IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96144

Cloud Computing Application for A Protected Medical Records

Darshan Jain S V[1], Swetha C S[2]

Student, Dept. of MCA, Bangalore Institute of Technology, Bangalore, India[1]

Professor, Dept. of MCA, Bangalore Institute of Technology, Bangalore, India[2]

Abstract: The design, implementation, and security measures for personal health records whenthey are kept in external locations, such as the cloud, are discussed in this study. People can access and organise their lifelong health information using a web-based tool called Personal Health Record.Access to the patient's own PHR is under their control. Before outsourcing the data, we apply attribute-based encryption to ensure the confidentiality of personal health records. Here, we concentrate on various PHR owner scenarios and divide users of personal health records into varioussecurity domains to simplify key management for both owners and users. The privacy of patients is ensured to a considerable degree. Our system allows the owner of a personal health record completecontrol over their data. Extensive security and performance analysis shows that the proposed schemeis highly efficient.

KEYWORDS: Personal health records, attribute based encryption, cloud computing, secure sharing

1. INTRODUCTION

The idea of a personal health record (PHR) has gained popularity recently. Since the patient has complete control over their data, we may claim that the model is patient-centric. His PHR can be created, deleted, modified, and shared online. PHR service is offered by third-party service providersdue to the high expense of creating and maintaining data centers.
But there are numerous security and privacy issues for PHR when employing third-party service providers. The fundamental issue is whether or not the PHR owner genuinely has complete control over his data, especially when it is housed on servers run by unreliable third parties. It is crucial to offer data access control methods so that patients have patient-centric privacy control over their own PHRs
We use encryption to protect the data before outsourcing. The PHR owner controls which people have access to what information in his PHR record. Only users with the appropriate decryption key should have access to PHR files. Additionally, the patient will always have the option to remove theiraccess privileges. The PHR may need to be accessed by the authorized users for either personal Or professional reasons. Users are divided into two domains: the personal domain and the public domain.To protect personal health data stored on semi-trusted servers,we adopt attribute-based encryption asmain encryption primitive. Using ABE, access policies are expressed based on attributes of users or data

2. LITERATURE REVIEW

2.1 Personal health records

PHRs are primarily designed to assist user is fully understanding and using that awareness as a tool for controlling it throughout their entire lives The long-term accumulation of health data is what made PHRs valuable. EMR must abide by the tightest criteria for medical document integrity and non-repudiation, which is the main difference between PHR and EMR. The main purpose of PHRs is to aid individuals in gaining a comprehensive awareness of their own health and using that understanding as a tool for managing it for the rest of their life.
Consumer may find information on the internet that will aid in making the best choices and raising the standard of their healthcare. PHP system combine patient health data from a variety of sources, such as the patient's own measurements, the doctor's note,the hospital and records,etc. Data about medications, therapies, drug usage, and other non-medical management topics my also be included in PHRs.The PHP might also include data form an EMR database
EMR must abide by the tightest criteria for medical document integrity and non-repudiation, which is the main difference between PHR and EMR. PHRs are primarily designed to assist people in developing a thorough awareness of their own health and using that understanding as a tool for managing it throughout their lives. PHRs are only valuable if long-term collections of health data accumulate. The main distinction between PHR and EMR is that EMR must adhere to the highest requirements for medical record integrity and non-repudiation. PHRs' primary goal is to assist users in learning as much as possible about their own health. The long-term collection of health records is where PHR value lies.
This not only support one's own health but also gives aspiring medical professionals the necessary training they need to

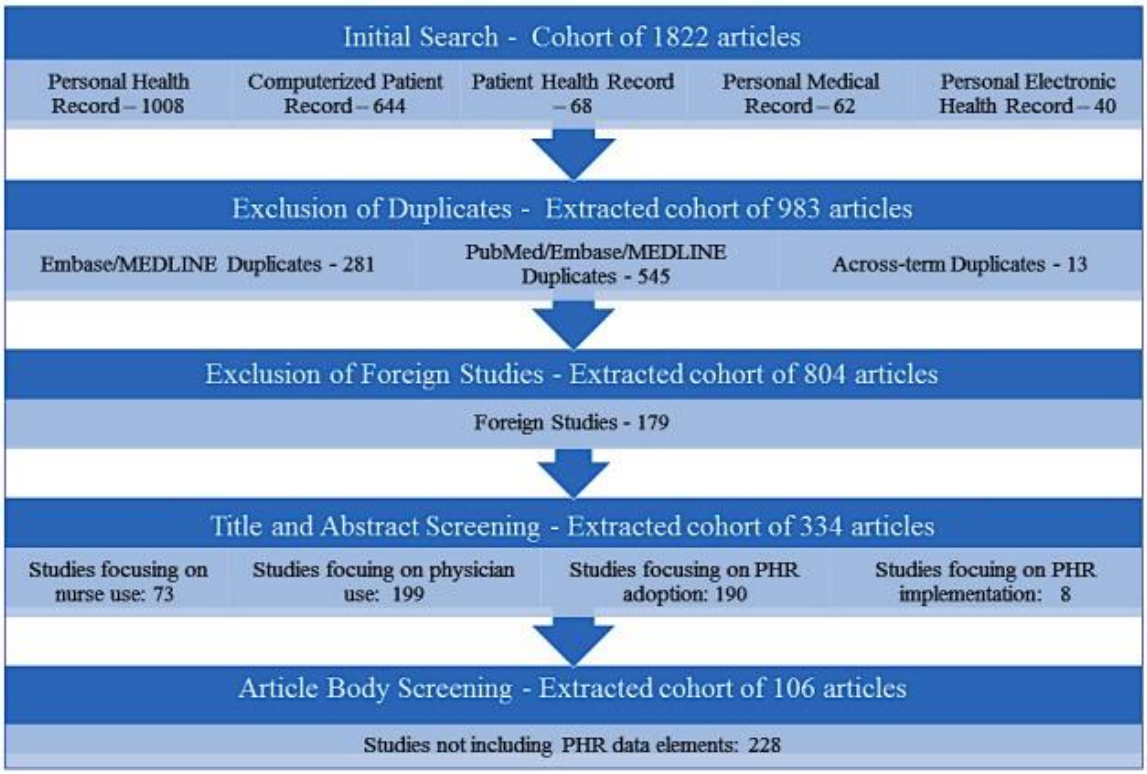
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96144

treat medical codition.PHRs combine and make use of all personal medical and health related records using digital means. PHR system can adapt to the information system of medical institution at all levels in standardized storage of medical institution at all levels in standardized storage format because the bulk of medical service originations information system are already based on HLPAA standards and employ the HL7seven-layer structure. They may update all of the user physiological parameters, medication details, health check results, and other data for lang term retention



Result of the literature review, fig 1: PHR

2.2 PHRs in cloud computing environments

PHRs are becoming more popular in us as result the many benefits of cloud computing. Many health management services ,such as context aware health monitoring, personal health-aware devices ,intelligent alert management, pervasive lifestyle incentive management ,pervasive lifestyle incentive management ,etc. ,are built on cloud computing framework. The American government recently released a proposal for a health cloud that would include cloud services for telemedicine ,hospital healthcare, clinical case histories, and individual health data. The clinical informatics research at the university of Washington developed the patient-center health record which the users own and control

Depending on three sources of the PHRs, there are four different types of emerging PHR system: third-party/free standing,provider-tethered,payer-thethered,and interoperable PHP systems The main issues with PHRs, though, are stability and security. As a means of functioning, the Internet is fully dependent on cloud computing. Based on the research of , this paper quickly cover the primary hazards encountered while constructing PHRs in cloud environments as follows: cloud computing manipulation,shaky user interfaces, impostor users, lost data, unknown PHR profiles, and cloud account theft.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96144

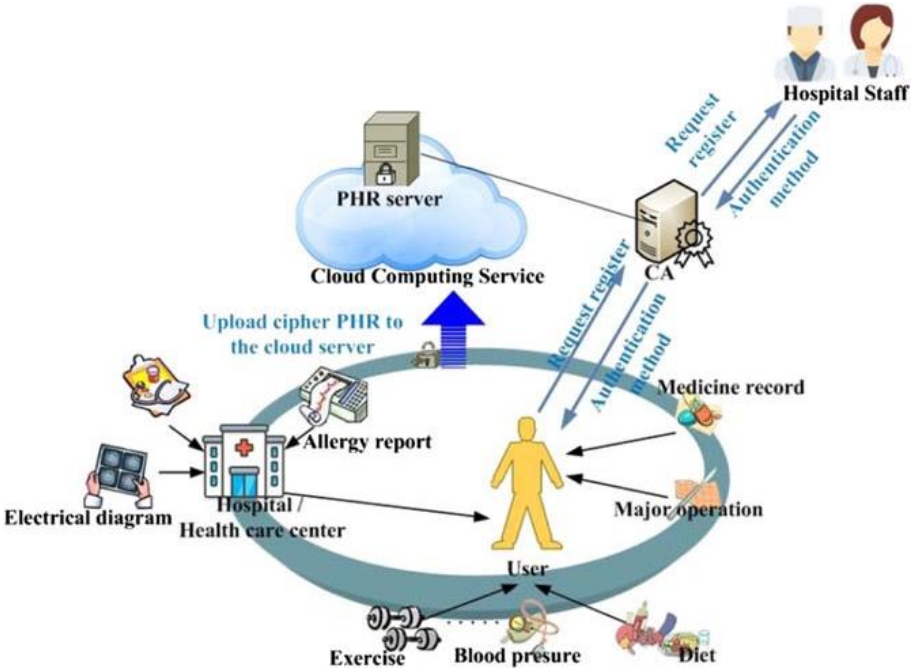


Fig. PHPs in cloud computing environments.

2.3 Electronic Health Records

Health care practitioners often enter and access information in an electronic health record, or "EHR." It might just contain data from a single healthcare professional or a group practice. The majority of social insurance providers have passed past the EHR adoption phase and are now focusing on their constantimprovement. All work processes identified with the patient's needs in mind moving forward must behandled by EHRs. These job procedures include handling external reports, messages, and correspondence with patients in general. To access all of their doctors and have conversations with them, patients should only need to sign into one patient entry EHRs will also need to allow free accessto confidential data. The majority of the real-world reports that social insurance providers will need to handle include clinical quality measurements, requests that will affect staffing numbers, and disease patterns In essence, EHRs' role as repositories for permanent data will progressively disappear. The future of EHRs is dependent on the level of connectivity between patients and their social insurance providers . Information about patients' health needs to be shared across all locations where care is sought. Quick access to information as well as quick communication with any provider of medical services

Fig. Electronic Health Records

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96144

3. METHODOLOGY

With the continued development of PHRs and similar initiatives ,patient-centered self-maintenance and management of the patients own health state and care have been advocated in recent years PHRs are being adopted by more and more medical facilities, which not only improves patient communication with caregivers but also has the potential to cut expenses and boost productivity.Due to the continual development of cloud environment, personal health statues are nor more effectively and precisely recoded and transferred through wireless network environment to cloud backed served for information integration In cloud environments, using PHRs in healthcare can provide a number of advantages and encourage consumer to enroll in healthcare plans. The dynamic access mechanism on the PHR system mut be able to meet the needs of numerous user in various context because PHR system store a variety of data (such as record of medical visits, medication record, physiological information.)that a can be used numerous user(including the patient, the attending physician, family member, caregivers etc.)When accessing the data privacy and security of the data must be ensured during transmission
In light of the aforementioned security concerns, this study suggests an efficient identity authentication system to confirm that users are legitimate. PHR systems must include a robust method to safeguard users' privacy at all times; for instance, some patients with specific illnesses do not want their condition to be made public. This is especiallytrue given that the architecture of such systems typically relies on cloud computing for data transmission. Traditional security architectures and protocols are incompatible with these conditionsand settings.

ADVANTAGES OF PROPOSED SYSTEM

- Obtain information about the patient's specifics quickly.
- In the event of an emergency, the doctor and other emergency departments will swiftly gather all the necessary information and begin administering care.
- The PHR owner is capable of taking care of his own health in the event that medicalprofessionals and facilities are not readily available.
- To offer information with quick and simple access.
- Creating an environment that is user-friendly.
- To offer write access control and data confidentiality.

APPLICATION

Any organization can use this application to store their employees‟ medical informant

4. CONCLUSION

Security against intruders and hackers is required for the personal health record system. Basic security measures are included in scalable and secure sharing to guard against loss and unauthorized access to the information. This study offered a new method for the PHR system now in use to increase security utilizing attribute-based encryption, which is crucial because these are distinctive and difficult to crack. As we improve privacy assurance, we are also minimizing the key management challenge.

5. REFERENCES

[1]. Johnston, D., Middleton, B., & Bates; Kaelber, D. C.; Jha, A. K.
[2]. D. W. (2008). An agenda for research on personal health records (PHRs). AmericanMedical Informatics Association Journal, 15(6), 729–736.
[3]. Joux, A. (2002). Public key cryptosystem building blocks: the weil and tate pairings. pp. 20–32 in International Algorithmic Number Theory Symposium.
[4]. J. AHIMA (2007). A united stance statement for healthcare consumers on the importance of personal health records. American Medical Informatics Association Journal, 78(4):22–24.
[5]. Johnson, K. B. and Kim, M. I. (2002). Personal health records: Analysis of usefulness and functionality. American Medical Informatics Association Journal, 9(2), pp. 171– 180.
[6]. P. Yujin and Y. Hyung-Jin (2020). Recognizing personal health records and promoting their market. Research in healthcare informatics
[7]. Patient-centric and fine-grained data access management in multi-owner settings forprotecting personal health records

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96144

in the cloud. Privateness and security in communication networks. the following URL: 10.1007/978-3-642-16161-2 62. Horvitz, E.J., Lauter, K.E., Chase, M.P., and Benaloh, J.C. (2009). Encryption managed by the patient: Keeping electronic medical records private. CCSW '09: Cloud Computing Security Workshop 2009 Proceedings, 103–114.

[8]. Chung, Y. F., & Liu, C. H. (2017). System for safe user authentication in wireless sensor networks in healthcare. 4. https://builtin.com/healthcare/recordbinding- healthcare-applications-companies. Computers & Electrical Engineering,