient's data is protected with high confidentiality to beat the paper based hospital data, the system will meet the necessary important role.

II. RELATED WORKS

Type A. Secured Electronic Health Record Management System

The paper [1] An electronic health record is an E-medical version which provides the medical reports in accessible way. EHRs as the flexibility to supply information about the patient care. The workflow of the cloud service is presented from the perspective of private and public cloud communication scenarios. The essential functionalities involved in this workflow are authentication, authorization, data persistence, Data integrity and data confidentiality.

The paper [2] Recently, privacy preserving in PHRs have drawn researchers' attention [2]-[6]. In this section, we review three categories of work: searchable encryption, order-preserving symmetric encryption and other related work. Search encryption schemes guarantee that the untrusted entity gains nothing about what data owners are searching for, and order-preserving symmetric encryption can guarantee the order of the ciphertexts following with that of the plaintexts. There has been a lot of works for searchable encryption [5], [10]-[15], [30], order-preserving symmetric encryption [34], [23], [29], [30], and other related work [40]–[45].

DOI: 10.17148/IJARCCE.2023.12259

The paper [3] Cloud computing provides a secure infrastructure to hospitals, medical practices, insurance companies, and research facilities. The main objective behind it is to improve computing resources at lower initial capital outlays. Also, cloud computing can reduce the barriers to innovation and modernization of healthcare systems and applications. It ultimately results in making the overall health data management system more flexible and scalable.

Cloud-based healthcare refers to integrating cloud computing technology for the creation and management of cloud-based health care services. More healthcare providers are looking to work with vendors that provide cloud computing solutions to save and retrieve their digital records. As the information can be stored securely off-site, it is regarded as a significant benefit for large and small provider organizations. A Cloud-based healthcare system addresses the following essential requirements in the healthcare industry

EHR includes both medical and non-traditional health and lifestyle-related information, with the consumer as the focus around which the information is recorded. Different health care professionals and administrative staff are using the EHR: physicians, nurses, pharmacists, laboratory technicians and other healthcare employees.

The paper [4] Data access control is another vital issue in cloud storage system. Many researchers focused on multiauthority access control scenario. aimed to address multi-authority problem, and proposed a data access. However, work may be attacked due to utilizing a bidirectional re-encryption method, and described their attack method. To address the data privacy problem and the user identity privacy both, proposed stated that the prior work cannot overwhelm the common shortcoming, like low efficiency and single-point bottleneck. So they proposed RAAC, a robust access control scheme. To reduce the overhead of decryption, Chase [46] proposed a scheme to remove the trusted central authority. proposed a threshold multi-authority ciphertext-policy attribute-based encryption access control solution. However, none of them can be directly utilized to address our problem due to ignoring hierarchical authentication query problem.

The paper [5] Machine learning is widely used technology in the field of science and technology and the rapid growth of the requirements of the people in their daily life improves the utilization of advanced technologies and they used to rule our daily life. Perhaps, consider medical industry. We need to identify the patient health information and in this kind of situation, we need an application which can monitor the patient’s health records from the client side and to the doctor's side. We need a proper channel to design application and have to maintain a model which can identify the predictions and insights of the data.

The paper [6] PEHRs (personal electronic health records) are a set of online technologies that connect individuals to their medical information and enable them to control their own health.as well as healthcare PEHRs allow for the collecting of health data. Information in a single location in order to establish an efficient system Pathway of communication between patients and healthcare providers, as long as essential data can be provided People's demands for medical computers are growing in various areas of healthcare. Extension of communication and information technology system, as well as dispensing massive amounts of medical information. It is crucial to have information systems. Some private hospitals and clinics use a computer-based data system to keep track of their patients, but there is no formal mechanism in place for exchanging
information.

III. OBJECTIVES

- To help the public in the .
- Identify and recover the problem
- An easy way to access patients medical records at any time, anywhere just through a simple click.
- To track the health details and case rates.
- Providing the Security and privacy patient record

IV. METHODOLOGY

Proposed System

The system propose an online web application where the patients data stored within the cloud. Health care practitioners are able to discover a patient with atleast one identification. By selecting the desired patient they can submit the patient’s EHRs(electronic health records) access request. Based on authorization result and allowed access by the patient. Patients are able to view their EHRs from particular health care providers that their associated with.

Algorithm

The user's sign in with the basic details and make themselves an account. The practice of encrypting crucial data when sending data from one computer to another or keeping data on a computer is known as cryptography. The usage of security model follows the principles of security standard. The requirement of confidentiality is achieved through the use of encrypted patient identifier in order to keep personal data separate from health care information through secure exchange. Python supplies a cryptography package that aids in the encryption and decryption of data.

Generating key

The key must be kept secure because it required to Decipher the cipher text. The user will be unable decrypt the communication if the key is lost.

Encrypt data

When the key is generated in plain text the encrypted token also included the current timestamp. If the date is in bytes, the encrypt procedure will fail.

Decrypt Data

The original plaintext is returned if the decryption is successful otherwise, an exception is thrown.

Centralized Access to Digital Health Records

Earlier, all the patients carried separate files or medical records for their every physician's visit. It has become challenging for doctors and staff to maintain and managing the paperwork. This process is now replaced and made more manageable through cloud migration. With cloud services, all the medical records are located at a single centralized location. These records remain accessible through web portals at healthcare centers and can be retrieved whenever required. A secure cloud platform ensures data storage facilities with hosting solutions and virtual machines for swift access to medical records and patients' quick diagnosis.

System Model

The cloud based healthcare system reduces operational spending while giving better personalize care, efficient workflows, resulting in better health services. At the same time patient receives quicker responses from healthcare providers and can access their healthcare data with improved tracking. The system can be used by the hospital administration by providing them with login/sign in credentials.

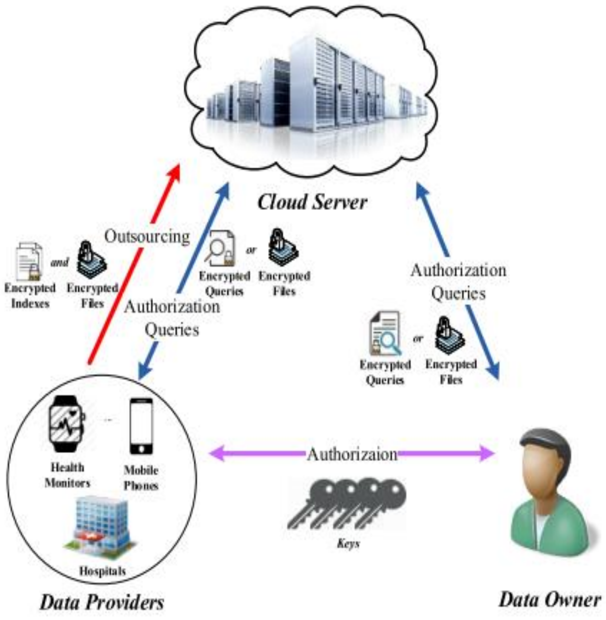

Fig 4.1 :System Model

DOI: 10.17148/IJARCCE.2023.12259

APPLICATION REQUIREMENTS

a) **Android studio:** Android Studio provides a unified environment where you can build apps for Android phones, tablets, Android Wear, Android TV, and Android Auto. Structured code modules allow you to divide your project into units of functionality that you can independently build and test.

b) **AWS:**

Amazon web service (AWS) provide many services, Amazon Elastic Compute Cloud (Amazon EC2) instance is used to deploy the code and run web application also can launch multiple virtual servers provides configure security and networking, manage storage and scalable to handle changes in requirements and reducing need for forecast traffic. Relational Database Service (RDS) is backend database provides setup, operate and scale a relational database on the cloud.

(c) Flask:

Flask Framework is used built the system, it provides configuration and conventions with sensible defaults to get started. It provides production and developer server in order build program and deploy the program. The main key feature using this is built in user convenient functions and roots also provided easily connection with both front end and backend databases.

V. ACKNOWLEDGEMENT

We would like to express our deep gratitude to **Mrs. PALLAVI K N** for her valuable and constructive suggestions during the planning and development of this project. Her willingness to give her time so generously has been very much appreciated. We would also like to thank all the professors of KSIT for their continuous support and encouragement.

REFERENCES

[1] XIN YAO 1,2, (Student Member, IEEE), YAPING LIN1,2, (Member, IEEE), QIN LIU1,AND JUNWEI ZHANG3, (Member, IEEE)1College of Computer Science and Electronic Engineering, Hunan University,Changsha 410006, China2Hunan Provincial Key Laboratory of Dependable Systems and Networks, Changsha 410082, China3School of Cyber Engineering, Xidian University, Xi'an 710126, China Corresponding author: Yaping Lin (yplin@hnu.edu.cn)

[2] Ensuring Privacy and Security in E- Health Records, Available at: https://ieeexplore.ieee.org/document/8440164 https://ieeexplore.ieee.org/document/8440164

[3] Enhanced e-Health Framework for Security and Privacy in Healthcare System, Available at:https://ieeexplore.ieee.org/document/7470795

[4] M.F. Walji, E. Kalenderian, M. Piotrowski, et al. "Are three methods better than one? A comparative assessment of usability evaluation methods in an EHR," International journal of medical informatics May 2014, vol. 83, pp. 361-368.

[5] E. Bélanger, G. Bartlett, M. Dawes, et al. "Examining the evidence of the impact of health information technology in primary care: An argument for participatory research with health professionals and patients," International journal of medical informatics October 2012, vol. 81, pp. 654-662.

[6] Comparing Paper-based with Electronic Patient Records: Lessons Learned during a Study on Diagnosis and Procedure Codes, Jurgrn 2003, Sept, NCBI https://www. healthit.gov/faq/what-electronic-health-record-ehr.

[7]Fellegi, A and mooney, S. (1998). Population and higher individual standard for the quality of life.

[8] Miller, R. J. (1994). "Modernizing Health care through Electronic Medical Record "information system http://www.clinictools.org [3] Brown, P.J. (2000). Evaluation of the quality of information retrieval of clinics finding from a computerized patient database using a semantic technological.

[9] Canadian Medical Protective Association [Internet]. Ottawa (CA): CMPA; 2014. Electronic Records Handbook [cited 2019 Jan]. Available from: www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/handbooks/com_electronic_records_handbook-e.pdf.Office of the Privacy Commissioner of Canada [Internet]. 2012 June. Cloud Computing for Small and Medium-sized Enterprises [cited 2019 Jan]. Available from: www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/