

**A Project Synopsis on**

***“A reliable authentication scheme of PHR in cloud computing”***

**For the Degree of Bachelor of Technology**

**In**

**Computer Science & Engineering**

**Under the Faculty of Engineering**

**By**

Mr. Vinod Shivaji Asabe

Mr. Sudhir Hanmant Takale

Mr. Kapil Navanath Pise

Mr. Ashok Subhash Pawar

**Under Guidance of**

Prof. M. S. Koli



**Department of Computer Science & Engineering**

**SKN Sinhgad College of Engineering, Korti, Pandharpur**

**Academic Year 2023-24**

**ABSTRACT**

A patient-centered personal health records system has been actively promoted in recent years. Its purpose is to maintain long-term personal records and health improvement plans. It combines a cloud computing environment to build a personal health records system to quickly collect personal information and transfer it to the back end for storage for future access. However, in a cloud environment, the message transmission process is more open. Therefore, a lack of an authority security mechanism for the users of such an architecture will result in distrust and doubt by the users. This adversely affects the implementation and quality of long-term health plans.

To protect the crucial privacy of the users from malicious attacks or theft, it is necessary to ensure that the users have different authority to access their personal health records under the cloud computing environment and manage the openness of their authority to other users. A secured identify authentication mechanism can ensure that only legitimate users can log in to the system and obtain system service resources through verification. For a personal health records system in the cloud computing environment, this study proposes a secure and reliable user authentication mechanism allowing relevant users access to the user’s PHR in the cloud based on their authority.

The proposed authentication method uses a password combined with a smart card, allowing the owner and authorized users to log in to the system and access the relevant personal records.

**Keywords:** PHR, Cloud Computing, Authentication, Encryption, etc.

**MODULES:**

1. Patient
2. Doctor

**Patient:**

1. View PHR
2. Report
3. Appointment

**Doctor:**

1. Appointments
2. History
3. Update Patient Records

**INDEX**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Title** | **Page Number** |
| 1 | Introduction |  |
| 2 | Literature Review |  |
| 3 | Problem Statement |  |
| 4 | Objective |  |
| 5 | Scope |  |
| 6 | Software / Hardware Requirements |  |
| 7 | Methodology |  |
| 8 | Conclusion |  |
| 9 | References |  |

1. **Introduction**
   1. **What is PHR?**

Personal Health Record (PHR) is an digital record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff with permission of individual

***Types of Health Record:***

**1) PHR:** A personal health record, or PHR, is an electronic application through which patients can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment.

**2) EMR:** An electronic medical record (EMR) is a digital version of all the information you’d typically find in a provider’s paper chart: medical history, diagnoses, medications, immunization dates, allergies, lab results and doctor’s notes within one health care organization.

**3) EHR:** An electronic health record (EHR) is a digital version of a patient’s paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users.

* 1. **Problems with current Health Record systems:**

Nowadays, most healthcare organizations do not have the facility to protect the patient’s data from unauthorized access, and hence present Health Record System may fail to meet the privacy requirements of patients.

The healthcare industry still seems to be an easy target for hackers and this is due to the lack of technological understanding within the industry. The recent attacks on the healthcare industry are the evidence of data security challenges in this sector. The target attacks include, but not limited to, phishing attacks and ransomware which are successful in retrieving personal data. In fact, the high success rate of ransomware attacks has shown the lack of basic security measures such as backup and system updates. Healthcare applications like PHR are very sensitive as they directly involve personal and critical data, which must be secured from unauthorized access.

* 1. **What is Cloud Computing?**

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant’s ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).

* 1. **Types of Cloud Models:**

***1) Public Cloud:*** Public blockchains are permissionless in nature, allow anyone to join, and are completely decentralized.  Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data.

***2) Private Cloud:*** Private blockchains, which may also be referred to as managed blockchains, are permissioned blockchains controlled by a single organization. In a private blockchain, the central authority determines who can be a node.

***3) Community Cloud:*** Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain.  Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.

***4) Hybrid Cloud:*** Hybrid blockchains are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations.

* 1. **Benefits of Blockchain in EMR**

Keeping our important medical data safe and secure is the most popular blockchain healthcare application at the moment, which isn't surprising. Security is a major issue in the healthcare industry. Between 2009 and 2017, more than 176 million patient records were exposed in data breaches. The perpetrators stole credit card and banking information, as well as health and genomic testing records. Some of the major befits of using Blockchain in EMR are:

***Decentralization:*** The same copy of healthcare records will be available to all

stakeholders and all of them have same access and control privileges. No single

entity will have control over the data.

***Security and Privacy:***Blockchain will help to create tamper-proof record through its

immutability property. All records are encrypted and time stamped and added in to

existing distributed databases in chronological order. Privacy and identity of patient

is protected through cryptographic keys.

***Data Ownership:*** Patients will get assurance that their records are not misused or

altered. He will get full control of his data. This is achieved by strong cryptographic

protocol and pre-defined smart contract.

***Data Verifiability:*** Every stakeholder can check the integrity and validity of records

stored on Blockchain. This feature is mostly applicable where data verification

process is required such as insurance claim processing.

***Trust:*** As Blockchain records are accessible to all, nobody has to question whether

information has been altered for personal benefit.

1. **Literature Review**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Author** | **Year** | **Objective** | **Pros** | **Cons** | **Platform**  **Used** |
| Chien-Yun Chang | 2021 | PHRs systems allow people to access and manage their own medical or health information. | * Proposed Solution follows GDPR/HIPAA | * Implementation and testing pending. - Ongoing monitoring and user feedback required. | Cloud Platform |
| Zhen-Yu Wu | 2021 | The users should possess the absolute power to control their own PHRs, decide which sections can be made open-access for those who are authenticated. | * Proposed Solution follows GDPR/HIPAA * The PHRs should cover all medical records and other healthcare information of the user; | * Any issues with data quality, such as inaccuracies or inconsistencies, could have serious consequences for patient care and safety. | Cloud Platform |

1. **Problem Statement**

Develop an Application which can contain “A reliable authentication scheme of personal health records in cloud computing”.

1. **Objectives**
   1. Our goal is to Develop Cloud-Based PHR System.
   2. Efficient Record Management.
   3. To study and increase the performance of PHR.
   4. Anytime, Anywhere Accessible.
   5. Securely Preserve Patient Medical Data.
2. **Proposed Work**

Electronic medical records (EMR) often contain highly sensitive healthcare data, which are periodically distributed among healthcare providers, pharmacies and patients for clinical diagnosis and treatment. Furthermore, critical medical information must be regularly updated and shared where proper consent is provided by the patient. Along with this we need strong availability, fast access and the appropriate encryption of these records.

There are currently several approaches regarding EMR management and howblockchain technology can be utilized to improve it. We present Hyperledger Fabric blockchain architectures for EMRs to create a trusted and transparent encyclopedia of patient data in EMRs that pledges controlled data access and integrity among the stakeholders of the EMR system.

Blockchain ensures that the majority of the network nodes must validate the information blocks stored on the ledger before being posted to the ledger based on stated and agreed rules.A private permissioned blockchain like Hyperledger Fabric is suitable in achieving patient’s privacy and confidentiality, such as their healthcare-related private details. Below are the steps showing the secure workflow of patient records and activities.

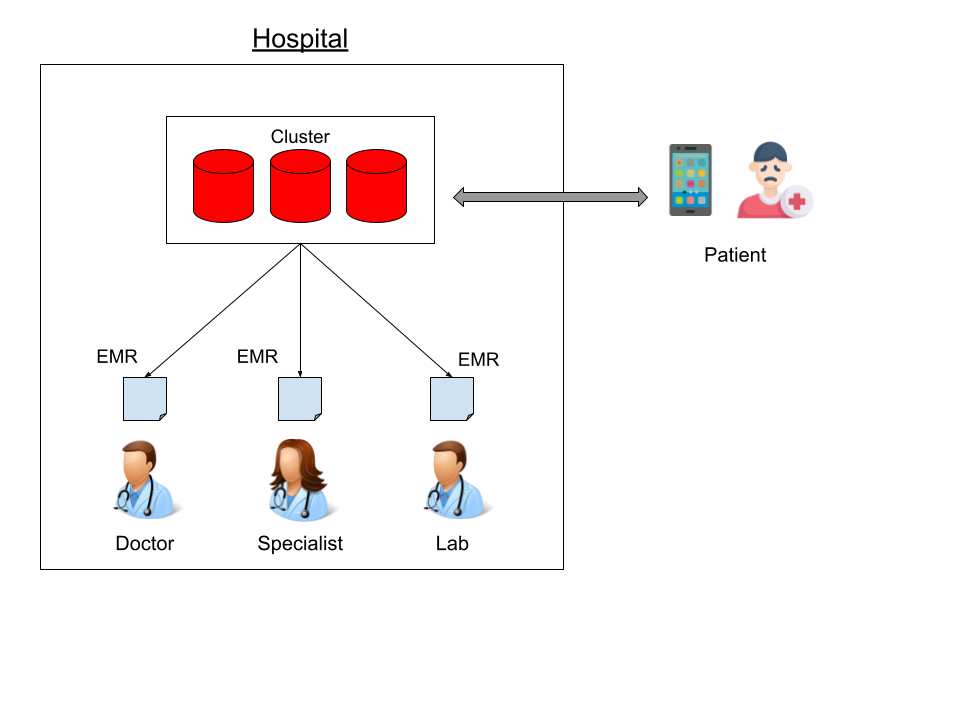
**Step-1:** Initially, the patient visits the physician (doctor) by registering itself to the hospital counter. This patient data consists of medical history, current problem and other physiological information and is stored in the local database connected to the system.

**Step-2:** An EMR is generated from the initial data collected in step (1) for each patient. Additionally, other medical information such as laboratory test results, medical imaging, nursing care, and drug history-related data will also encompass the EMR.

**Step-3:** The patient who is the owner of EMR has the sole authority to give different access rights and permissions of sharing and using the sensitive information to various stakeholders of the healthcare ecosystems to achieve data privacy and secrecy.

**Step-4:** The EMRs have now been stored permanently in the blockchain ledger and other decentralized storage systems. The local database is used to make sure that patient records at initial stage can be modified and stored locally before being updated at the ledger.

**Step-5:** Hospital and ad hoc clinics, are one of the critical stakeholders who have authorized access to the blockchain ledger to provide better and efficient medical services to the patient using the EMRs. This blockchain-enabled EMR system ensures the secure and transparent transfer of EMRs to various healthcare providers in the globe so that the patient’s records can be made available and accessible any time at any place validated and verified through a distributed ledger.



*Fig. Blockchain-enabled EMR management in healthcare*

**5.1Participant Permissions**

|  |  |
| --- | --- |
| **Role** | **Permissions** |
| Admin | Has full access to all users, doctors and system resources. |
| Doctor | Create, delete, read and update their own participant information.  • Read/update permissioned HR of Patient: If a patient has authorized a practitioner, the latter is able to read or update the patient’s HR.  • Refer to other practitioners: Practitioners can grant update rights to other practitioners on EMRs they have been authorized to update. |
| Patient | Create, delete, read, and update their own participant information.  • Grant update rights to practitioners: the patient can grant the doctor the correct permissions to update their PHR.  • Remove permissions from practitioners: The patient can revoke rights from a practitioner if they see fit. |

**5.2 EMR Architecture using Hyperledger Fabric Enabled Blockchain**

We choose Hyperledger enabled private permissioned consortium blockchain, which uses the Hyperledger Fabric platform. Multiple healthcare providers with in a hospital are connected to form a private peer-to-peer consortium network. The permission to join the fabric network is determined based on consensus among the participating stakeholders. Furthermore, the efficiency of fabric is much more compare to other public blockchains as it executes more than 3,500 transactions per second.

In the fabric architecture, a permissioned private blockchain network is created where all the participating healthcare stakeholders and their end-users are identified and registered by the health authority using the membership service (MSP) component of the fabric using certificate issuing (C.A.) authorities. To create a trusted environment between untrusted participants, the fabric provisions an identity management system that introduces the notion of membership service that established rules and regulations by which different stakeholders (identities) are governed, authenticated, validated, and verified to be part of the network and allowed to access the EMRs systems for ensuring secrecy, privacy, and confidentiality among the stakeholders in the network. The fabric network comprises different peer nodes, and each peer node can be an endorser or committer node. It also contains an ordering service component, also called Orderers. This service accepts the endorsed transactions from the patient, orders them into groups of blocks with cryptographic signatures of the ordering peers, and finally broadcasts these blocks to the committing peers in the blockchain network for validations against the endorsement policies.

*Fig. Hyperledger fabric consensus mechanism for EMRs*

**6. Software / Hardware Requirement**

1. Windows OS
2. 8GB RAM, 256 GB SSD/ 1TB HDD
3. Languages: Java ( Spring Boot ) & Angular
4. Cloud Platform: AWS
5. Database : MySQL / Cloud-Native Database Service.
6. IDE : Eclipse, Visual Studio Code
7. Git (For Application Controlling & Development)

**Methodology**

**Algorithmic steps/Procedure--------------------------------------------------------------------------------------------------------------------**

**Conclusion**

Cloud-based PHR systems offer flexible, on demand access to the individuals. This System support proactive patient engagement in healthcare. Efficient record management and secure data handling are the main advantages of the PHR system. Cloud resources enable scalable PHR services. PHR has innovative security mechanism which enhances data protection and data privacy.

**References**

1. Miller, R. H., & Sim, I. (2004). Physician’s use of electronic medical records: Barriers and solutions. Health affairs, 32(2), 116–126

2. AHIMA, J. (2007). The value of personal health records: A joint position statement for consumers of healthcare. Journal of the American Medical Informatics Association, 78(4), 22–24.

3. US Public Law. (1996). Health Insurance Portability and Accountability Act of 1996, 104th Congress, Public Law, 104–191.

4.Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). Journal of the American Medical Informatics Association, 15(6), 729–736.

5.Shamir, A. (1985). Identity-based cryptosystems and signature schemes. Advances in Cryptology-Proceedings of CRYPTO’84, Springer-Verlag LNCS 196.

Estimated Date of Completion:

Date: 15/11/2023

Mr. Vinod Shivaji Asabe

Mr. Sudhir Hanmant Takale

Mr. Kapil Navanath Pise

Mr. Ashok Subhash Pawar

Prof. S. S. Ingole Prof. S. S. Bhimade Prof. S. V. Pingale

(Project Guide) (Project Coordinator) (HOD, CSE)

Place: Korti, Pandharpur.

Date: