ISSN: 2040-0748 Vol-10 Issue-01 JAN 2021

Implementing blockchain-based medical file sharing systems with decentilization attributes

G.Sri Lakshmi [1], Amritha Mishra [2],
Assistant Professor [1],[2],
Department of IT, SRK INSTITUTE OF TECHNOLOGY ENIKEPADU VIJAYAWADA
Mail Id : sree.gpk@gmail.com, Mail id : amrithapandey@gmail.com

ABSTRACT

Electronic health record (EHR) is patient data that store health information in digital format. Patient-centred data enables an authorized user to access the data at any time, anywhere. E-healthcare provides increasing social benefits, health benefits and reduced medical errors. The most difficult aspect of improving the use of IT frameworks in healthcare is the security issues of the systems that store health information. In the health sector, Blockchain is a revolution that may bring considerable changes in offered health services. It solves the issue of adapting and building a health care system in the healthcare community, pharmaceutical industry and insurance companies. This paper presents a framework for securing healthcare data. Public Ledger, private ledger, smart contracts and context-based access control are the basic principles behind the proposed framework. This proposed model further provides interoperability, secure storage, and reliable access to patient's data

Keywords:Blockchain, Healthcare, Smart Contracts, Distributed Ledger, Hashing, Electronic Health Record

INTRODUCTION

Patient data that store personal health information in digital format is the core of electronic healthcare. Data focused on patients allow any approved user to access the data from anywhere and at any time. The electronic health system also saves money by minimizing the efforts and storage space (Simpson, 2015). Increased social and health benefits, as well as reduced chances of mistakes, are achieved through e-healthcare. The digital reproduction of paper-based health documents is the electronic medical record (EMR). EMR further evolved into EHR that help the various stakeholders to share medical information quickly. The primary goal is to exchange medical information between multiple doctors and diverse stakeholders, including the Government, patients, health service providers, insurers (Menachemi & Collum, 2011). Healthcare Information and Management Systems Society, Inc. (HIMSS) is a non-profit corporation to extend health protection, security and convert health information through information technology. The main operation domain of HIMSS is North America, Asia Pacific, the UK and the Middle East. HIMSS' primary objective is to develop worldwide e-healthcare. Healthcare problems include attackers trying to modify health figures, leading to serious health system harm and

severe attacks, such as a ransomware attack and a lack of cybersecurity. The challenge of increasing the use of IT frameworks in healthcare is probably security concerns when systems are supposed to have health information (Ermakova et al., 2013). The system includes the information security component (Samad et al., 2017)(Raghuvanshi et al., 2021). Researchers in (Avizienis et al., 2004) mention common health care security concerns such as privacy, approval and honesty. Following are the main requirements to consider the security of an EHR system: 1.1 Confidentiality Confidentiality is one of the core tasks of the healthcare provider. The health data are confidential information that must be protected against unauthorized access (Bigini et al., 2020). The system gives the approved user access to the information and requires the creation of a trusted environment for the patient to seek healthcare. According to the 1997 HIPAA act, the patient's health information had to be protected (Shuaib, Alam, Shabbir Alam, et al., 2021a). 1.2 Integrity Keeping eHealth record integrity is important because it is used to locate patients and pursue them when moving from one provider to another. In order to decide the level of patient care, the integrity of information in medical services becomes essential. It delivers precise and unaltered health information throughout the life cycle. It maintains data accuracy, consistency and reliability (M U Bokhari & Alam, 2013). 1.3 Authorization The EHR system agrees to provide access to the record and to be recorded by physicians, thereby improving the process of medical recording for an authorized user (Shuaib, Alam, & Daud, 2021). The organizations of medical services are required to alleviate these risks and are responsible for authorization. It is important to mention the access control mechanisms to protect the privacy of the patient. The authorization process is limited to external users. The system needs to determine eHealth data access privileges and the user responsibilities. 1.4 Availability The availability is an

element that requires a framework to allow authorized users to open, use and access a record. It means that, if required by an approved user, the information is constantly accessible to customers. The system must ensure that health records are available by preventing interruption to service due to hardware failures, improvements to the framework and safeguard the availability of health records (Mohammad Ubaidullah Bokhari et al., 2014). The remaining part of this articles has been divided into three sections. Section 2 contains related work; section 3 contains blockchain description and advantages of using Blockchain in healthcare data security. Section 3 also contains a framework to secure healthcare data using Blockchain. Section 4 concludes the paper.

PROPOSED SYSTEM

The proposal is a multifaceted ABS system that can be applied to healthcare using blockchain technology. This model of EHR system has the subsequent four parts: an EHR server, N experts, patients and records verifiers. The EHR server resembles a distributed storage server, answerable for putting away and transmitting EHR. N Authorities are different associations, for example, emergency clinics, health care coverage associations, and clinical research foundations that are answerable for the transmission and move of patient data. Prognostics can be characterized when the information verifier permits patients to make, oversee, direct and sign their EHRs and access this mark and check its exactness.

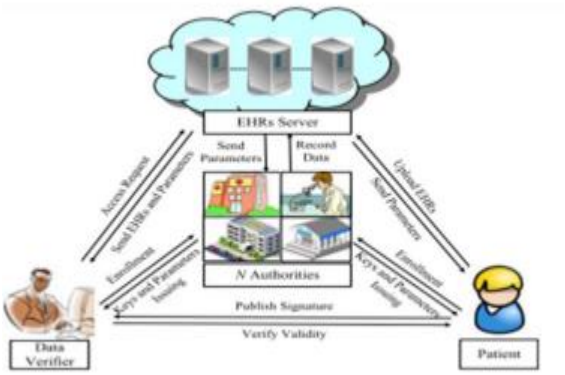


Figure 1. System Architecture

EHR SYSTEM PERFECT

This EHR framework model comprises of the accompanying four sections: an EHR server, N authority, patients and information verifiers. The EHR server resembles a distributed storage server, liable for putting away and transmitting the EHR. N The specialists are answerable for the enlistment and move of patient data by different associations, for example, clinics, health care coverage associations and clinical research foundations. Patients can make, oversee, regulate, sign and characterize their EHR and the information verifier has the ability to get to and confirm these marks.

BLOCKCHAIN

To preserve patient confidentiality in an EHR scheme on blockchain, more authorities are presented in ABS and the ABS system is proposed, which complies with the requirements of the blockchain structure and guarantees anonymity and information without changes. PRF seeds are wanted between authorities, patients' private keys must be made, corrupt N-1 authorities cannot succeed in collective attacks.

SECURE TRANSPORTING

The welfares of blockchain skill include decentralized upkeep, data backup in the blockchain structure, secure transportation and access to data, as well as undisputable security against data falsification. One of the distinctive features above is that the blockchain allows you to take advantage of an EHR system and manage the authentication, confidentiality, responsibility and sharing of data during the transmission of information relating to privacy. It also provides medical resources for the patient and improves people's health care.

ATTRIBUTE AUTHORITIES

Alice acquires these qualities from various attribute authorities who do not trust or know each other. In some cases, some of the allocation authorities may suffer damage. In this case, this should not prevent you from obtaining attributes from further hornet authorities. Alice is authorized to accept your message based on the previous complaint, without revealing how the complaint responds to the complaint. Authorities jointly claim Alice's signature on identity-based signature system.

HARDWARE REQUIREMENTS

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB

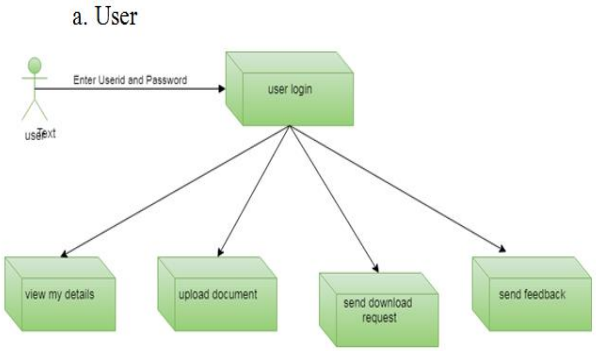
SOTWARE REQUIREMENTS

Operating System	: Windows 8
Front End	: Java/DOTNET
Database	:Mysql/HEIDISQL

LITERATURE SURVEY

The patient's health information is generated and encrypted by the patient's public key (Shen et al., 2018). Based on unique information such as an e-mail address, etc., the public key is created. The patient now wishes to access the medical record, then authenticates the private key linked with the public key. This key is used only for a specific health record (Benet et al., 2018). The authorized key issuer creates a public key and the user's private key. An access structure over attributes is linked with every private key. Doctors enable the decryption of data by private key; they should also comply with the access policy during the decryption process. A monotonic access structure like AS, OR, Etc. is kept in the attribute-based encryption process (Qian et al., 2015). Techniques for attribute-based encryption policy permit non-monotonic access systems. The health record is encrypted and linked to a number of attributes, which are each private key linked to the attributes access structure. The physician attempts to access the encrypted record of health. It is only acceptable if the ciphertext has qualities and the access structure associated with a private key is satisfied (Shi et al., 2015). The downside is that the encrypter cannot determine who is able to decipher the data and that the data proprietor must also trust the key issuer. These problems have been overcome by encryption based on Ciphertext attributes. The fine-grained encryption technology is used to encrypt the health record and preserve the access policies of each health record. In ciphertext, a user's private key is associated with the set of characteristics, and ciphertext has to do with attribute-base access policies (Jiang et al., 2018). The doctor should decrypt this ciphertext, for example, a doctor or patient trying to access the health record, access if and only if the doctor's attribute fulfils the access policy for the ciphertext. Health records are encrypted and stored in the cloud by following these methods. It is the individual responsibility of the cloud servers to safeguard health information in the cloud. As the patient maintains confidential information in the cloud, it is important for the cloud service provider to keep the data secure and reliable (Shuaib, Alam, et al., 2020). Although patient data are performed with various encryption techniques and stored in the cloud. The one central node is the most important portion of the job in a centralized network (Alam et al., 2019) . However, eHealth data in the cloud is inadequate since the cloud has confidence in the third party and a single failure point (Abdus et al., 2018). Nodes are distributed to other nodes in a decentralized framework. The distributed framework provides a stable and highly usable system and a fault-tolerant mechanism that stops the issue of a single point of failure. Included in the cloud is the accuracy of the eHealth record and done with Blockchain (Tanwar et al., 2020).

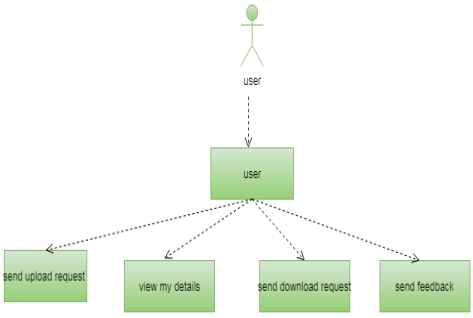
COMPONENT DIAGRAM:



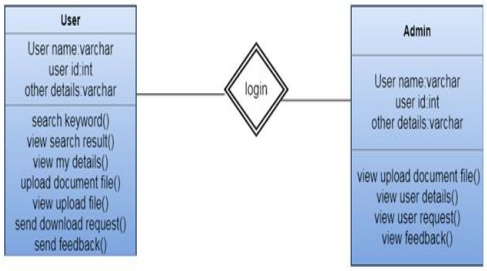
ISSN: 2040-0748 Vol-10 Issue-01 JAN 2021

USE CASE DIAGRAM:

a. User

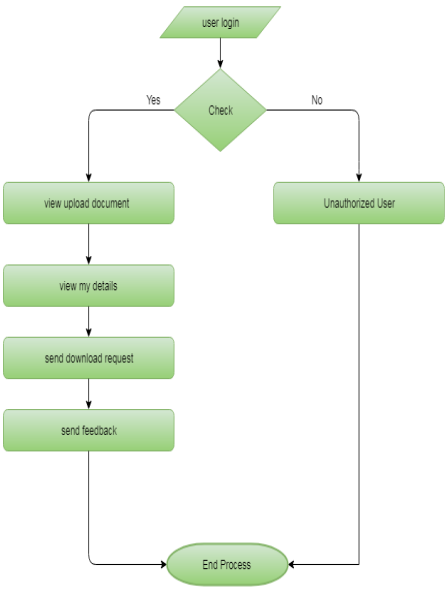


CLASS DIAGRAM:



DATA FLOW DIAGRAM

a. User



UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.

2. Provide extendibility and specialization mechanisms to extend the core concepts.

3. Be independent of particular programming languages and development process.

4. Provide a formal basis for understanding the modeling language.

5. Encourage the growth of OO tools market.

6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

7. Integrate best practices.

ISSN: 2040-0748 Vol-10 Issue-01 JAN 2021

INTRODUCTION TO PYTHON FRAMEWORK

Introduction to Django This book is about Django, a Web development framework that saves you time and makes Web development a joy. Using Django, you can build and maintain high-quality Web applications with minimal fuss. At its best, Web development is an exciting, creative act; at its worst, it can be a repetitive, frustrating nuisance. Django lets you focus on the fun stuff — the crux of your Web application — while easing the pain of the repetitive bits. In doing so, it provides high-level abstractions of common Web development patterns, shortcuts for frequent programming tasks, and clear conventions for how to solve problems. At the same time, Django tries to stay out of your way, letting you work outside the scope of the framework as needed. The goal of this book is to make you a Django expert. The focus is twofold. First, we explain, in depth, what Django does and how to build Web applications with it. Second, we discuss higher-level concepts where appropriate, answering the question "How can I apply these tools effectively in my own projects?" By reading this book, you'll learn the skills needed to develop powerful Web sites quickly, with code that is clean and easy to maintain.

What Is a Web Framework?

Django is a prominent member of a new generation of Web frameworks. So what exactly does that term mean? To answer that question, let's consider the design of a Web application written using the Common Gateway Interface (CGI) standard, a popular way to write Web applications circa 1998. In those days, when you wrote a CGI application, you did everything yourself — the equivalent of baking a cake from scratch. For example, here's a simple CGI script, written in Python, that displays the ten most recently published books from a database:

```
import MySQLdb

print "Content-Type: text/html"
print
print "<html><head><title>Books</title></head>"
print "<body>"
print "<h1>Books</h1>"
print "<ul>"

connection = MySQLdb.connect(user='me', passwd='letmein', db='my_db')
cursor = connection.cursor()
cursor.execute("SELECT name FROM books ORDER BY pub_date DESC LIMIT 10")
for row in cursor.fetchall():
    print "<li>%s</li>" % row[0]

print "</ul>"
print "</body></html>"

connection.close()
```

This code is straightforward. First, it prints a "Content-Type" line, followed by a blank line, as required by CGI. It prints some introductory HTML, connects to a database and executes a query that retrieves the latest ten books. Looping over those books, it generates an HTML unordered list. Finally, it prints the closing HTML and closes the database connection. With a one-off dynamic page such as this one, the write-it-from-scratch approach isn't necessarily bad. For one thing, this code is simple to comprehend — even a novice developer can read these 16 lines of Python and understand all it does, from start to finish. There's nothing else to learn; no other code to read. It's also simple to deploy: just save this code in a file called latestbooks.cgi, upload that file to a Web server, and visit that page with a browser. But as a Web application grows beyond the trivial, this approach breaks down, and you face a number of problems:

Should a developer really have to worry about printing the "Content-Type" line and remembering to close the database connection? This sort of boilerplate reduces programmer productivity and introduces opportunities for mistakes. These setup- and teardown-related tasks would best be handled by some common infrastructure.

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTING UNIT TESTING:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific

business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

FUNCTIONAL TEST

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted. Invalid Input : identified classes of invalid input must be rejected. Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

SYSTEM TEST

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

WHITE BOX TESTING

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

CONCLUSION

The proposed theoretical blockchain-based framework highlights the concepts and techniques used and referenced for developing a blockchain-based reliable medical ecosystem and defines how complicated medical processes can be streamlined. We propose an innovative approach to medical record management through smart contracts that provide auditability, interoperability, and accessibility. In health data management, we have suggested potential uses of blockchain technology. We have adopted a data management and sharing system based on medical needs. It is possible to ensure that access to EHR data is guaranteed through blockchain technology, privacy, security, availability and refined control. The ultimate aim of strengthening health procedures and patient records is to introduce Blockchain using smart contracts to simplify processes, minimize administrative burdens, and eliminate intermediaries. Blockchain may further strengthen patients' control over their personal data and support researchers in data collection, processing, and sharing health data reliably and securely while maintaining anonymity.

REFERENCES

1. Abdus, S., Shadab, A., Mohammed, S., & Mohammad.Ubaidullah, B. (2018). Internet of Vehicles (IoV) Global Development, March, 4037–4040.

2. Shuaib, M., Alam, S., Mohd, S., & Ahmad, S. (2020). Blockchain-Based Initiatives in Social Security Sector. EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD), 8.

3. Alam, S., Shuaib, M., & Samad, A. (2019). A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing. In Lecture Notes in Networks and Systems (Vol. 55, pp. 231– 240).https://doi.org/10.1007/978-981-13-2324-9_23

4. Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–33.

5. Arunkarthikeyan, K., Balamurugan, K., Nithya, M. and Jayanthiladevi, A., 2019, December. Study on Deep Cryogenic Treated-Tempered WC-CO insert in turning of AISI 1040 steel. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 660-663). IEEE.

6. Arunkarthikeyan K., Balamurugan K. & Rao P.M.V (2020) Studies on cryogenically treated WC-Co insert at different soaking conditions, Materials and Manufacturing Processes, 35:5, 545-555, DOI: 10.1080/10426914.2020.1726945

7. Balamurugan, K., 2020. Compressive Property Examination on Poly Lactic Acid-Copper Composite Filament in Fused Deposition Model–A Green Manufacturing Process. Journal of Green Engineering, 10, pp.843-852.

8. Balamurugan, K., Uthayakumar, M., Ramakrishna, M. and Pillai, U.T.S., 2020. Air jet Erosion studies on mg/SiC composite. Silicon, 12(2), pp.413-423.

9. Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. ArXiv Preprint ArXiv:1407.3561.

10. Benet, J., Dolin, R. H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F. M., Biron, P. V, Shabo, , Jiang, S., Cao, Wu, H., Yang, Y., Ma, M., He, J., Shi, Y., Zheng, Q., Liu, J., Han, Z., Qian, H., … Zarnekow, R. (2018). A secure data sharing using identity-based encryption scheme for e-healthcare system. 2018 Ieee International Conference on Smart Computing (Smartcomp), 14(1), 221–231

11. Bigini, G., Freschi, V., & Lattanzi, E. (2020). A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. In Future Internet (Vol. 12, Issue 12, pp. 1–16). MDPI AG. https://doi.org/10.3390/fi12120208

12. Bigini, G., Freschi, V., & Lattanzi, E. (2020). A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. In Future Internet (Vol. 12, Issue 12, pp. 1–16). MDPI AG. https://doi.org/10.3390/fi12120208

13. Bokhari, M U, & Alam, S. (2013). BSF-128: a new synchronous stream cipher design. 14. Proceeding ofInternational Conference on Emerging Trends in Engineering and Technology, 541–545.

14. Bokhari, Mohammad Ubaidullah, Alam, S., & Hasan, S. H. (2014). A Detailed Analysis of Grain family of Stream Ciphers. International Journal of Computer Network & Information Security, 6(6).