Survey on Personal Health Record using Cloud Computing

H Karthik[1], Dr. Suma[2]

[1]Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India.

[2]Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India.

---*******---

Abstract

As a result of using an online personal health record (PHR), individuals may save, access, and share their private health information in a more efficient manner. To take advantage of the cloud's scalability and lower operational costs, PHR service providers should shift their apps and data to the cloud. In order to prevent unauthorised access to their personal health records, patients must encrypt their PHR data before storing it on cloud servers. Access to Personal Health Records (PHRs) can be challenging to scale and environmentally friendly under encryption. PHRs must be encrypted in such a way that the number of persons with access to the data does not become an issue. An important consideration when there are several users of a PHR device and each user has access to a unique set of encryption keys is the ease with which the keys may be distributed to each user. For the time being, management information can only be accessed through cryptographic methods for single-proprietor companies.

A novel cloud-based solution to PHR management is proposed in this study, as explained above. Using ABE methods to encrypt each patient's Personal Health Record (PHR) data enables for granular and scalable access control for PHRs. Additionally, our approach provides green and on-call revocation of individual access credentials, as well as break-glass access in the event of an emergency.

Keywords: Personal health records, cloud computing, Electronic Health Record, fine-grained access control.

I. Introduction

The Personal Health Record (PHR) allows people to share health information with one another (PHR). A patient's personal health information can be accessed at any time through a PHR service if they have access to a web browser and an active Internet connection. Accessing and exchanging medical records has never been easier thanks to this cutting-edge technology. Anyone can request access to a patient's clinical data, including family members and friends, as well as other healthcare professionals and academics who are working on related projects. Healthcare expenditures may be decreased, while quality and patient happiness would be improved, if this strategy were to be used.

There are almost unlimited and elastic storage and processing resources available when using the cloud as a computer platform for software development. Thus, in order to save money, PHR carriers are more likely than not to migrate their PHR storage and alerting systems onto the cloud. Two of the most popular personal health records are Google Health and Microsoft HealthVault (PHRs).

However, even if security and privacy worries about cloud-based PHR services are unfounded, they may not be extensively used. At this time, we're concerned about who has access to the PHRs stored on a cloud server and how that information is used. Confidential medical records are no longer accessible to patients after they are stored on a computer. Misbehaviour by a cloud service provider employee might result in the disclosure of Personal Health Records (PHRs) (PHI). An employee of the Veterans Affairs Department took the Social Security numbers and medical conditions of 26.5 million war veterans without permission. This comes as no surprise, given the amount of research done on the subject. Because the cloud platform is exposed to the public, servers running in the cloud are vulnerable to outside threats.

Individuals with personal health records (PHRs) have the option to choose whether or not to share their information with PHR providers, who may encrypt the data. Access manipulation mechanisms on the server employ same encryption methods, thus PHR records must be encrypted in the same way. Patients must produce and distribute their own decryption keys to their genuine customers. Anyone who does not have the proper keys to access PHR data should not have any access to it. A company's PHR has to be able to restrict access to certain features and functionalities to specific consumers. Once they've mastered it, they'll require the higher levels of access that come with it. With several owners, PHR systems are described as "patient-centric" since each owner has a unique cryptographic key to safeguard his or her personal data.

II. Theoretical Background

2.1 Cloud Computing

Based on the method of distribution, cloud computing may be broken down into three distinct layers: Because only contractual clients have access to the dedicated resources of the cloud computing vendor at a pay-per-use rate, this "is a single tenant cloud tier" (Ram govind et al. 2010) [3]. Since so much hardware, such as servers, routers, and load balancers, may be saved with IaaS, the missing starting costs are particularly substantial. Depending on how much time is spent using this service, there is a monthly fee. Platform as a Service (PaaS) provides an integrated environment for the design, development, testing, installation, and replacement of customised web applications. If (Xu, 2010) [4] is correct. Software vendors, developers, and value-added resellers can operate prefabricated services on the PaaS platform. A "SaaS" software programme can be accessed, utilised, and maintained from a remote location by one or more service providers. According to Smith (2010). A typical outsourcing approach and proprietary software are at odds with each other under the SaaS model (Buxmann et al. 2008). You'll have to pay for more features if you wish to customise or expand the programme. Use of "pay per use" (Ramgovind et al. 2010) allows fixed expenditures to be transformed into variables, therefore reducing the overall cost of the project.

An further approach of distinction is to classify clouds depending on their deployment mode [6]. A private cloud and a public cloud are the two most popular kinds of cloud computing. Hybrid cloud options are available, including community and government cloud options, depending on your needs. Overlapping clouds have many of the same characteristics. Internal statistical facilities that aren't accessible to the general public are known as "private clouds," which are defined as those that are large enough to profit from cloud computing. Using "the company itself, akin to Intranet capabilities," "all cloud assets and apps are controlled by using the business itself." [7]. A private cloud is a superior option than a public cloud when it comes to security, compliance, and regulatory requirements. [8]. To define a public cloud, we use the phrase "the cloud infrastructure is created to be the complete public or a huge business institution." Most public cloud services are based on pay-as-you-go pricing structures, which allow IT organisations to avoid future capital expenditures and substitute them with more flexible operational costs. Public cloud computing raises security and privacy issues despite its widespread availability. Due to the increased burden of protecting all apps and data accessed on a broad public cloud, public cloud models are considered less secure than other cloud models. The secure network of the hybrid cloud connects private cloud services to at least one or more external cloud services, which are thus centrally controlled and provided as a unified unit. No matter whether type of external cloud service is used, data and applications may be transported between them since they all use the same technology, regardless of whether they are private, public, or community clouds.

III. Electronic Health Records

EHRs are digital representations of a patient's medical history, which are kept by a company over time and include demographics, developed notes, problems, medications, vital signs, previous hospital history, immunizations, laboratory information, and radiology reports for that person's care under a specific company. Two of the advantages of having an EHR include automated access to data and the potential to streamline a clinician's workflow. Other care-related tasks, such as evidence-based decision support and effective management and reporting, can also benefit from the usage of several interfaces.

Keeping track of a patient's health state throughout time is the goal of electronic health records (EHRs). As a result, patients don't have to spend as much time hunting through old paper scientific data, and the information they do have is more recent, correct, and easy to understand. Privacy and security are also provided, yet open contact between the patient and provider may be maintained at all times. It is less probable that documents would be misplaced because there is just one record that may be altered. Additionally, it is less expensive. Virtual data stored in a single EMR (electronic medical record) makes EMRs more powerful when retrieving medical records for analysis of possible developments and long-term changes in a patient. EHRs and EMRs are making it easier to perform population-based research on medical records because of their widespread use.

When it comes to EHR deployment, the benefits of cloud computing include scalability, security, and privacy; a shared platform and independence; reduced errors and improved quality; structure, structure flexibility; and the capacity to share data [9].

3.1 Cost

consumers save money on hardware, software, and services expenses by using cloud computing, which eliminates the need to install and maintain software and speeds up data access. [10, 14, 19, 24, 27-29].

3.2 Security and Privacy

In electronic health records, the storage location of patient data is a concern. Data privacy must be protected by strict restrictions. Techniques such as character-based encryption, authentication, and digital signatures are employed in cloud environments to maintain the confidentiality of health information. [11, 12, 13, 15-20, 22, 24, 26-28].

3.3 Scalability

Network or process feature that decreases the burden on a network or process. "Scalability" refers to a system's ability to increase resources while maintaining or improving overall performance. When developing and deploying large and complex systems, such as databases, it is vital to keep scalability in mind. There is no requirement for users to be ready for maximum resource consumption, as resources can be supplied as needed by the users themselves. [10, 11, 14, 15, 19, 22].

3.4 Implementation

The ability to install software that is not reliant on Windows and can also be loaded on a mobile phone is one factor that contributes to the independence of this technology as well as other devices operating in this market. It is possible to implement numerous databases, such as SQL, Oracle, or cash, while using cloud computing, which is one of the advantages of using this method. The installation of software does make it feasible to achieve a higher level of independence. This particular system does not call for any kind of hardware due to the fact that all of the files and programmes are stored in a singular format. [10, 23, 30].

3.5 Ability to search and exploration

Using a broad variety of search algorithms, cloud-based electronic health records may be searched for so much information and data about patients [10, 16, 18, 23, 25]. Electronic health records (EHRs) can preserve information on a patient's mental and behavioural state as well as their prescription history [24]. Clinical and insurance data can be retrieved independently of each other.

3.6 Flexibility

Electronic health clouds should be able to meet the demands of healthcare providers of all sizes and specialisations. For operations, users, management, and service quality, this functionality should be viable. There should be considerable configuration flexibility in the cloud computing infrastructure to meet the various requirements of healthcare providers. Adaptability is key, and this may be accomplished with little work and expense. [10, 13, 21, 25, 30].

3.7 Exchange and Sharing ability

Data and information transfer and sharing are extremely important in health information systems, but they must be handled with extreme caution due to the presence of several diverse components. Sharing electronic health information via the internet and in the cloud has its drawbacks. In order to get over these obstacles, the following materials need be assembled: A single, secure and integrated specification for HER will be available to you as part of this [19].

IV. Conclusion

Personal health records stored in the cloud are the focus of this study's findings. In order to protect their privacy, we believe that patients should be given the ability to encrypt and fine-tune access to their Personal Health Records (PHRs). Using several PHR owners and customers instead of just one helps the framework simplify key control when there are many PHR owners and consumers. Consider the advantages of cloud computing in EHR implementation, such as cost savings, improved privacy and security, scalability, reciprocal performance, the implementation of search and exploration capabilities, flexibility and sharing capabilities. These are all important aspects of cloud computing. There are certain downsides to cloud computing, such as the lack of administrative help. In addition, the lack of user competence, knowledge, and expertise is a challenge for cloud computing [9].

References:

1. by M Li · Cited by 640 — main concern is about the privacy of patients' personal health data and who could gain access to the PHRs when they are stored in a cloud server.
2. Security and Privacy in Communication Networks: 6th International ICST Conference, SecureComm 2010.
3. by S Ramgovind · Cited by 628 — where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. https://uir.unisa.ac.za/bitstream/10500/3883/1/ramgovind.pdf
4. Adaptive Applications in Cloud Environments - European ... https://ec.europa.eu/research/participants/documents.
5. Challenges for adopting cloud-based software as a service ... https://www.researchgate.net/publication/221409564_Challenges_for_adopting_cloud-based_software_as_a_service_SAAS_in_the_public_sector
6. Privacy Engineering: Personal Health Records in … Another way of distinguishing clouds is the classification by type of deployment.
7. Personal Health Records in Cloud Computing Environments. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.667.7673
8. What is Cloud Computing? Everything You Need to Know https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing
9. Capabilities and Advantages of Cloud Computing in the Implementation of Electronic Health Record

   https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5869277
10. Bahga A, Madisetti VK. A cloud-based approach for interoperable electronic health records (EHRs). IEEE J Biomed Health Inform. 2013; 17(5): 894-906.
11. Huang J, Sharaf M, Huang CT. A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud. In Parallel Processing Workshops (ICPPW). 2012 IEEE 41st International Conference on 2012: 279-87.
12. Demelo Silva L, Araujo R, da Silva FL, Cerqueira E, editors. A new architecture for secure storage and sharing of health records in the cloud using federated identity attributes. e-Health Networking, Applications and Services (Healthcom), 2014.
13. Ibrahim A, Mahmood B, Singhal M, editors. A secure framework for sharing Electronic

Health Records over Clouds. Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on, 2016.

14. Fernández-Cardeñosa G, de la Torre-Díez I, López-Coronado M, Rodrigues JJ. Analysis of cloud-based solutions on EHRs systems in different scenarios. J Med Syst. 2012; 36(6): 3777-82.
15. Preethi M, Balakrishnan R, editors. Cloud-enabled patient-centric EHR management system. IEEE conference of Advanced Communication Control and Computing Technologies (ICACCCT), 2014; 1678-80.
16. Liu Z, Weng J, Li J, Yang J, Fu C, Jia C. Cloud-based electronic health record system supporting fuzzy keyword search. Soft Computing. 2016; 20(8): 3243-55.
17. Deshmukh P. Design of cloud security in the EHR for Indian healthcare services. J of King Saud University-Computer and Info Sci. 2017; 29(3): 281-7.
18. Xhafa F, Li J, Zhao G, Li J, Chen X, Wong DS. Designing cloud-based electronic health record system with attribute-based encryption. Multimedia Multimed Tools Appl. 2015; 74(10): 3441-58.
19. Mohammed S, Servos D, Fiaidhi J. Developing a secure distributed OSGI cloud computing infrastructure for sharing health records. Conference of Autonomous and intelligent systems. 2011: 241-52.
20. Stingl C, Slamanig D. Health records and the cloud computing paradigm from a privacy perspective. J Healthc Eng, 2011; 2(4): 487-508.
21. Hoang DB, Chen L, editors. Health records protection in cloud environment. Network Computing and Applications (NCA), IEEE 13th International Symposium on, 2014.
22. Manoj R, Alsadoon A, Prasad P, Costadopoulos N, Ali S. Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud. 5th IEEE International Conference onSan Francisco, CA, USA, 2017.
23. Souza S, Gonçalves R, Leonova E, Puttini R, Nascimento A. Privacy-ensuring electronic health records in the cloud. Concurrency and Computation. Concurr Comput. 2017; 29.
24. Khansa L, Forcade J, Nambari G, Parasuraman S, Cox P. Proposing an intelligent cloud-based electronic health record system. IJBDCN. 2012; 8(3): 57-71.
25. Alabdulatif A, Khalil I, Mai V, editors. Protection of electronic health records (EHRs) in cloud. Engineering in Medicine and Biology Society (EMBC), IEEE 35th Annual International Conference, 2013.
26. Schweitzer EJ. Reconciliation of the cloud computing model with US federal electronic health record regulations. J Am Med Inform Assoc. 2011; 19(2): 161-5.
27. Ramu G, Reddy BE. Secure architecture to manage EHR's in cloud using SSE and ABE. Health Technol. 2015; 5(3-4): 195-205.
28. Wu R, Ahn GJ, Hu H, editors. Secure sharing of electronic health records in clouds. Collaborative Computing: Networking, Applications and Work sharing (Collaborate

Com), IEEE 8th International Conference on, 2012.

29. Zangara G, Corso PP, Cangemi F, Millonzi F, Collova F, Scarlatella A. A cloud-based architecture to support Electronic Health Record. Stud Health Technol Inform. 2014; 207: 380-9.

30. AbuKhousa E, Mohamed N, Al-Jaroodi J. e-Health cloud: opportunities and challenges. Future Internet. 2012; 4(3): 621-45.