International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 01-06

Blockchain Based Cloud Smart Healthcare System with Dual Assses Control Framework

MRS .PRIYADARSHINI.S
(ASSITANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE)
MADHUBALA R
SIVASHANKAR M
YESHWANTH C
(STUDENTS, DEPARTMENT OF COMPUTER SCIENCE)

ABSTRACT
The concept of Blockchain has penetrated a wide range of scientific areas, and its use is considered to rise exponentially in the near future. Executing short scripts of predefined code called smart contracts on Blockchain can eliminate the need of intermediaries and can also raise the multitude of execution of contracts. In recent years Blockchain has also shown optimum reliability in multiple sectors such as Smart Home, Healthcare, Banking, Information Storage Management, Security and etc. This work in terms is further concerned to the sector of Smart Healthcare, which has grown to a much affluence regarding the efficient technique of serving and dictating medical health care to the patients. An access control framework based on smart contract, which is built on the top of distributed ledger (blockchain), to secure the sharing of EMRs among different entities involved in the smart healthcare system. For this, we propose four forms of smart contracts for user verification, access authorization, misbehaviour detection, and access revocation respectively. Also Dual Access control framework is proposed to get permission from the corresponding patient and the hospital.

Date of Submission: 07-05-2022 Date of acceptance: 22-05-2022

I. INTRODUCTION

Access control

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. At a high level, access control is a selective restriction of access to data. It consists of two main components: authentication and authorization, says Daniel Crowley, head of research for IBM’s X-Force Red, which focuses on data security. Authentication is a technique used to verify that someone is who they claim to be. Authentication isn’t sufficient by itself to protect data, Crowley notes. What’s needed is an additional layer, authorization, which determines whether a user should be allowed to access the data or make the transaction they’re attempting. Without authentication and authorization, there is no data security, Crowley says. “In every data breach, access controls are among the first policies investigated,” notes Ted Wagner, CISO at SAP National Security Services, Inc. “Whether it be the inadvertent exposure of sensitive data improperly secured by an end user or the Equifax breach, where sensitive data was exposed through a public-facing web server operating with a software vulnerability, access controls are a key component. When not properly implemented or maintained, the result can be catastrophic.”

Types of access control

Organizations must determine the appropriate access control model to adopt based on the type and sensitivity of data they’re processing, says Wagner. Older access models include discretionary access control (DAC) and mandatory access control (MAC), role based access control (RBAC) is the most common model today, and the most recent model is known as attribute based access control (ABAC).

Discretionary access control (DAC)

With DAC models, the data owner decides on access. DAC is a means of assigning access rights based on rules that users specify.

Mandatory access control (MAC)

MAC was developed using a nondiscretionary model, in which people are granted access based on an information clearance. MAC is a policy in which access rights are assigned based on regulations from a central authority.

Role Based Access Control (RBAC)

RBAC grants access based on a user's role and implements key security principles, such as "least privilege" and "separation of privilege." Thus, someone attempting to access information can only access data that's deemed necessary for their role.

Attribute Based Access Control (ABAC)

In ABAC, each resource and user is assigned a series of attributes, Wagner explains. "In this dynamic method, a comparative assessment of the user's attributes, including time of day, position and location, are used to make a decision on access to a resource." It's imperative for organizations to decide which model is most appropriate for them based on data sensitivity and operational requirements for data access. In particular, organizations that process personally identifiable information (PII) or other sensitive information types, including Health Insurance Portability and Accountability Act (HIPAA) or Controlled Unclassified Information (CUI) data, must make access control a core capability in their security architecture, Wagner advises.

Smart Contracts

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are track able and irreversible. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. While blockchain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency.

Smart Contracts Work

Smart contracts were first proposed in 1994 by Nick Szabo, an American computer scientist who invented a virtual currency called "Bit Gold" in 1998, fully 10 years before the invention of bitcoin. In fact, Szabo is often rumored to be the real Satoshi Nakamoto, the anonymous inventor of bitcoin, which he has denied. Szabo defined smart contracts as computerized transaction protocols that execute terms of a contract. He wanted to extend the functionality of electronic transaction methods, such as POS (point of sale), to the digital realm.

In his paper, Szabo also proposed the execution of a contract for synthetic assets, such as derivatives and bonds. Szabo wrote: "These new securities are formed by combining securities (such as bonds) and derivatives (options and futures) in a wide variety of ways. Very complex term structures for payments can now be built into standardized contracts and traded with low transaction costs, due to computerized analysis of these complex term structures."

Cloud Storage

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with "anytime, anywhere" data access.

Cloud Storage Work

Cloud storage is purchased from a third party cloud vendor who owns and operates data storage capacity and delivers it over the Internet in a pay-as-you-go model. These cloud storage vendors manage capacity, security and durability to make data accessible to your applications all around the world. Applications access cloud storage through traditional storage protocols or directly via an API. Many vendors offer complementary services designed to help collect, manage, secure and analyze data at massive scale.

II. MODULES

The modules are:

- Health Care Framework Development
- Secure EMR Upload
- Smart Contract Based Access Control Framework
- Dual Access Control EMR Retrieval

Health Care Framework Development

- Hospitals: Hospitals in our scheme mainly include government or private hospitals that generate and share medical data among themselves.
- Patients: Patients are a vital part of our scheme. The access control mechanism is designed to make them the real owners of their data.
- Cloud Server: Cloud server is responsible for authenticating an entity's credentials.

Secure EMR Upload

- The encrypted EMR file gets uploaded in the cloud while the corresponding reference hash and the index number is stored in the blockchain.
- The patient and hospitals are given a access control for the data. These are stored in the blockchain.

Smart Contract Based Access Control Framework

- For data to be shared and received by any hospital, the patient and the sender hospital have to access control for that health data, this is called as Dual Access Control.
- Both have to access key to the receiver hospital, they can access the health data by providing the two keys from patient and hospital.

Dual Access Control EMR Retrieval

- For data to be shared and received by any hospital, the patient and the sender hospital have to access control for that health data, this is called as Dual Access Control.
- Both have to access key to the receiver hospital, they can access the health data by providing the two keys from patient and hospital.

III. SYSTEM TESTING

Unit Testing

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases. Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

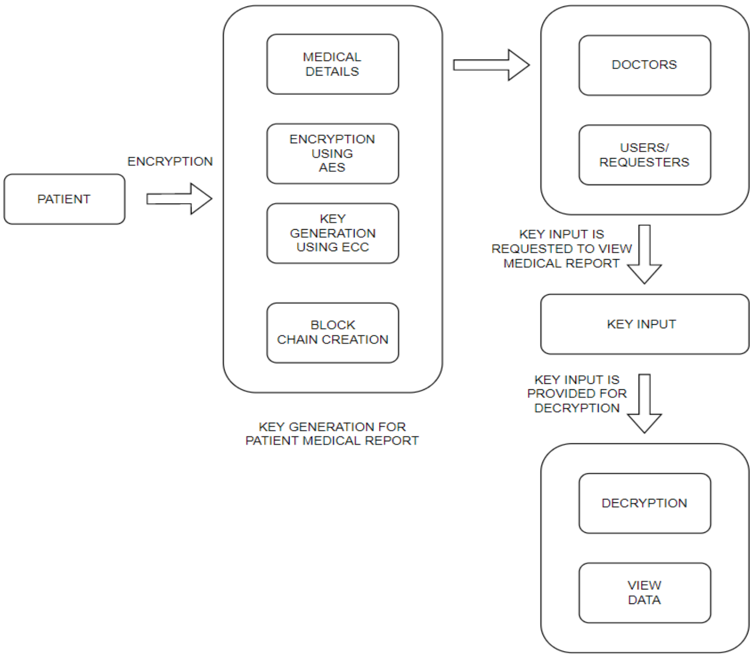
Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Testing

Test Case ID :01
Title: Android Home Screen
Test Steps: Run the project
Expected Results: The project to be executed and the android home screen is to be displayed.
Final Result: The project has been executed and the android home screen has displayed.
Test Case ID :02

Title: Project Home Screen
Test Steps: Run the project or Click the icon of the project.
Expected Results: The project to be executed and the project splash screen is to be displayed. Then the screen will disappear after some milliseconds.
Final Result: The project has been executed and the android home screen has displayed. Then the screen disappears after some milliseconds.
Test Case ID :03
Title: Login Form Activity
Test Steps: Enter username and password. Then click the Sign in button. To register click the sign up button.
Expected Results: The username must not be empty and the password must not be empty. The sign in button navigates the user to Main Activity Screen. The sign up button navigates the user to Signup activity screen.
Final Result: The username must not be empty and the password must not be empty. The sign in button navigates the user to Main Activity Screen. The sign up button navigates the user to Signup activity screen.
Test Case ID :04
Title: Main Activity
Test Steps: Click the view friends button
Expected Results: The View friends button navigates the user to FriendList Screen.
Final Result: The View friends button navigates the user to FriendList Screen.
Test Case ID :05
Title: Sign Up Activity
Test Steps: Enter the required fields.
Expected Results: The required fields must not be empty. The email id should be in correct format. The mobile number must not exceed 10 in length.
Final Result: The required fields must not be empty. The email id should be in correct format. The mobile number must not exceed 10 in length.
Test Case ID :06
Title: Friends List Activity
Test Steps: Click any one of the friends listed.
Expected Results: The page navigates to the message activity. The list of friends will be viewed correctly.
Final Result: The page navigates to the message activity. The list of friends will be viewed correctly.
Test Case ID :07
Title: Message Activity
Test Steps: Enter the message in textbox and click the send button.
Expected Results: The message will be send without any interrupt. The textbox must not to be empty.
Final Result: The message will be send without any interrupt. The textbox must not to be empty.

IV. SYSTEM FLOW



V. CONCLUSION

The World present day has moved on to the verge where global connectivity and synchronization is the primary thing that everyone is looking. Also, the present scenario of people around the world has shown a change in terms of the lifestyle and a busy schedule so, it has always been observed that people tend to neglect minor abnormalities with regard to the health.

An access control framework based on smart contract, which is built on the top of distributed ledger (blockchain), to secure the sharing of EMRs among different entities involved in the smart healthcare system. For this, we propose four forms of smart contracts for user verification, access authorization, misbehaviour detection, and access revocation respectively. Also Dual Access control framework is proposed to get permission from the corresponding patient and the hospital. With much consideration to the Accuracy, Security, and authenticity of the data generated from the patients, there has always been a requirement that the data must be always governed in a proper way. Therefore, for access management and storage of the data to manage the transactions, we tend to propose the concept of blockchain which is a consortium of multiple stakeholders such as Hospital, Doctors, Pharmacy, Pathology, Imaging Centres, Medical Research Centres, and Insurance Companies. Therefore, such systems can be considered as a significant whole in uplifting the society with accurate and efficient healthcare.

REFERENCE

[1]. A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," Computer Networks, vol. 112, pp. 237–262, 2017.

[2]. N. Fatema and R. Brad, "Security requirements, counterattacks and projects in healthcare applications using wsns-a review," arXiv preprint arXiv:1406.1795, 2014.

[3]. J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, 2009.

[4]. L. J. Kish and E. J. Topol, "Unpatients-why patients should own their medical data," Nature biotechnology, vol. 33, no. 9, p. 921, 2015.

[5]. S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in internet-of-things: A survey," Journal of Network and Computer Applications, vol. 144, pp. 79–101, 2019.

[6]. S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," ACM Transactions on Information and System Security (TISSEC), vol. 3, no. 2, pp. 85–106, 2000.

[7]. R. S. Sandhu, "Role-based access control," in Advances in computers. Elsevier, 1998, vol. 46, pp. 237–286.

[8]. V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," Computer, vol. 48, no. 2, pp. 85–88, 2015.

[9]. R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE communications magazine, vol. 32, no. 9, pp. 40–48, 1994.

[10]. E. B. D. Hussein and V. Frey, "A community-driven access control approach in distributed iot environments," IEEE Communications Magazine, vol. 55, no. 3, pp. 146–153, 2017.

[11]. M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[12]. S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13]. "Blockchain momentum rallies healthcare," http://www.ibm.com/blogs/blockchain/2017/01/blockchain-momentum-rallies-healthcare/, [Online; accessed 06-January-2017].

[14]. J. Priisalu and R. Ottis, "Personal control of privacy and data: Estonian experience," Health and technology, vol. 7, no. 4, pp. 441–451, 2017.

[15]. "Introduction to ethereum," http://ethdocs.org/en/latest/introduction/index.html, [Online]

IX. BIOGRAPHY

Priyadarshini.S is currently working as Assistnant Professor in Hindusthan Institute of Technology.She received BE degree in Computer Science and Engineering from Avinashilingam University for Women, Coimbatore, India in 2011.She received ME degree in Software Engineering Anna University, Chennai from SNS College of Technology. She has around 5 years experience in teaching. Her interest were around Machine Learning, Artificial intelligence, Augmented Reality. She has published around 8 papers in various journals and 3 papers in various conference.

Madhubala R, Final year student in the Department of Computer Science at Hindusthan Institute of Technology.

Sivashankar M, Final year student in the Department of Computer Science at Hindusthan Institute of Technology.

Yeshwanth C, Final year student in the Department of Computer Science at Hindusthan Institute of Technology.