Journal of Research Administration
Society of Research Administrators International

OPTIMIZED ACCESS-CONTROL FRAMEWORK FOR REVITALIZING THE SECURITY OF PATIENT-CENTRIC ELECTRONIC HEALTH RECORDS

Dr.Pankaj Rahi*
*Associate Professor, Health Information Technology Management, Institute of Health Management & Research, Bangalore, Karnatka, India pankaj.rahi@outlook.com

Dr. Devesh Kumar Bandil
Professor, Deptt. of Computer Engineering, Poornima University, Jaipur, Rajasthan, India
devesh.bandil@poornima.edu.in

Dr. Savita Shiwani
Professor, Dept. of Computer Engineering, Poornima University, Jaipur, Rajasthan, India
savita.shiwani@poornima.edu.in

Pratibha Soni
Associate Professor, Dept of Computer Application
audipratibha@yahoo.com

Vivek Saxena
Director Infiqueaiservices Pvt Ltd, Jaipur, Rajasthan, India, viveksaxenads@gmail.com

***Corresponding Author:** Dr. Pankaj Rahi

*Associate Professor, Health Information Technology Management, Institute of Health Management & Research, Bangalore, Karnatka, India pankaj.rahi@outlook.com

Abstract.
Artificial intelligence is being rapidly incorporated into healthcare systems, but it is not a panacea for all problems. Challenges include a shortage of medicinal datasets for training AI simulations, adversarial assaults, and dearth of confidence owing to its black box operating style are holding back AI's tremendous potential. We looked at how blockchain technology may raise the dependability also credibility of AI-based medical systems. To examine the most recent research articles on healthcare applications created using various AI approaches and Blockchain Technology, this paper performed a systematic literature review. This systematic literature review examines three distinct pathways in healthcare systems that include the ones that utilize natural language processing, those that employ computer vision, and those that rely on acoustic AI. As a consequence, we have created an intangible framework for AI-based healthcare applications utilizing Blockchain Technology that takes into account the requirements of every Computer Vision, NLP, and Acoustic AI application using etherscan.In this chapter, a Patient based Access

Control Mechanism for a patient-centric e-Health System is presented to regulate the user resources. The proposed system establishes access control policies to automate the process of sharing health information across health service providers inside the e-Health system. The access control policies of the proposed system establish the access privileges and transfer permissions of the individuals involved in the Blockchain. The suggested method additionally enables data owners to revoke access, thereby restricting users' ability to view the data.

Keywords: Healthcare, Computer Vision, Blockchain, Natural Language Processing, Acoustic AI, Adversarial Attack, Etherscan, Access Control.

1 Introduction

Healthcare systems throughout the globe are under strain as a result of the SARS-CoV-2 virus, which sparked the worst pandemic in millennia. The pandemic has exposed weaknesses in even the most advanced healthcare systems, such as the difficulties in monitoring people with pre-existing conditions, apart from the acute concerns caused by the virus. Despite having stronger resources than other countries to combat the outbreak, over 1 million Americans died as a result of the virus in industrialized nations like the United States. This is because tackling a global calamity of this magnitude involves the dynamic deployment of resources to meet constantly changing care needs. The Institute of Medicine (IoM) estimates that over 100,000 persons each year in the US pass away as a result of avoidable medical mistakes [1]. The issue of how many fatalities may have been avoided comes when the Institute of Medicine's results from before Covid are taken into account, as well as the shocking number of deaths in the US. The healthcare industry includes information on the patients, their visits, their diagnoses, their medications, and their prescriptions[2]. Unfortunately, the tactics employed to neglect safety and internet security have become inseparable from innovation. Particularly in the medical care sector, prosperity records usually include private information including patient names, government-sponsored retirement numbers, and residences, making them a prime target for data theft[3]. The requirement for a plan and the vulnerability of security frameworks have led to the theft of EHRs swiftly becoming common and absurdly easy. Since EHRs are often handled by a single vendor, all personal data is kept in data sets that are under the control of the company in charge of the archive. It raises concerns about control, security, and protection that need to be resolved[4]. The Medical Health Record (MHR) contains a variety of paper notes that have been filled up throughout time by healthcare specialists, instructions for the efficient administration of medications and treatments, Test results,X-rays, and many other items. Initially, medical experts were in charge of organizing and maintaining medical health records. According to science, electronic health records are the patient data and information that are virtually preserved in a digital format[5]. These details might include anything from a patient's most basic allergies to their financial transactions at multiple healthcare facilities to the drugs and treatments they have received. The information from patients' electronic health records is being used by online storage providers to preserve different sorts of therapeutic data, which turn enables them to classify the sick patients. Schemes for maintaining

electronic health records (EHRs) are created in a way that ensures the accuracy and security of patient data. EHR records assist in reducing the possibility of losing a patient's medical history[6].

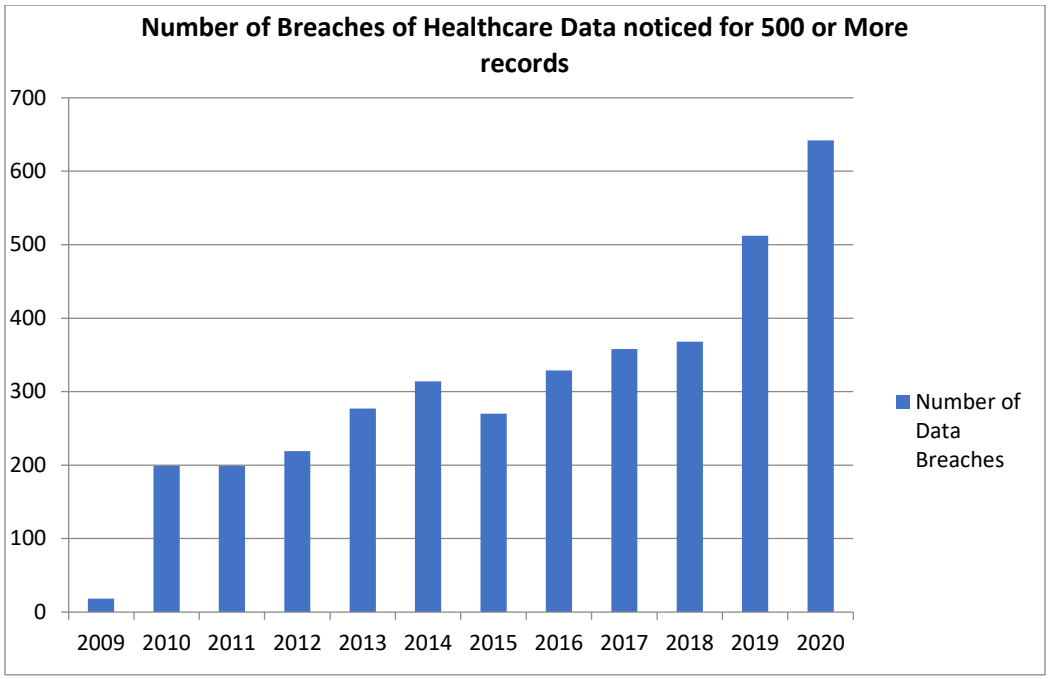

Fig. 1 Represenation of 500 or more healthcare data breaches are recorded between 2009 and 2020[7].

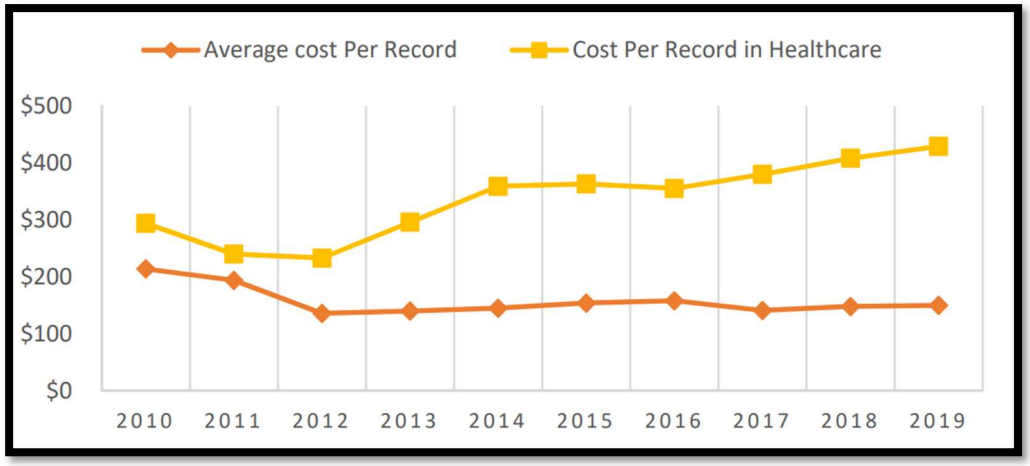

Fig. 2 Representation of Average Cost of Record and cost of Heallthcare Records from 2010 through 2019[8]

Fig. 1 shows the number of 500 or more healthcare data breaches from 2009 to 2020, whereas Fig. 2 presents a visual representation that compares the average costs of breached records and healthcare compromised records over the years. In the subsequent segment of this study, A periodic sequence investigation will be performed in order to determine the trend of healthcare data breaches and the corresponding costs they incur..

The key contributions of this paper are:

1. Proposed an efficient patient monitoring scheme using blockchain.
2. Acquaint readers with the recommended system design, which is followed by the suggested algorithms. All of the previously mentioned gaps are filled by the recommended architecture, including data extraction from handwritten prescriptions and connection with EHRs.

1.1 Applications of Blockchain Technology Outside of Healthcare:-

Blockchain technology has many potential applications in the business and medical sectors, and its widespread adoption would result in significant cost savings for introducing novel therapeutic approaches into clinical practise.

In recent years, blockchain technology's notoriety in the field of data security has grown substantially. The blockchain is a decentralized system designed to record and uphold transactional data. A blockchain is a digital ledger of blocks that contains a distributed, decentralised, and immutable record of transactions between peers. A blockchain is made up of two or more interconnected blocks of transactions.

There has never been a more pressing time for rapid technological advancement in the realms of public health and medical care. In today's world, people expect to have access to first-rate healthcare facilities that make use of state-of-the-art diagnostic and treatment tools. As such, blockchain technology would be an integral part of the healthcare sector's larger shift towards digitalization. Furthermore, the healthcare industry is reorganising itself to prioritise patient needs, with a focus on two key elements: accessibility of services and ready access to adequate healthcare resources.

The utilization of Blockchain technology enhances the capacity of healthcare organizations to deliver suitable patient care and uphold medical facilities of high quality.

Another labor-intensive and redundant procedure that adds to healthcare's astronomical price tag is the Health Information Exchange. Because of this technology, we can now address these concerns rapidly. By utilising Blockchain, citizens can take part in a variety of health research programmes. Better research and the sharing of data on the general population's health will also lead to more effective care for many different communities. The entire healthcare system, including all of its institutions, is administered by means of a single database [8-10]

2 Literature Review

R. Shaikh et al. [2022] explain the basics of blockchain technology. The aspects of cloud computing that provide security and transparency in conjunction with current solutions are also covered. The management system for patient health records is one of the applications that raise questions regarding cloud data storage. The security of a cloud service for patient electronic health records is explored, including the use of encryption and the sensitivity of data. Regarding the patient health record monitoring system that is kept in a cloud computing environment, the application features of blockchain are examined. The cloud is where the encrypted versions of the

electronic health records are kept. The degree of encryption is utilized following how sensitive the data is[9].

Y. Zhao and K. Du [2022] present a double-chains-parallelized asymmetric encryption (homomorphic encryption) and blockchain technology-based electronic health record matching scheme. In this dual-chain parallel system, the matching nodes are found in the EHR-demand chain while the sharing nodes are found in the EHR-supply chain. By using blockchain smart contracts, system can provide decentralization, secure and effective sharing, voluntary value exchange, and effective resource expansion for EHRs[10].

V. B, S. N. Dass, S. R, and R. Chinnaiyan[2021] examine the likelihood that medical records will be represented to offer data privacy, data accessibility, and data interoperability for the particular circumstances of healthcare. Data privacy refers to the security measures used to ensure that data is available when needed and is not accessed, used, transmitted, modified, or destroyed while being stored, retrieved, or conveyed. The ability to access data regardless of unanticipated or anticipated events, hardware, or other conditions is referred to as data accessibility. Every individual and organization must have the chance to strengthen privacy safeguards while ensuring that the healthcare sector has easier access to patient information[11].

M. M. Mahdy [2021] The planned system incorporates the distributed systems data storage framework into a centralized system Along with maintaining a ledger, it also blockchain, which permits security, patient pseudo-anonymity, the necessity of patient permission for EHR use, and ultimate uniformity of data across peers. The main concerns are patient data security and privacy; multiple hospital data breaches have resulted in the loss of patient EHRs. There have been several proposals to provide patients choice over their EHR data access, but there is currently no safe, private infrastructure that would for seamless EHR exchange[12].

O. Ajayi, M. Abouali, and T. Saadawi [2020] The suggested design is capable of detecting and stopping harmful activity on EHRs while they are in transit as well as at rest. Additionally, it presents them in a way that different healthcare nodes can easily understand while validating the accuracy and consistency of EHR requirements and responses from other healthcare systems. We compare the security examination against frequently observed external and internal risks within a healthcare system in early results. The outcome demonstrates that the architecture stops unauthorised access to patient data and identifies and stops insider threats from uploading compromising EHRs to the block chain[13].

A.Mukherji and N. Ganguli [2020] focuses on creating a safe, decentralised, and cost-effective environment for permissioned blockchain adoption in EHR administration. Our suggested design aims to increase the blockchain's capacity to scale when coupled with EHR to enable improved access to a patient's medical information. It has been a significant area of study and research in recent years since it has the potential to revolutionise several sectors. According to recent research[14].

M. Kassab et al. [2019] present the early findings of a collected works study on the use of blockchain technology to assist administration of EHR in health systems, along with the advantages and disadvantages. The implementation of a centralized system for electronic health

records, facilitating comprehensive access to a patient's complete medical history by several providers. An efficient answer to the aforementioned healthcare technology difficulties, blockchain might assist privacy enhancement, and insurance choices and transactions[15].
B. L. Radhakrishnan et al. [2019] outlines a tiered authentication-based defence strategy to defend blockchain from various threats. The patient's prescription information and medical history are included in electronic health records. The attackers are drawn to the medical records because they contain important information. A incorrect medicine or operation results from the loss of an electronic health record. Less security is offered by healthcare institutions to protect patient records. The use of blockchain in healthcare institutions safeguards patient data from hackers[16].

2.1 Research Trend

The 2020 analysis used the same process. Searches for SCIE and SSCI publications on the coronavirus that have been published since 2020 were conducted using the Web of Science core collection database. The language was set to English, and the exploration method was "TS = Corona-virus". Table 1 displays the publication's key facts.

Table 1. Main Evidence of the 2020 literature search of Smart EHR system.

Period	**2020 January to March**
Number of publications	684
Source journals	273
Author keywords	456
Avg. citations per document	3.24
Authors(having single authorized documents)	69
Authors(having Multiple authorized documents)	1955
Collaboration Index	6.5

A total of 384 publications have been published since the EHR system started to spread in late 2019. To research viral infection, epidemiological information is used. Both the Keyword Plus feature provided by Web of Science and the author keywords are utilized in the generation of a trend map for the analysis of patient monitoring research within the electronic health record (EHR) domain.

3 Problem Domain

Based on the findings of a scholarly study [17], the integration of blockchain technology within the healthcare sector has the potential to enhance the security of information by facilitating the processing and dissemination of healthcare data, all while upholding the principles of data privacy and security. This study [18] conducted a thorough analysis of the prevailing challenges now afflicting the healthcare sector. It focused on investigating the potential application of blockchain technology to augment the security, privacy, and interoperability of healthcare data. The present

study suggests some innovative blockchain presentations that are suitable for use within the healthcare sector. including blockchain cooperation, intelligent claim processing, and authorization based on smart contracts, as well as the integration of wearable fitness devices and health monitoring. The research [19], [20] focused on telemedicine, telehealth, and e-health while identifying aids of blockchain technology for healthcare as well as its prospects and limitations. The review [21] only covers facts. [22] solely on blockchain applications for electronic health records. We find a few issues with the earlier investigations, which may be summed up as follows:

• The existing research does not concentrate on blockchain for AI-enabled healthcare; previous training is mostly dedicated to EHR and certain particular specialized healthcare services, such as Telemedicine. Hence, the aforementioned study lacks comprehensive elaboration on the potential applications of blockchain technology in mitigating adversarial attacks [23].

The user's text does not provide any information to rewrite in an academic manner. Furthermore, the aforementioned studies did not investigate the utilization of blockchain technology to enhance the dependability of NLP, Computer Vision, and Acoustic AI in the context of accurate and automated healthcare services. While blockchain technology in healthcare has been the subject of previous studies [24], it is important to note that it is not the primary focus of this assessment. Nonetheless, this assessment distinguishes itself significantly from other research.

4. Proposed Work

The term "research methodology" pertains to the systematic approaches or strategies employed in the identification, selection, manipulation, and examination of data pertaining to a certain subject. To address the research issues focusing on the resilience of the healthcare system, the authors performed a literature analysis using the systematic analysis methodology. A data processing method called machine learning mechanizes the formation of analytical models. It is an area of AI that is concentrated on the idea that computers can learn from data, see patterns, and make judgments with little to no human input. To complete these tasks, verified data had to be obtained. After the classifiers were successfully trained, the model had to be deployed. Retraining and feedback loops for enhancing performance might then be implemented. Data is the most important part of artificial intelligence. Without data, no model can be developed, and all current technical advancements would be for nothing. It costs a lot of money just to get as much precise data as you can. The attack's data-targeting strategy has a significant effect on AI-based systems. By taking advantage of AI models' extraordinary sensitivity to slight changes in the i/p, which is known as poisoning and evasion attack, respectively, data may be negotiated during either training stage or the testing phase. These assaults may be promoted via spoofing [25]. It is a kind of cyberattack when a malicious party uses a computer, device, or network to pretend to be someone else to trick other computer networks. Malicious opponents typically do not have access to the model's training phase. To trick a classifier or avoid being detected by a neural network during testing, they provide hostile input. These assaults might be of the physical or digital kind. To maintain patient data securely and provide access, we suggest doing research into creation of a decentralized, peer-to-peer network of patients in which transactions are recorded on a shared distributed ledger. By

consensus, network participants would rule and decide how to update the ledger's records. Additionally, each record would have its cryptographic signature and timestamp.

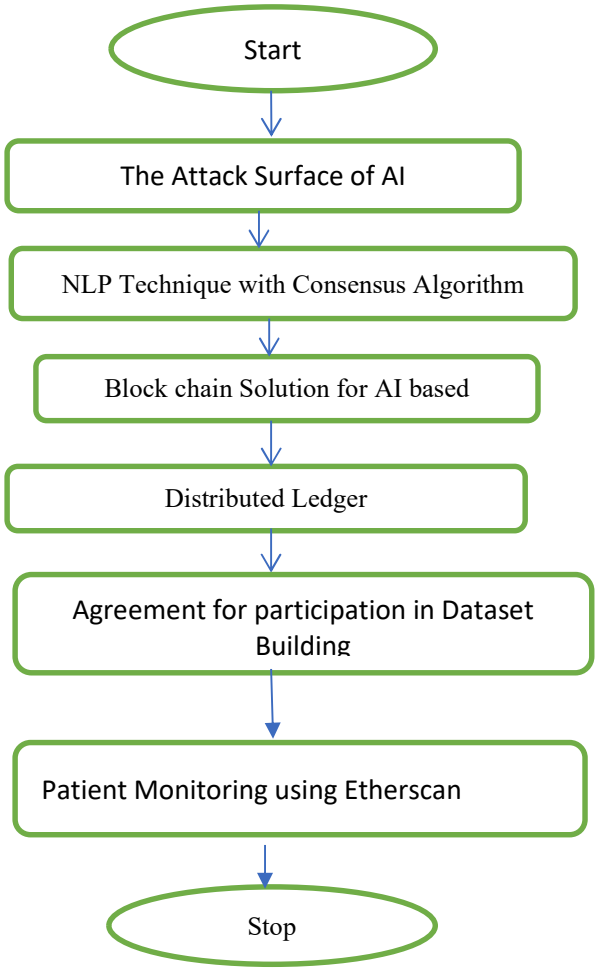

Fig. 3 Proposed Flow Chart

The Fig. 3 familiarizes oneself with the prescribed system design flowchart, which is thereafter accompanied by the proposed algorithms. The recommended design effectively addresses the aforementioned shortcomings, encompassing the extraction of data from handwritten prescriptions and establishing connectivity with Electronic Health Records (EHRs).

4.1 Proposed Algorithm

Step 1: Start

Step 2: User with input images

Step 3: The attack surface of AI using kali linux.

Step 4: Initial access to model

Step 5: Distributed Ledger (Post-Training Phase)

Step 6: Agreement for participation in Dataset Building.

Step 7: Medical acoustic data should be kept on local devices, and blockchain technology should be used to enforce federated learning.

Step 8: Asses Patient's Health record.

5. Result & Discussion.

The pandemic emphasizes the critical necessity for spending money and modernizing the healthcare system in order to efficiently store and monitor patient health data. If we go back over the preceding 50 years of computer technologies and architectures, we could see a pattern of fluctuation between subsequent decentralization and centralization of computing power, storage, infrastructure, protocols, and if we go back over the preceding 50 years of computer technologies and architectures, we could see a pattern of fluctuation between subsequent decentralization and centralization of computing power, storage, infrastructure, protocols, and code.

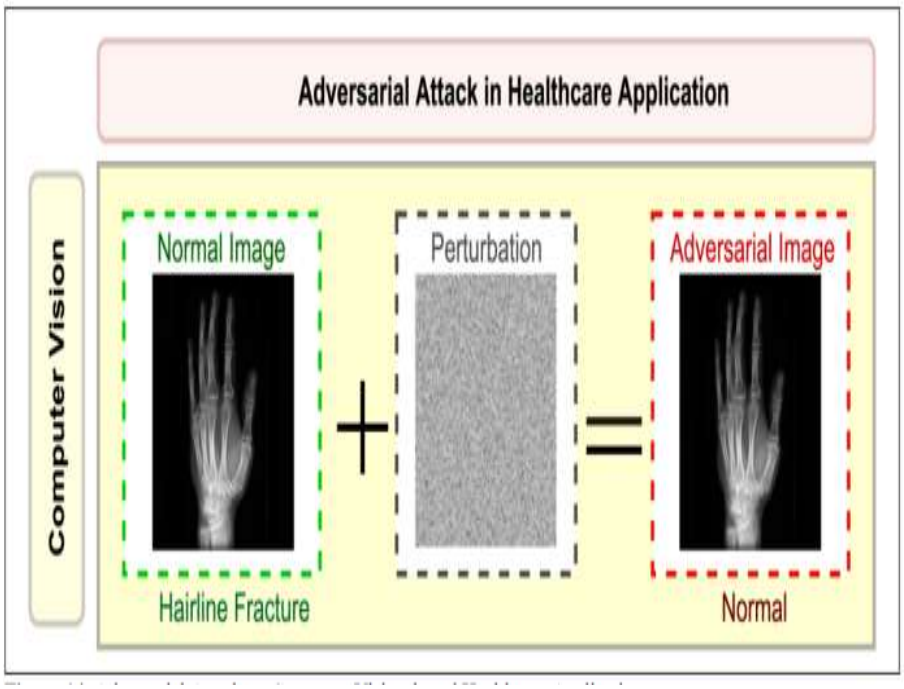

Fig. 4 Adversarial Attack on a Healthcare Application Based on Computer Vision.

Fig 4 illustrates the antagonistic result of introducing some disturbance to the initial hand X-ray picture. The perturbed picture is the same as the original image as seen by a human, but after

processing, the AI model interprets the output incorrectly. For instance, the adversarial strategy transforms the hairline fracture forecast into a typical fracture.

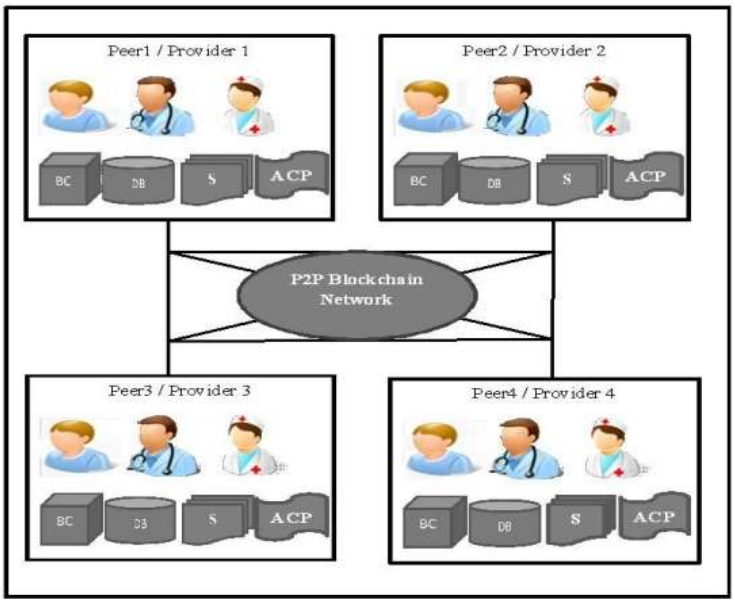

Fig. 5 Architecture of the Proposed Patient-based Access Control Mechanism

The Fig.5 suggested Patient-based Access Control Mechanism for an e-Health system built on a permissioned Blockchain network is detailed in this section's architecture. Figure 5 shows the design of the Patient-based Access Control Manager (PACM) that is suggested for the e-Health system.

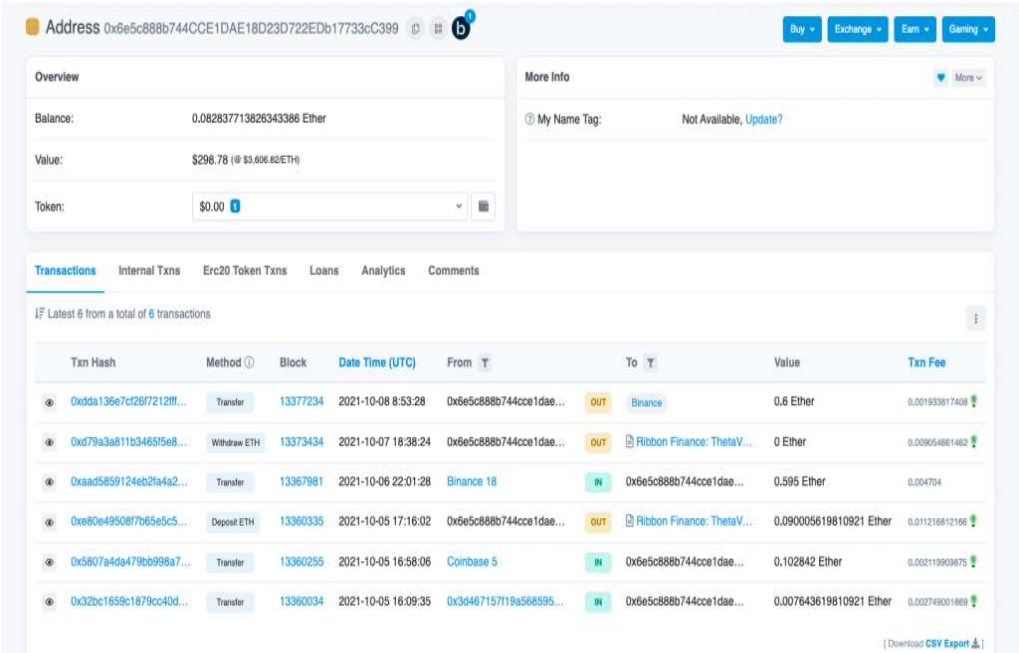

Fig 6 Kept data protected in Ethereum-Based Blockchain System.

Fig.6 represnets the application level view of data, protected in Ethereum-Based Blockchain System.The Ethereum is a publicly accessible blockchain platform that offers the capability to design and execute smart contracts, with a primary focus on the advancement of blockchain technology.

Researchers from many professions offered several plans for using blockchain technology to address the issue that exists in the healthcare industry.

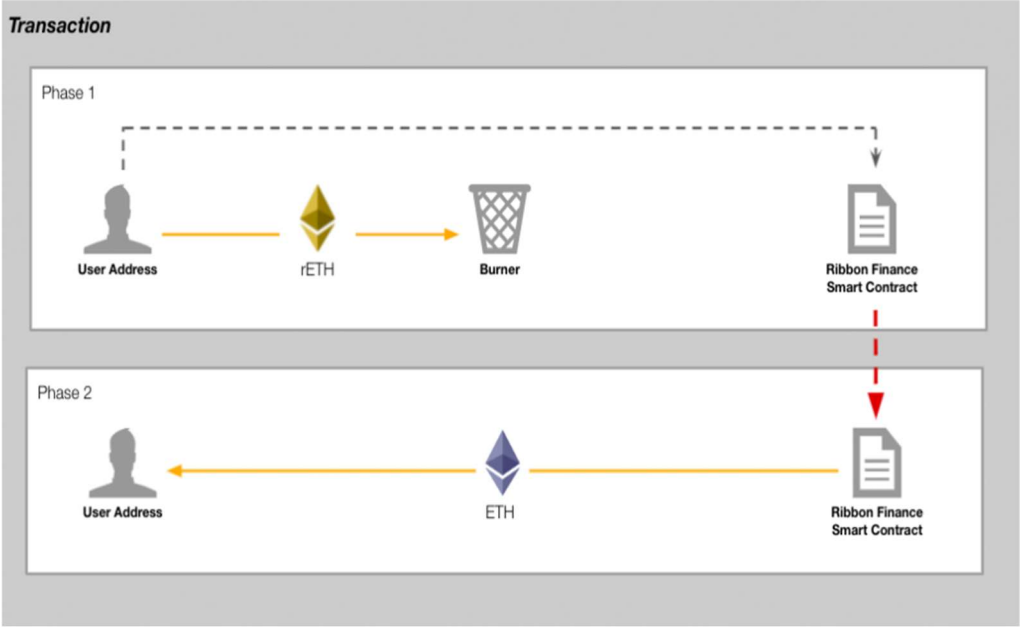

Fig. 7 Patient implementation using Etherscan

The Fig. 7 represnets the implementaion of Etherscan in Patients related transaction senarios. Etherscan, is accessible at https://etherscan.io/ and also functions as an Ethereum blockchain explorer, enabling users to conveniently view any transaction on the blockchain. Hence, through the process of crawling the Etherscan platform, we are able to acquire the necessary transaction records. Subsequently, an Ethereum transaction network is established, whereby each node represents an account and each edge denotes a transaction occurring between two accounts.

The demand for remote patient monitoring has grown and requirement is more than ever before, especially during pandemics when regular lifestyle is disturbed and people are predictable to remain at home.

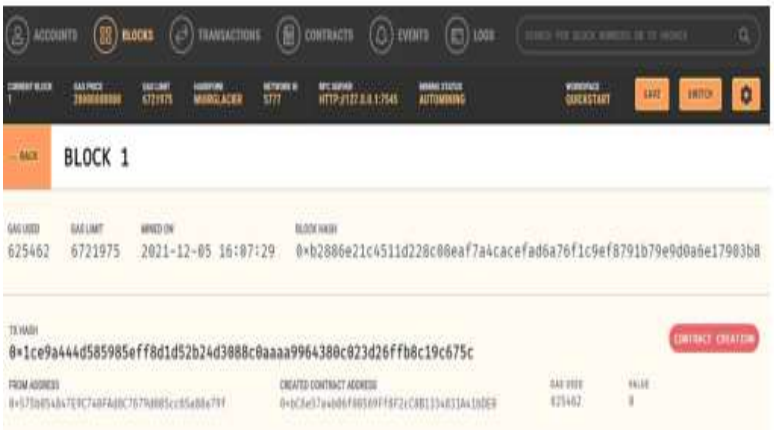

Fig. 8 Represenations of obtained results of Block 1

After showing one of the blocks, preferably Block 1, Fig. 8 is used showcase the results. We use the PoW method because, as was previously said, this system has an impact on both medical data and data privacy. The data simply has to be maintained and preserved for traceability and security on our blockchain, which is permissioned. For a small group of patients, the paper's minimalistic proposal for a method has been established.

Each patient has a private blockchain system that is accessible only to authorised medical personnel. A doctor may take part in many blockchain systems that correlate to the various patients that they treat in specific duration.

```
>>> e-Health_main.py
main under execution...
[['Grant_Access:Add_User', 'Revoke_Access: Remove_User', 'View_Users'],
['MineBlock'], ['ClientView'], ['done', 'quit']]

>>> adduser
Username: Patient1
Password: Patient1_123
UserType: dataowner

>>> adduser
Username: Patient2
Password: Patient2_123
UserType: dataowner

>>> adduser
Username: Patient3
Password: Patient3_123
UserType: dataowner

>>> adduser
Username: Pharma1
Password: Pharma1_123
UserType: stdr

>>> adduser
Username: MicroLab1
Password: MicroLab1_123
UserType: stdr
```

Fig.9 Results of Granting User Rights in the e-Health System

In the proposed health Blockchain, the granted users are now permitted to view the health asset. The proposed system executes granting access for e-Health users and the same is presented in Fig 9

Fig10. Results of e-Health System Users with Access Rights

The view user's method shows the list of users with their access rights. Based on the user permissions, the proposed system automatically generates the viewing access. The results of sample users created in the e-Health system and their details such as user ID, user name, and access rights are presented in Fig.10.

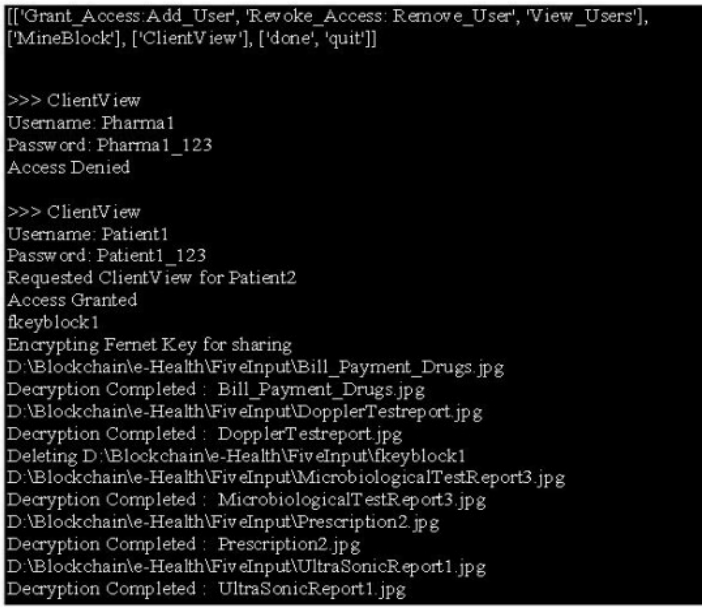

Fig. 11. Results of Granting and Denying Access Rights in the eHealth System

Since the user is a permissioned user with access rights, the user Patient1 is permitted to access the requested health information and hence the status provided to the user is “Access Granted”. The details of accessing the content and denying the access are presented in Fig. 11.

Fig.12. Results of Revoking Access with the Proposed System

The aboove Fig. 12 represents the Results of revoking rccess with the Proposed System

Challenges of blockchaın wıth AI

In this part of the article, we will talk about the challenges that have been experienced up to this point in the process of attempting to combine the technologies of AI and blockchain. In connection with the unification and integration of both technologies, the following is a list of some of the foreseeable difficulties that will arise:

• Protection of privacy is the ability to collect and analyse data is of paramount significance in the field of medicine. It is not appropriate for members of the general public to have easy access to this information. Although public blockchain ledgers make it possible to process data in a secure and authentic manner, the data that are collected in this manner are viewable by the general public and are made available to all readers. This is because the ledgers are open to the public. This is cause for concern as it poses a potential threat to the privacy of an individual. This situation is a matter of worry as it presents a possible risk to an individual's privacy. Furthermore, the extensive use of interconnected sensing systems within the framework of the Internet of Things (IoT) leads to the continuous aggregation of personal and sensitive data from individuals. The public dissemination of this data on openly accessible ledgers has the potential to elicit concerns over privacy. One potential strategy for safeguarding the confidentiality of information kept on private blockchains involves the utilization of encryption methods and the implementation of controlled access protocols for the ledgers maintained inside these blockchains. In contrast, private blockchain platforms may restrict the availability and transparency of vast amounts of data that are crucial for artificial intelligence (AI) to conduct thorough analysis and render exact conclusions. This phenomenon can be attributed to the design of these platforms, which is intended for the exclusive use of a restricted group of people.

• The capacity for scaling, in addition to having side chains. Scalability is one of the primary properties that can manage an increasing volume of work by adding resources to the models.

Scalability can be achieved through the use of parallel processing. Increasing the number of available resources is one way to achieve scalability. concerns regarding the platform that is currently known as the blockchain. When it comes to platforms for blockchain-based cryptocurrencies, the blockchain for bitcoin has the ability to perform an average of four transactions per second, while the blockchain for Ethereum has the ability to perform an average of twelve transactions per second. Such performance is simply inexcusable when compared to that of Facebook, which processes millions of transactions every second, including likes, posts, and comments. Increasing the speed of blockchains is accomplished through the utilisation of side chains, which are also referred to as side channels. In this implementation, transactions are settled between parties in a timely manner outside of the main chain, and they are settled on the main chain only once per day. Transactions are settled between parties in a timely manner outside of the main chain. There are two names for side chains: side channels and side chains. The algorithms for reaching consensus that are put to use by mining nodes have seen significant advancements thanks to the proliferation of new types of blockchains.

Platforms with the potential to deliver performance that is significantly superior to that of Ethereum and Hyperledger blockchains include Algorand and IoTA, for example. On the other hand, additional work needs to be done in order to improve the scalability so that it is on par with that of Facebook and other websites that operate in a similar manner.

• The reliability of blockchain technology. The potential for abuse and incorrect utilization of blockchain technology arises when its decentralized capacity is not employed judiciously. Although blockchain technology offers strong security measures for IoT and predictive analysis, it is important to acknowledge that blockchain systems are susceptible to cyberattacks, notably the 51% attack. The potential compromising of the consensus mechanism, which relies on the hashing power of the miner, is a plausible scenario. The consequence of this would be the transformation of the formerly decentralized platform into a centralized system, with a limited number of mining farms assuming control over both the finality of settlement and the consensus-building process. The susceptibility in cybersecurity is particularly conspicuous in public blockchains, exemplified by Ethereum and Bitcoin. The presence of pre-defined consensus mechanisms among the parties involved in private blockchain platforms mitigates the challenges associated with this issue. The susceptibility of execution outcomes to manipulation poses a significant challenge, particularly for private blockchain platforms such as Hyperledger. These platforms have a restricted number of mining nodes, which leads to a lack of protection in the execution environment of these nodes. The latest versions of blockchain platforms are equipped with the requisite hardware to enable execution under a Trusted Execution Environment (TEE), such as Intel SGX. The purpose of undertaking this endeavor is to ascertain a resolution to the aforementioned matter that was previously deliberated.

Deterministic execution and vulnerabilities are two prominent attributes harnessed by Smart Contracts, which are essentially a form of computer program. Ensuring the bug-free and secure implementation of a smart contract is of paramount significance, as it necessitates the ability to

withstand potential attacks. Ensuring the resilience of the smart contract against potential attacks is of paramount significance. Ensuring the security of both computer code and network-stored information is of paramount significance, as the compromise of either element could potentially endanger the other. An instance that exemplifies this is the smart contract utilized by the Decentralized Autonomous Organization (DAO), which was constructed on the Ethereum platform. This particular smart contract was found to possess a significant code weakness, leading to a successful hacking incident in 2016. Consequently, a substantial amount of 3.6 million Ethers was lost as a result of this breach. The occurrence can be attributed to the presence of a vulnerability within the code. This occurrence took place as a direct consequence of the security vulnerability included in the code. The necessity of blockchain engineering is evident in addressing the challenges associated with creating smart contracts and other applications operating on blockchain technology. The vulnerability vulnerabilities in the smart contracts might be attributed to the programming practices employed in languages such as Solidity and Chaincode, which were utilized for writing the code. These programming practices exhibit a lack of attention to detail and fail to meet acceptable standards. The assessment of smart contract source code for security vulnerabilities has become a matter of utmost significance, prompting the development of several tools for this purpose. The assessment of vulnerabilities in smart contracts has become a matter of utmost significance.

Furthermore, as present, the outcomes of smart contract executions are entirely deterministic and devoid of any probabilistic elements. There are several justifications for this assertion.This can present a significant challenge for decentralised AI, which is an approach to AI and machine learning in which algorithms for decision making are executed as smart contracts by mining nodes. In most cases, the results of these executions are not deterministic; rather, they are random, unpredictable, and approximate. Because of this, a creative solution is required to deal with approximate computation and to design consensus protocols for mining nodes. These protocols must enable mining nodes to agree on results with a specific degree of certainty, accuracy, or precision, despite the fact that the data input may be highly variable due to the Internet of Things (IoT) and sensory readings. In addition to this, this needs to be done with the help of data input, which should include readings from sensors and other devices that are linked to the internet.

Blockchaın strength wıth artıfıcıal ıntellıgence

In this section, we will discuss the difficulties that have been encountered to date when attempting to combine AI and blockchain technologies. The following is a list of some of the foreseeable difficulties that will arise in connection with the unification and integration of both technologies:

• Confidentiality. In the field of medicine, the importance of data cannot be overstated. This information should not be readily accessible to the public. Although public blockchain ledgers make it possible to process data in a secure and authentic manner, the data so collected are viewable by the general public and are made available to all readers. The aforementioned issue poses a possible threat to an individual's privacy and elicits a sense of apprehension. In addition, it is worth noting that pervasive sensing systems inside the Internet of Things (IoT) constantly

gather personal and sensitive data from individuals. The act of publicly disclosing this information on open ledgers may potentially lead to apprehensions regarding privacy. One strategy for safeguarding the privacy of data kept on private blockchains involves the implementation of encryption and the establishment of controlled access mechanisms for the ledgers. However, private blockchain networks may limit the accessibility and visibility of extensive data necessary for AI to effectively analyze and make appropriate decisions.

The capacity for scalability, together with the inclusion of side chains. Scalability is a fundamental characteristic that enables the effective handling of a growing workload through the addition of resources to the models. The attainment of scalability is possible through the addition of additional resources. There are now several worries around the blockchain platform. In terms of systems facilitating blockchain-based cryptocurrencies, the transaction processing capacity of the Bitcoin blockchain is estimated to be around four transactions per second, while the Ethereum blockchain exhibits a higher average of twelve transactions per second. In contrast to Facebook, a platform that handles a substantial volume of transactions on a continuous basis, encompassing behaviors such as likes, posts, and comments, the level of performance being discussed is deemed unacceptable. Side chains, alternatively referred to as side channels, are employed in order to enhance the efficiency of blockchains. In the present implementation, the settlement of transactions occurs promptly between involved parties outside the primary chain, and such settlements are only conducted once daily on the primary chain. Side chains, alternatively referred to as side channels, are an additional designation for this particular concept. The efficacy of consensus algorithms employed by mining nodes is greatly enhanced by the proliferation of novel blockchain variants.

Examples of platforms such as Algorand and IoTA has the capacity to exhibit significantly enhanced performance compared to Ethereum and Hyperledger blockchains. Nevertheless, further efforts are necessary to enhance the scalability of the platform, aiming to achieve a level comparable to that of Facebook and similar websites.

• An Examination of the Security Measures in the Blockchain Technology. The decentralized nature of blockchain technology renders it vulnerable to exploitation and misuse. Blockchain systems are vulnerable to cyberattacks, including the 51% attack. However, it is important to note that blockchain technology offers strong security measures for protecting Internet of Things (IoT) devices and facilitating predictive analysis. The potential compromise of the consensus mechanism, contingent upon the hashing power of miners, may lead to the centralization of a decentralized platform around a limited number of mining farms. These farms would then exert control over both the finality of settlement and the consensus-reaching process. The aforementioned security vulnerability is particularly conspicuous in public blockchains such as Ethereum and Bitcoin. The issue at hand is less prevalent on private blockchain systems due to the pre-established consensus mechanisms among the relevant parties. Furthermore, the absence of protection in the execution environment of mining nodes is a significant challenge, particularly for private blockchain platforms such as Hyperledger. These platforms operate with a restricted

number of mining nodes, thereby rendering the outcomes of executions vulnerable to potential manipulation. The recently developing blockchain systems are equipped with the requisite hardware to provide execution under a Trusted Execution Environment (TEE), such as Intel SGX. This action is undertaken in order to address and find a solution to the problem at hand.

The Smart Contracts platform is a computer application that integrates Deterministic Execution and vulnerability. Ensuring the absence of defects and vulnerabilities, as well as the resilience against potential assaults, is of paramount significance when deploying a smart contract. Ensuring the protection of both the code and the information kept on the network is of utmost importance, as they are susceptible to potential attacks. As an illustration, the smart contract utilized by the Decentralized Autonomous Organization (DAO), constructed on the Ethereum blockchain, experienced a significant code vulnerability leading to a security breach in 2016. This incident resulted in the misappropriation of around 3.6 million Ethers. The occurrence can be attributed to the presence of a vulnerability within the code. The necessity of blockchain engineering becomes evident in addressing the challenges associated with building smart contracts and other applications that operate on blockchain technology. The vulnerability vulnerabilities might be attributed to the programming practices employed in the languages utilized for writing code for smart contracts, such as Solidity and Chaincode. These programming practices exhibit negligence and inadequacy. The assessment of security vulnerabilities in smart contracts has become a matter of utmost significance, prompting the development of several methods aimed at evaluating the integrity of a smart contract's code.Furthermore, at present, the results of smart contract execution are entirely deterministic and devoid of any probabilistic elements.

The aforementioned scenario can provide a substantial hindrance to the implementation of decentralized artificial intelligence (AI). In this context, algorithms that utilize AI and machine learning for decision-making purposes are executed as smart contracts by mining nodes. The results of these executions are generally characterized by non-determinism, exhibiting randomness, unpredictability, and approximation. An novel approach is necessary to address the challenges of approximation computation and the development of consensus protocols for mining nodes. These protocols aim to achieve agreement on outputs with a specific level of certainty, accuracy, or precision. Furthermore, they must accommodate highly fluctuating data inputs, such as those from the Internet of Things (IoT) and sensory readings. Furthermore, it is imperative to perform this task by utilizing data input provided from sensors and internet-connected devices.

6. Conclusion & Future Scope

In order to evaluate the performance of the proposed system, a number of experiments are designed to assess the system performance. During the experimentation, it is observed that the proposed Patient based access control mechanism enables seamless and automatic access between the data owner and requester. Since the proposed system removes the trusted third party, the generation of grant access and grant transfer access rights could identify the authorized and privileged users. This paper's goal is to examine the work that has been done in blockchain for reliable AI-based healthcare. There isn't much literature in this field, as has been discovered.

Additionally, the authors of this study have included literature on acoustic AI in healthcare, computer vision, and natural language processing, among other categories. There is an undeniable consensus that the utilization of blockchain technology, particularly in conjunction with the etherscan platform, has become increasingly prevalent in various academic and professional domains. The diverse characteristics of blockchain technology collectively converge to substantiate a compelling assertion: it possesses the capacity to effectively reconcile the inherent conflict between data sharing and privacy, particularly within the realm of AI-driven healthcare. In this paper, a new Patient based Access Control Mechanism for permissioned e-Health Blockchain system has been designed and implemented to automate the sharing of digital resources. Since the permissioned Blockchain provides a transparent, immutable and tamperresistant environment, the transparency property fails to provide privacy to data owners. Hence an access control mechanism for enhancing the relationship between providers with an objective to provide efficient access between patients and other health participants via access control policies has been designed in this chapter. The proposed mechanism is implemented and evaluated in an EHR scenario. The results of the implementation prove that the patient based access control mechanism is more adequate for the automatic accessing of health information between the Blockchain participants of the e-Health system

7. Conflict-of-interest statement

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript and there is no financial interest to report.

Authors Contributions

Dr.Pankaj Rahi1, Dr. Devesh Kumar Bandil, and Dr. Savita Shiwani conceived of the presented idea and developed the theory and performed the computations.

Pratibha Soni and Vivek Saxena and drafted the manuscript and verified the analytical methods. Vivek Saxena encouraged Dr. Devesh Kumar Bandil, and Dr. Savita Shiwani for investigate result and also help in supervising the findings of this work. All authors discussed the results and contributed to the final manuscript.

8. Declarations

This is purely a scientific study and linked with the Blockchain- Information Communication Technology (ICT) concept and Digital Scientific devices used in Healthcare System so that Patients data transmission may happen in secure-way, it is beneficial in data-protection with optimum level of security-control. This study does not linked or modify the results of treatment processes, medication etc. used for treating patients, animals or other well-beings.

Consent to Participate: This study does not applies secondary analyses for de-identified data OR concept. Informed consent was obtained by all levels for the project.

Consent to Publish: Not Applicable

Funding

This research study is not funded by any organization. Hence no funding disclosure is required.

References

1. Mettler Matthias and HSG M.A., “Blockchain Technology in Healthcare The Revolution Starts Here,” 2016. doi: 10.1109/HealthCom.2016.7749510.
A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, Sep. 2016, pp. 25–30. doi: 10.1109/OBD.2016.11.
2. D. Roman and G. Stefano, “Towards a reference architecture for trusted data marketplaces: The credit scoring perspective,” in Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, Sep. 2016, pp. 95–101. doi: 10.1109/OBD.2016.21.
A. al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “MediBchain: A blockchain based privacy preserving platform for healthcare data,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, vol. 10658 LNCS, pp. 534–543. doi: 10.1007/978-3-319-72395-2_49.
3. Wehbe Youssef, Zaabi Mohamed Al, and Svetinovic Davor, “Blockchain AI Framework for Healthcare Records Management: Constrained Goal Model,” 2018 26th Telecommunications Forum (TELFOR), pp. 420–425, Oct. 2018, doi: 10.1109/TELFOR.2018.8611900.
4. Z. Shae and J. J. P. Tsai, “Transform blockchain into distributed parallel computing architecture for precision medicine,” in Proceedings - International Conference on Distributed Computing Systems, Jul. 2018, vol. 2018-July, pp. 1290–1299. doi: 10.1109/ICDCS.2018.00129.
5. P. Mamoshina et al., “Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare.,” Oncotarget, vol. 9, no. 5, pp. 5665– 5690, 2018, doi: https://doi.org/10.18632/oncotarget.22345.
6. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Healthcare Data Breaches: Insights and Implications. Healthcare 2020, 8, 133. https://doi.org/10.3390/healthcare8020133
7. R. Shaikh, "Blockchain Based Cloud Storage of Patients Health Records," 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 2022, pp. 1-5, doi: 10.1109/DELCON54057.2022.9753574.
8. Y. Zhao and K. Du, "A Matching Scheme from Supply and Demand Sides of Electronic Health Records Based on Blockchain," 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2022, pp. 1089-1092, doi: 10.1109/ICSP54964 .2022.9778725.
9. V. B, S. N. Dass, S. R and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402689.

10. M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2021, pp. 1-4, doi: 10.1109/ICCCEEE49695.2021.9429554.
11. O. Ajayi, M. Abouali and T. Saadawi, "Secured Inter-Healthcare Patient Health Records Exchange Architecture," 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2020, pp. 456-461, doi: 10.1109/Blockchain50366.2020.00066.

A. Mukherji and N. Ganguli, "Efficient and Scalable Electronic Health Record Management using Permissioned Blockchain Technology," 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2020, pp. 1-6, doi: 10.1109/IEMENTech51367.2020.9270106.

12. M. Kassab, J. DeFranco, T. Malas, V. V. Graciano Neto and G. Destefanis, "Blockchain: A Panacea for Electronic Health Records?," 2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH), Montreal, QC, Canada, 2019, pp. 21-24, doi: 10.1109/SEH.2019.00011.
13. B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 699-703, doi: 10.1109/ICACCS.2019.8728483.
14. Jo B.W., Khan R.M.A., and Lee Y.-S, “Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring,” Sensors 2018, vol. 18, no. 12, 2018, doi: https://doi.org/10.3390/s18124268.
15. S. A. Nusrat, J. Ferdous, S. B. Ajmat, A. Ali, and G. Sorwar, “Telemedicine System Design using Blockchain in Bangladesh,” 2019.
16. N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, “A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services,” Future Generation Computer Systems, vol. 100, pp. 569–578, Nov. 2019, doi: 10.1016 /j.future.2019.05.059.
17. “Blockchain-based Remote Patient Monitoring in Healthcare 4.0,” in 2019 IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 87–91. doi: 10.1109/I ACC48062.2019.8971593.
18. J. Passerat-Palmbach et al., “Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data,” in Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, Nov. 2020, pp. 550–555. doi: 10.1109/Block chain50366.2020.00080.
19. M. Shamim Hossain, G. Muhammad, and N. Guizani, “Explainable AI and mass surveillance systembased healthcare framework to combat COVID-I9 like pandemics,” IEEE Network, vol. 34, no. 4, pp. 126–132, Jul. 2020, doi: 10.1109/MNET.011.2000458.

20. F. F. Alruwaili, "Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records," PeerJ Computer Science, vol. 6, pp. 1–14, 2020, doi: 10.7717/PEERJ-CS.323.
21. V. B. Lobo, J. Analin, R. M. Laban, and S. S. More, "Convergence of Blockchain and Artificial Intelligence to Decentralize Healthcare Systems," in Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020, Mar. 2020, pp. 925–931. doi: 10.1109/ICCMC48092.2020.ICCMC-000171.
22. R. Gupta, U. Thakker, S. Tanwar, M. S. Obaidat, and K. F. Hsiao, "BITS: A Blockchain-driven Intelligent Scheme for Telesurgery System," Oct. 2020. doi: 10.1109/CITS49457.2020. 9232662.