IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN-ENHANCED ELECTRONIC MEDICAL RECORDS FOR SECURE HEALTHCARE DATA MANAGEMENT

[1]K.Anbuthiruvarangan, [2]R. Kavi prasath, [3]S.Koogul, [4]S.Nirmal, [5]V.Vinothan
[1]Professor,Department of Computer science and Engineering
B.Tech,Students, Department of Computer Science and Engineering[2,3,4,5]
Sri Manakula Vinayagar Engineering College,Madagadipet,Puducherry,India-605107

Abstract : Electronic Medical Records systems play a vital role in the health care industry. It serves as an intermediatory between healthcare providers and patients. This paper presents an blockchain based Electronic Medical Record which enhances integrity, security, and efficiency of system, which stores the records of the patient and logs transactions data on the Ethereum blockchain, and additionally this system encrypts data with the XChaCha20 algorithm before it is stored in the Interplanetary File System IPFS which adds an additional layer of resilience and it also strengthens the system framework and security of the systems. And to enhance the performance and efficiency of storing in the network it includes an additional layer of level 2 rollups for improved scalability of the systems.

IndexTerms **– Decentralized,pow,pos,encryption,logs,IPFS.**

I.INTRODUCTION

The advanced growth of the information technology leads to the increase in the volume of the data, this leads to the increased pressure in handling those data, so mostly all the health care industries rely in the electronic medical record systems but due to limited amount of resources and other techniques for implementing the method, such as the traditional method of storing of these records in the cloud based systems, has many advantages such as lower maintenance of systems and also cost free and efficient systems and it also leads an way to disadvantages such as security, efficiency and scalability and other privacy concerns, by storing of huge amounts of patient data leads to loss of data without proper maintenance.

So, by implementing cloud based medical storage systems and methods, patients' data are prone to different types of cyberattacks and other types of insider threats. And it increases the lack of more advanced based methods and storage techniques for an efficient and effective method of management of systems, this also increases the risk of trust among the patients, in which these records are prone to malicious actors and insecurities among patients.

To address the above issues and the concerns. This system proposes an alternate method to store managed and to share data among public health providers and it effectively handles those data in an efficient and effective manner. The recent study suggests that the usage of asymmetric encryption and other attribute-based encryption systems leads the healthcare institutions to grant different levels for access to different users based on their roles or their working attributes and the advanced system. Which trusts that only the authorized parties have the rights and the data to share and handle data which leads to increased trust among patients.

Consider a case where a hospital needs to give access to and rights to those who are required and are necessary to access those services and data among various operations and this cannot be achieved in the traditional system of the symmetric key encryption. To address these issues, researches have explored an new advanced encryption method which offers an extensive control over the data and security of the data, for this they have used Asymmetric method for the above approach in which the private key remains more secure over the other parties and the public network in which the data remains secure even if it is shared over the untrusted network and source.

This methods of securing of data and techniques remains an key role among sharing of data and records over the untrusted network source as today the development of the technology and computers health care industry relays on the cloud based storage and techniques for sharing of data by addressing the issues and the drawbacks in those systems and also maintaining those issues with advanced technologies and also increase the risk of privacy and security of those systems can greatly increase the patients trust over these systems which results in the safety and the integrity of the data.

II. LITERATURE REVIEW

The growth of the information systems which results in the increased usage of cloud-based storage systems and compute for managing data and records which results in the data breaches and other privacy concerns in the systems. An recent report suggests that the usage of online based computer systems results in the insecurity of the data and privacy concerns and the lack of data security and trust among the systems, which results in the need of the advanced technology and other methods for data security.
Encryption methods and techniques have been used for decades of time and it is considered as one of the safest method for transaction of data and information from any source and to any other advanced systems the usage of the traditional method for data security and privacy which results in the various drawbacks and in various data resource limits which results in the trust and the insecurity among the data and methods and the recent publications and news suggest that over more than eighty percent of the resources and the data is insecure design systems and architecture systems. A study by Lee (2022) has found that the usage of the asymmetric encryption systems in the healthcare system has been a greater advantage by minimizing the risk of the key sharing and they also have found that the increase computation resources as the records have been in an larger amount.

Attribute-Based Encryption (ABE) methods have emerged as an solution for implementing in the healthcare industry and also it used for defining the access policies of the users role and also used for the sensitive data transfer methods and also used for secure method of data transfer without the risk of losing the integrity of the data and also it aims to foundations of the information security systems and methods by usage of the CIA triad of the systems without exposing the information of the patients and records as it covers the HIPPA AND GDPR, which plays an important role in the protection suite of the systems.

Another important role in the research which integrates the study of the hybrid approach model in which the usage of both the symmetric and asymmetric encryption model for exchanging of sensitive information in digital systems.

This ensures that this model plays a key role in the effective management of the systems, and they play an essential role in the security of the systems for authentication and the system efficiency and their linear approach for continuous deployment and systems.

I. EXISTING SYSTEM

The system aims to enhance the security and privacy of cloud-based Electronic Medical Records (EMRs) by including the advanced encryption methods, including symmetric encryption, and asymmetric encryption, and attribute-based encryption (ABE). This method enhances the security of the records and the model in which it has many limitations and such as scalability and other access control issues.

At the base model that is the traditional model in which it relies on the module such as the security features like firewall and it also ensures continuous monitoring and detection capabilities which ensures an efficient and an effective approach for secure transmission of data and ensures that the data remains unauthorized security features and access policy issues and other methods. granular access control, assigning decryption rights based on user attributes or roles, allowing for tailored and restricted data access. The above method has an access control system in which it uses an specific policies for an particular data and systems and this works for certain rules and functions and it also uses an encryption and an decryption mechanism function in which it uses an authorized key functions and also uses an monitored layered tracks for all the system actions that it functions in the above methods and also it ensures that it is free from other sources of data and methods as it is ensures that is free from the other source of data and it is regularly based on the government standards and also the it ensures various rules and facts such as HIPAA and GDPR

And this method and existing function delivers an insecure design architecture function in which all the records of the patients that have been based on the functional model and the architectural diagram and the functional methods and the unauthorized data access into the system which leads to reduced trust among the patients system and the existed system are vulnerable to various attacks such as insider threats, and other means attacks and functions, the proposed system that we have used have been an clear definition and they are used to reduce those limitations into the system and also reduce further attacks of the model and the system.

This proposed method that we have implemented into the function have been used to reduce those cyber-attacks by logging all the data that have been used into the system by analyzing the cyber threats and the attack surfaces by reducing the error which results in the legal risks into the system, and also it is developed in such an way and designed to make with an access rights and uses an advanced encryption standards which adds an extra layer of security into the system and also the storage module we have used is the IPFS server which is an interplanetary file server which serves as an intermediate server for storage and other means of security.

This proposed system offers an best approach in means of security, privacy concerns, and also it logs all the data into the Ethereum blockchain and for storage of the function it utilizes the IPFS server which acts as an system for storage server, and MetaMask plays an important role in the creating smart contracts for efficient storage of data into the blockchain network and also it effectively handles the log data into the blockchain which is an private blockchain for efficiency.

IV. ALGORITHM

In the proposed system, several advanced algorithms will be implemented to optimize functionality, accuracy, and adaptability. The primary algorithms are as follows:
Proof of Work algorithm is used which plays an important role in solving complex problems that are used to add blocks into the blockchain network, and it ensures security and transaction integrity into the blockchain system. Blockchain technology which

ensures that the record values are stored in an secure format and which it ensures that it is stored in an decentralized network of systems in which there is no central authority system which adds block to the blockchain and also plays an important role in ensuring the integrity of the data, while the validators are used to ensure the amount of work and the cryptography stake data ensures that the data in securing the integrity for the transactional data and the systems which ensures that the need for the central authorized nodes for the interactions between the systems are reduced amount and the participants.

Proof of Stake(Pos) Algorithm

This method which is the Proof of Stake is an alternate method which is integrated into the system which is alternated method to the Proof of Work system in which the block which is added into the blockchain network is ensures that the system is with the smart contract selection in which it reduces the energy consumption and by using the Ethereum transaction from the state of the PoW to the Pos which aims to improve scalability and also it aims to improve the environmental issues and the major drawbacks of the system by using this method over the traditional method of the system which results in the focuses on the sustainable blockchain network solutions.

Staking and Slashing Mechanism

In the Proof of Stake system in which the system involves an certain amount of cryptocurrency awards which involved in the participation of the blockchain network system, and these are selected and rewarded based on the stake and they are used of validating the blocks properly and effectively. The staking process is managed by the smart contract systems, which ensures that the system are held securely into the blockchain network and also it ensures that the additional involvement of the verification process for the transaction system which ensures that the integrity of the network and also encourages the decentralization of the transactions, any system which has an enough amount for the cryptocurrency can participate in the staking mechanism without the need for special hardware.

Scalability and Environmental Considerations

PoW has some of the drawback features such as the energy consumption and the lack of the reliability feature of the system which is reduced in the Pos and Pow. Which ensures the reduced emissions for the blockchain network system and in the other side of the Pos system where it ensures that the maximum throughput ensures an efficient system which is preferable and used for most of the systems which has high usability of the system and applications that require high transactional power and system. And system which includes Ethereum relies on the Pos system which ensures an efficient decentralized system of network, which ensures that the system network is prone to grow over time with effectively and efficiently of the system.

V. PROBLEM STATEMENT

The rapid growth of the technology in the health care industry which results in the more advanced and efficient usage of the medical record system which results in an improved patient care system and in decision making system. However, which also relays on the other side of the system such as the privacy and the security of the systems. The traditional system which is equipped with the cryptographic hash functions, but it lacks the encryption of the data, which is the major disadvantage and it also lacks the trust among the patients and the data remains vulnerable to breaches and also unauthorized access of the data This paper also uses the Ethereum blockchain technology and also uses the smart contracts for automation system , which ensures with the XChaCha20 encryption technology combined with the additional method of logging of transaction data in the blockchain network. This system ensures data privacy, security and automation of the system, this ensures that the trust among the patients and the healthcare providers remains constant.

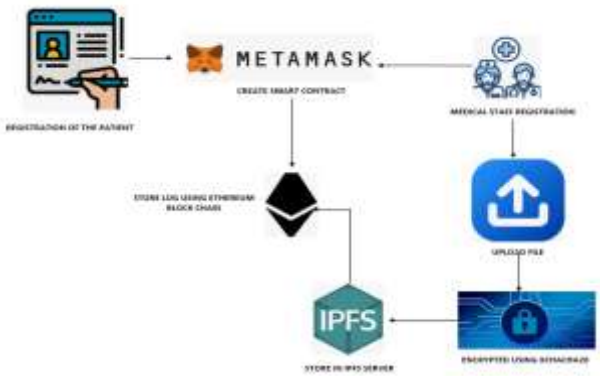
VI. PROPOSED SYSTEM

The above proposed system uses an Ethereum blockchain technology which addresses the privacy and the security concerns of the system in the advanced system of the healthcare industry of the Electronic medical record systems. This system ensures that all the record details of the patient history and the data are securely logged onto the Ethereum blockchain technology, which ensures the integrity of the data and the tamper proof record of the data and also ensures the immutability of the data and the systems, this blockchain network serves as an ledger which allows only authorized access to the data and the records of the patients, and the system and it also ensures that the security of the data and the privacy concerns are enhanced and equipped and thus they cannot be easily altered and modified into the system which prevents unauthorized access into the system.

For encryption standards the system includes an advanced encryption standards system such as the Chacha algorithm system, which deals and also ensures that only the authorized users are able to access the data and it also ensures that the data are stored onto the Interplanetary File System, which is an decentralized storage technique which ensures an additional security and also it ensures that only the members who have access to the data have only permissions to encrypt and also decrypt the data and they are able to access those records into the system and the technique.

By these implementations and technique, the system ensures a secure and enhanced system for the authentication of the data and the methods which ensure that the data remains secure and secure exchanging of the information and the data in modern healthcare systems.

VII. ARCHITECTURE DIAGRAM OF THE PROJECT



Proposed system architecture diagram

VIII. CONCLUSION

In conclusion, The proposed system which offers an advanced and an secure and an immutable method for the privacy and the security of the electronic medical record systems, which includes an Ethereum blockchain technology, XChaCha20 encryption technology system and an IPFS server which is an decentralized way of storing of data and medical records and also it ensures an enhanced way of securing data and privacy concerns of the patient record system, and also by logging of all the data into the blockchain technology system which ensures that only the ledger is allowed to access to those data and the security of the system and it ensures that the trust among the patient and the healthcare providers are managed and only the providers are authorized the records, which ensures that this system reduces the modern challenges in the healthcare industry.

REFERENCES

[1] Gaofan Lin, Haijiang Wang , Jian Wan , Lei Zhang, Jie Huang A blockchain-based fine-grained data sharing scheme for e-healthcare system.

[2] hamza javed, zainab abaid, shahid akbar, kifayatullah, Blockchain-based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems 2023.

[3] hazilah mad kaidi, mohd azri mohd izhar , rudzidatul akmam dziyauddin A Comprehensive Review on Wireless Healthcare Monitoring: System Components 2023.

[4] abdullahalmamun, sami azam, and clementine gritti,Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction.

[5] Samad Rashid & Arash NematiHuman-centered IoT-based health monitoring in the Healthcare 5.0 era: literature descriptive analysis and future research guidelines.

[6] Vonteru Srikanth Reddy, Kumar Debasis Statistical Review of Health Monitoring Models for Real-Time Hospital Scenarios.

[7] Kegomoditswe Boikanyo, Adamu Murtala Zungeru Remote patient monitoring systems: Applications, architecture, and challenges 2023.

[8] Basem Assiri A Modified and Effective Blockchain Model for E-Healthcare Systems 2023.

[9] Yazeed Yasin Ghadi, Tehseen Mazhar, Tariq Shahzad, Muhammad Amir khanThe role of blockchain to secure internet of medical things.

[10] Dhaneshwar Shah, Sunanda Rani, Khadija Shoukat Blockchain Factors in the Design of Smart-Media for E-Healthcare Management.

[11] HaoGuo,WanxinLi,MarkNejad,Chien-ChungShen**,**A Hybrid Blockchain-Edge Architecture for Electronic Health Records Management with Attribute-based Cryptographic Mechanisms (2023).

[12] PhongTran,ThongNguyen,LongChu,NhiTran,HangTa,*A* Solution for Commercializing, Decentralizing and Storing Electronic Medical Records by Integrating Proxy Re-Encryption, IPFS, and Blockchain (2024).

[13] AbayomiAgbeyangi,OlukayodeOki,ApheleleMgidi**,**Blockchain in Healthcare*:* Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital (2024).

[14] Md.AhsanHabib,KaziMd.RokibulAlam,YasuhikoMorimoto,A Secure Medical Record Sharing Scheme Based on Blockchain and Two-fold Encryption (2023).

[15] GaofanLin,HaijiangWang,JianWan,LeiZhang,JieHuang**,**A blockchain-based fine-grained data sharing scheme for e-healthcare system.

[16] HamzaJaved,ZainabAbaid,ShahidAkbar,KifayatUllahBlockchain-based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems (2023).

[17] HazilahMadKaidi,MohdAzriMohdIzhar,RudzidatulAkmamDziyauddin,A Comprehensive Review on Wireless Healthcare MonitoringSystem Components (2023).

[18]AbdullahAlMamun,SamiAzam,ClementineGrittiBlockchain-BasedElectronicHealthRecordsManagement,A Comprehensive Review and Future Research Direction.

[19] SamadRashid,ArashNemati*Human*-centered IoT-based health monitoring in the Healthcare 5.0 era*:* literature descriptive analysis and future research guidelines.

[20] VonteruSrikanthReddy,KumarDebasisStatistical Review of Health Monitoring Models for Real-Time Hospital Scenarios.