Journal of Information Systems Engineering and Management
2025, 10(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Blockchain-Enabled Information Systems for Secure Health Management: A Case Study on Patient Data Privacy

Dr. Girish M Dhote[1], Dr. Jambi Ratna Raja Kumar[2], Neha P. Lanke[3], Dr. Parikshit N. Mahalle[4], Dipannita Mondal[5], Yatin Gandhi[6]

[1]*Assistant Professor, Department of Mechanical Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India. girishdhote@gmail.com*

[2]*Department of Computer Engineering, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, Maharashtra, India. ratnaraj.jambi@gmail.com*

[3]*School of Computer Science and Engineering, Ramdeobaba University (RBU), Nagpur, India. neha.lanke@gmail.com*

[4]*Vishwakarma Institute of Technology, Pune, Maharashtra, India. parikshit.mahalle@viit.ac.in*

[5]*Assistant Professor, Department of Artificial Intelligence and Data Science, Dr. D.Y. Patil College of Engineering and Innovation, Talegaon Dabhade, Maharashtra, India. mondal.dipannita26@gmail.com*

[6]*Competent Softwares, Pune, Maharashtra, India. gyatin33@gmail.com*

ARTICLE INFO

Received: 24 Oct 2024

Accepted: 12 Nov 2024

ABSTRACT

The integration of blockchain technology in healthcare has emerged as a promising solution for addressing the growing concerns of data privacy and security. This case study looks at how blockchain-enabled information systems (BEIS) can be used to handle patient health data, with a focus on making sure that personal medical data is kept private, correct, and easy to access. As telemedicine services grow and electronic health records (EHRs) become more common, the risk of data leaks and illegal access to patient information has grown. Traditional ways of protecting medical data, like centralized systems and security protocols, have trouble making it possible for healthcare providers to share data in a way that is clear and can't be changed. Blockchain is a strong answer to these problems because it is independent. By using smart contracts and cryptography, BEIS makes sure that records of patient information are safe, clear, and can't be changed. Only allowed parties can access these records in real time, which lowers the risk of data being changed or shared without permission. This case study looks at a blockchain-based patient data management system that was put in place in a regional healthcare network. It looks at how it protected privacy, made data easier to access, and made the system scalable. It also talks about the legal effects of using blockchain in healthcare, like how to get patients' permission and make sure that data security rules like GDPR and HIPAA are followed. The study's results show that blockchain has the potential to change the way healthcare data is managed. It could provide a safe and patient-centered way to keep personal health information safe while also encouraging healthcare systems to work together.

Keywords: Blockchain technology, Patient data privacy, Health data management, Electronic health records (EHRs), Smart contracts, Data security.

I. INTRODUCTION

Digital technologies are being used more and more in healthcare to handle and share patient data. This makes data protection and security a very important issue. As healthcare systems move toward telemedicine and electronic health records (EHRs), the amount of private medical data being created and kept online has grown by a huge amount. These improvements have made healthcare more accessible and more efficient, but they have also put the

field at great risk for data leaks, illegal access, and loss of patient privacy. Since of these issues, keeping understanding information secure has gotten to be exceptionally imperative for healthcare laborers, officials, and patients. Conventional ways of ensuring therapeutic information, like centralized information store frameworks, encryption, and get to controls, aren't working as well as they utilized to since online dangers are getting more complicated and far reaching [1]. Also, centralized frameworks are more likely to be hacked, have information changed, or be shared without authorization since they depend on a single point of control. With its independent, open, and unchangeable highlights, blockchain innovation appears guarantee as a way to unravel the issues of overseeing healthcare information. Blockchain can settle numerous of the issues with standard information store frameworks by making it conceivable to see therapeutic information securely and in genuine time whereas ensuring protection and security. Blockchain stores data in a worldwide log. Each occasion or piece of information is scrambled, time-stamped, and tied to records that came some time recently it. This makes it nearly inconceivable to alter information without being caught, giving an awfully secure setting for taking care of private persistent information. Moreover, shrewd contracts in blockchain make it conceivable for programmed and secure information sharing, making beyond any doubt that as it were permitted individuals or bunches can get to certain information. Since of these benefits, overseeing persistent data is more private and dependable. Blockchain is the culminate way to fathom the information security issues that are getting to be more of a issue within the healthcare industry.

A. Healthcare Data Management Challenges

As healthcare groups switch to digital methods for keeping and sharing patient data, they face a number of difficult data management issues. One of the main problems is the huge amount of data that different healthcare services produce, such as medical records, treatment reports, and data from real-time patient tracking. A big problem is keeping track of this huge amount of data quickly while also making sure it is accessible and correct. Centralized systems [2], which create a single point of failure, are often used in traditional ways to store data. Because the system is so centralized, it can be attacked online, have unwanted users access it, or have data stolen, which could put private patient data at risk. It's also hard for different healthcare systems and tools to work together, which makes things even more complicated. A lot of health care facilities have their own systems that don't easily talk to each other. This makes it hard for providers to share info easily with each other. The fact that patient records are spread out across multiple systems and that putting them all together can be hard makes care less efficient and limits the ability to get a full image of a patient's needs. Furthermore, problems with sharing correct and fast patient data to help with making decisions, especially in emergencies, make it clear that healthcare needs stronger, more open, and safer data management solutions right away.

B. Data Privacy and Security in Health Systems

Because patient information is naturally private and sensitive, data privacy and security are very important in healthcare. Personal information, health conditions, treatment experiences, and other private information must be kept safe in medical records so that patients and healthcare workers can continue to trust each other. Identity theft, financial scams, and damage to a person's image are just a few of the bad things that can happen when patient privacy is broken. Also, healthcare data leaks can lead to regulatory violations, big fines, and damage to the organizations' reputations. As electronic health records (EHRs) and other digital health tools become more common in healthcare, it is even more important to make sure that these data are kept private and correct. Telemedicine, mobile health apps, and smart tech are becoming more popular very quickly [3]. This has made patient data more vulnerable to hacking. Digital health systems are more difficult to secure because they are linked together, and each connection point opens up new security risks. The General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) make healthcare companies follow strict data protection rules. This makes strong security measures even more important. For high-quality, patient-centered care to continue, it is important to be able to protect patients' privacy while giving approved users smooth, real-time access to health information. Taking care of data security issues not only saves patients but also makes sure that digital health systems will be around for a long time.

C. Blockchain Technology and Secure Data Management

Blockchain innovation has gotten to be a better approach to bargain with protection and information security issues, particularly in areas like healthcare where genuineness and protection are exceptionally critical. At its core,

blockchain is an independent, conveyed log system that keeps track of occasions over numerous hubs in a arrange. This makes beyond any doubt that data can't be changed and is evident. The framework is exceptionally secure against scams and changes made without consent since each "square" within the chain contains a set of occasions or information passages.

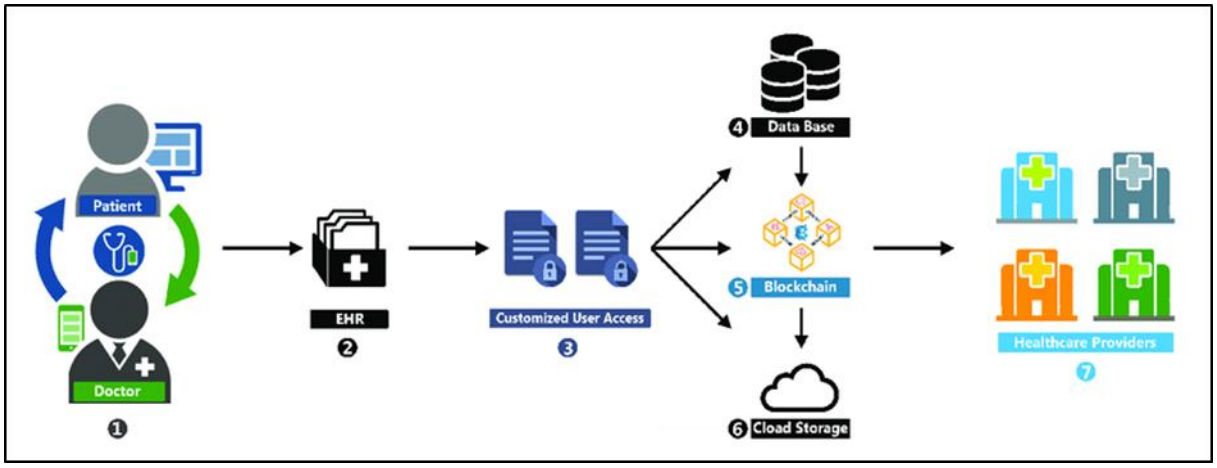

Figure 1: Overview of Healthcare used with blockchain

Once a piece is included to the chain, it can't be changed without changing all the pieces that come after it. Blockchain can offer assistance healthcare organizations superior handle their information by making a open, unchangeable record of quiet data that as it were permitted clients can see. This secures the protection and security of the data. Since blockchain is independent, it doesn't depend on a single specialist. This brings down the hazard of single focuses of disappointment and makes frameworks more safe to hacking. Blockchain's utilize of cryptography moreover makes it secure for healthcare suppliers to share information with each other, keeping private understanding information secure whereas it's being sent. Savvy contracts, which are agreements that consequently carry out conditions that have as of now been set, can robotize information get to consents, making beyond any doubt that as it were individuals who have the correct consents can see certain wellbeing information. It is exceptionally vital to ensure persistent protection with this work since it lets you fine-tune who can see or change patient data. Blockchain lets healthcare providers make frameworks that are safer, more open, and able to work with other systems. These systems can fathom many of the information protection and security issues that the industry is currently having. As shown in Figure 1, blockchain is used in healthcare systems to create a safe, open way to handle patient data. Key features are emphasized, including managing patient permission, storing data in a protected way, and giving people real-time access to medical information. The graph shows how blockchain protects data security, makes sharing safe and clear between healthcare providers, boosts privacy, lowers the risk of data breaches, and makes it easier for healthcare networks to work together.

This paper looks at how blockchain-enabled information systems (BEIS) might be able to help protect patient data in hospital management. The paper uses a case study to show how blockchain technology can be used to make health data management safer, more open, and more focused on the patient. The case study looks into how a blockchain-based patient data management system was put into use in a regional healthcare network and how it changed the privacy, security, and usability of data. The study also looks at the legal effects of using blockchain in healthcare, like making sure it follows data protection rules like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). As more healthcare groups switch to digital patient management tools, blockchain's ability to improve data protection and build trust between patients and healthcare workers is becoming a more important area of study and development. The goal of this study is to add to what is already known about how blockchain can change the way healthcare data is managed and protect the safety of private patient data.

II. BACKGROUND AND LITERATURE REVIEW

Electronic health records (EHRs), treatment reports, and test results are stored in centralized databases, which are the main way that health information systems work today. These systems are meant to make healthcare better, make work easier, and make it easier for healthcare workers to talk to each other. But they have some problems,

especially when it comes to data protection, connectivity, and patient privacy. One of the biggest problems with centralized systems is that they are easy to hack. Since all the data is kept in one database, if the system is hacked, a lot of private data becomes public, which is a serious privacy breach [3]. On top of that, these systems often use old software that might not be able to handle new security risks [4]. Interoperability is another problem because a lot of healthcare companies use different software systems that don't work well together to share data. It's hard for healthcare workers to view and update patient data in real time because of this lack of standards [5]. This makes it harder to coordinate care and make decisions. Concerns about patient agreement are also raised by centralizing patient data, since patients often don't have much say over who can see their information. This makes people worry about sharing data without permission [6]. As healthcare systems change and digital technologies change how patients are cared for, these problems show how we need safer, clearer, and more connected ways to fix the problems with old health information systems [7]. People who work for healthcare organizations often get their data stolen because the data they hold is private and valuable. If someone gets access to a patient's health record, they could steal their identity or commit fraud using the personal information that is in it, which includes medical histories, illnesses, treatment plans, and insurance information [8]. Cybercriminals are taking advantage of flaws in standard health information systems to cause more and more healthcare data breaches over the years. Millions of patient information have been leaked in different events in the healthcare industry, making it one of the worst for data leaks [9]. One main reason for these hacks is that most healthcare data systems are centralized, which leaves them open to hackers who want to steal large amounts of private data [10]. Human mistakes, like not keeping track of passwords properly or not teaching employees enough, can also cause data leaks or illegal access [11]. Concerns about privacy in healthcare go beyond hacking. Patients don't always know who can see their medical records or how they are shared, which raises ethical issues about data privacy [12]. It has been found that healthcare organizations sometimes share patient data with third parties without the patients' permission or without telling them enough about their data privacy rights [13]. Not only do these private leaks and worries hurt patients' trust, but they also cost healthcare workers money and time [14]. As healthcare systems become more digital, it is important to solve these issues by putting in place strong security measures and clear data management systems [15].

Blockchain technology has gotten a lot of attention because it could help healthcare with its problems with data safety and security. Blockchain is a distributed ledger technology at its core. It keeps track of events across a network of computers, or nodes, in a way that is open, unchangeable, and spread out [16]. Blockchain does not need a single point of control like standard controlled systems do. A "chain" of blocks, or pieces of data, is made by cryptographically connecting each block to the one before it. This structure makes it almost impossible to change or mess with any data on the blockchain without also changing all the blocks that come after it [17]. This gives the data a high level of security and reliability. One incredible thing around blockchain is that it isn't controlled by a single substance. There's less chance of a settled point of disappointment in a blockchain framework since no one individual or gather controls the complete arrange [18]. Since of this, the system is more grounded against hacking, since a breach at one point doesn't influence the total thing. Another thing that creates blockchain interesting is that it is open. The record keeps track of all occasions and information sections, and anybody with the proper consents can see them. This makes it simple to see who gotten to and changed the information [19]. Since each alter to the information is recorded and checked by everybody, this openness makes sure that individuals are responsible and builds believe among clients. In healthcare, this openness makes it conceivable for a secure, dependable record of understanding information that can be seen in genuine time by endorsed clients. This makes it less demanding for healthcare workers to share information [16]. Using cryptography also protects patient information and lets only allowed people view and change records safely [17]. Because it is decentralized, can't be changed, and open to everyone, blockchain technology is a strong answer to many of the problems that current healthcare data management systems have, especially when it comes to data privacy, security, and trust [18, 19].

Table 1: Summary of related work in Healthcare

Approach	Key Findings	Method	Application
Decentralized Data Storage [7]	Decentralization improves resilience against single-point failures.	Literature review, theoretical modeling	Medical records management in decentralized systems.
Blockchain and Smart Contracts [8]	Smart contracts automate data access and ensure patient consent is respected.	Experimental design, smart contract implementation	Patient consent management in EHR systems.
Blockchain-based Patient Authentication	Blockchain can provide tamper-proof patient authentication and access records securely [9].	Prototype development, security testing	Secure patient login for online healthcare portals.
Blockchain for Healthcare Interoperability [10]	Blockchain improves interoperability between different healthcare platforms.	Comparative analysis, simulation	Data exchange across various healthcare platforms.
Permissioned Blockchain in Healthcare [11]	Permissioned blockchains offer controlled access, improving privacy while ensuring transparency.	Development of a permissioned blockchain model	Access management in large healthcare institutions.
Blockchain for Drug Tracking [12]	Blockchain can enhance drug traceability and counteract counterfeiting in supply chains.	Blockchain implementation, system integration	Pharmaceutical supply chain monitoring.
Patient Data Privacy with Blockchain [18]	Blockchain ensures that patient data is immutable and only accessible by authorized individuals.	System analysis, cryptographic validation	Protecting patient privacy in EHR systems.
Blockchain in Telemedicine [19]	Blockchain helps ensure secure and transparent transmission of telemedicine data.	Survey analysis, system architecture design	Secure video consultation and patient record management.
Blockchain for Health Insurance [20]	Blockchain improves fraud detection and claims management in health insurance.	Case study, analytical modeling	Claims verification and fraud reduction in health insurance.
Blockchain for Regulatory Compliance [21]	Blockchain assists healthcare institutions in complying with GDPR and HIPAA data privacy regulations.	Legal and technical analysis	Ensuring compliance with healthcare data protection laws.
Blockchain for Real-Time Data Access [22]	Blockchain facilitates secure, real-time access to patient data for healthcare providers.	System design, performance testing	Emergency care systems accessing patient data securely.

III BLOCKCHAIN TECHNOLOGY AND HEALTHCARE

A. Detailed explanation of blockchain components

Blockchain technology ensures data integrity, security, and decentralization with numerous key components. Blockchain's blocks, chains, encryption, and consensus processes make it a good option for healthcare data management, especially for patient privacy, transparency, and trust. Blockchain blocks capture transactions and information. Each block has a timestamp, a list of data elements (such patient records or health events), and a link to the preceding block. The blocks form a data chain with each additional block securely attached to the end. A block becomes immutable once added to the blockchain, making it impossible to change prior entries without modifying the whole chain. This may help preserve patient data in healthcare. Once a patient's data is put to the blockchain, it cannot be changed, guaranteeing that healthcare professionals always have an accurate and verified medical history.

Blockchain technology also requires cryptography. It protects square information and exchanges. Blockchain employments hashing and public-private key encryption. A piece of information is hashed to supply a special identifier (or "hash"). The block's information decides this hash, therefore even a minor adjustment changes it. Healthcare information astuteness depends on this highlight, which denies unauthorized understanding record changes. In any case, public-private key encryption secures communication and information get to. As it were authorized clients with the private key may interpret and get to understanding data encrypted with a public key in healthcare. This methodology keeps touchy information private whereas empowering trusted parties like healthcare specialists to securely get to it. Agreement calculations confirm exchanges and ensure blockchain organize individuals concur on record state. Confirmation of Work (PoW) and Proof of Stake (PoS) are the overwhelming consensus procedures, be that as it may PBFT is additionally utilized. A agreement strategy is required in healthcare to guarantee blockchain information exactness and believe. The PoW process in a open blockchain framework powers clients to unravel complicated numerical issues some time recently including a piece, making blockchain altering computationally expensive. PoW is highly secure yet resource-intensive, hence healthcare applications may select PoS or other lightweight agreement strategies, which are more energy-efficient and secure.

B. Healthcare Data Management Benefits from Blockchain

Blockchain technology is great for healthcare data management since it solves many of the problems conventional systems encounter. These advantages stem from blockchain's decentralization, transparency, security, and immutability.

- Data Security and Privacy: One of the primary benefits of using blockchain in healthcare is enhanced data security. Blockchain protects patient data from unwanted access, alteration, and cyberattacks using powerful cryptography. Blockchain restricts healthcare record access to physicians and patients via public-private key encryption and hashing. This reduces data breaches, a major issue in healthcare, when hackers
- Transparency and Auditability: Blockchain records all transactions and makes them available to authorized users. This simplifies patient data and access record tracking, providing comprehensive traceability. Doctors may see who accessed a patient's information, what was changed, and when. Transparency builds confidence and responsibility among healthcare professionals and patients.
- Improved Interoperability: Blockchain allows healthcare organizations to securely share data across software platforms. Decentralized blockchain removes the need for a single authority to handle data, and standardized data formats allow diverse providers to access and exchange information smoothly. This enhances care coordination and provider efficiency across organizations, increasing patient outcomes.

Blockchain can streamline billing, patient identification verification, and data interchange, lowering healthcare administration expenses. Blockchain may reduce data management, fraud protection, and compliance expenses by automating procedures using smart contracts and minimizing data verification middlemen. Reusing these savings might enhance patient care.

B. Comparison with traditional centralized data storage systems

Blockchain technology differs from centralized data storage systems in security, control, and efficiency.

- Centralization vs. Decentralization:
  Hospitals and insurance companies hold all understanding records in a single database. Centralization may set up a single point of disappointment, making the framework more vulnerable to cyberattacks, data breaches, and blackouts. Blockchain's decentralized arrange disseminates information over a few hubs, bringing down the plausibility of a single point of disappointment. If one node fails, the others keep a copy of the information, guaranteeing framework progression and security.
- Information Integrity and Tamper Resistance:
  Centralized frameworks are more powerless to altering. Unauthorized get to to a central database might alter understanding data or expel crucial information. Blockchain records information changelessly. Data contributed to the blockchain cannot be changed without arrange understanding. This tamper-resistant include ensures persistent information and avoids therapeutic record extortion.
- Get to Control and Security:

Centralized information security depends on the central specialist. All persistent information may be jeopardized on the off chance that the central framework falls flat. Decentralized get to control utilizing cryptographic strategies like open and private keys makes blockchain more secure. Each exchange is cryptographically affirmed by many organize individuals, and as it were those with the proper keys may get to or alter information. This decentralized methodology decreases the threats of trusting one institution with sensitive information.

- Compatibility:
  Healthcare practitioners utilizing different frameworks may struggle to communicate understanding information due to the need of compatibility in conventional information capacity strategies. Need of consistency may cause care delays, mistakes, and wastefulness. Blockchain permits uniform information designs over frameworks, making it less complex for healthcare professionals to get to and trade persistent information over stages and companies. This improves care coordination and eliminates medical mistakes from lost or wrong information.

IV. CASE STUDY: IMPLEMENTATION OF BLOCKCHAIN IN PATIENT DATA MANAGEMENT

A. Description of the Healthcare Network Involved in the Case Study

This case study's healthcare network is a regional healthcare group made up of primary care doctors, hospitals, outpatient clinics, testing centers, and other healthcare providers in a big urban area. The network is meant to offer a range of care services, from regular doctor visits to emergency medical services, to a wide range of patients. In the past, the network used old-fashioned centralized electronic health record (EHR) systems, which had problems with data separation, security holes, and healthcare workers not being able to talk to each other easily. This led to wasteful things like doing the same tests twice, waiting too long for evaluations, and having trouble safely sharing patient information between different organizations. The network chose to look into putting in place a blockchain-enabled information system (BEIS) to deal with these problems. The main goals were to improve security, make patient data more private, and make it easier for data to flow freely across the network's many nodes. This case study looks at how blockchain was used to make sure that patient data was managed in a safe and open way. It also looks at how it was used to speed up the sharing of medical information between healthcare companies while still following data protection rules.

B. Detailed Process of Implementing a Blockchain-Enabled Information System (BEIS) for Patient Data Privacy

Before the blockchain-enabled information system (BEIS) was put into place, it was necessary to do a full needs assessment to find out what the main problems were with managing patient data in the hospital network. This meant looking at the security holes in the current EHR system, the fact that data isn't shared in real time, and the problems with managing patient permission. In this process, a permissioned blockchain was made so that healthcare labourers, clinics, and patients can be given distinctive levels of get to based on their occupations and agreement choices. One imperative portion of the BEIS was the utilize of savvy contracts to consequently and entirely execute persistent assent. This made beyond any doubt that understanding information might as it were be shared with permitted healthcare suppliers in line with rules that had as of now been set. The blockchain too made it conceivable to form changes to persistent data in genuine time, which got freed of the need to enter information by hand and cut down on the chance of botches. Each transaction or alter to the patient's record was too cryptographically marked and time-stamped. This made a record that can be checked to create beyond any doubt that everyone was capable and legitimate. A part of consideration was paid to making beyond any doubt that blockchain worked with the network's existing IT foundation which the framework might work with their current EHR tools and other healthcare apps. Healthcare specialists were moreover given full preparing on how to utilize the blockchain system as portion of the rollout.

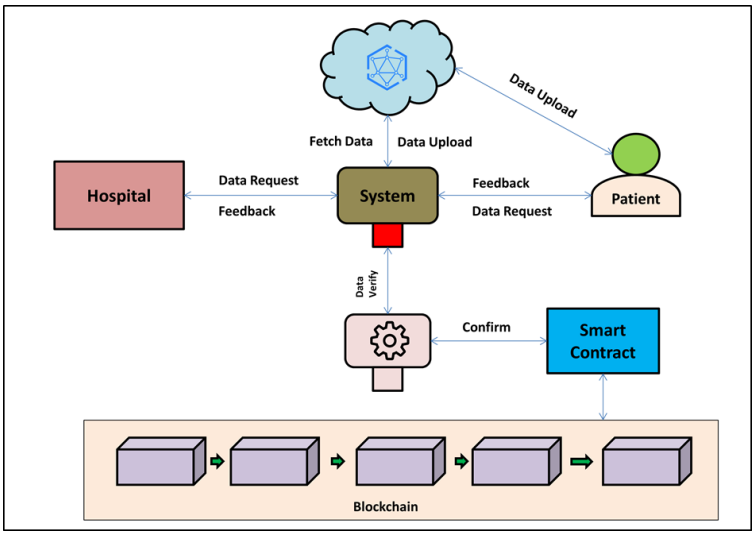

Figure 2: System Architecture of Blockchain-Enabled Information System (BEIS) for Patient Data Privacy

This made beyond any doubt that the system would be easily received which daily operations would be interrupted as small as conceivable. The Blockchain-Enabled Data Framework (BEIS) for patient data assurance is appeared in Figure 2 as a framework plan. The image appears an independent blockchain arrange that spares quiet information securely. Allowed clients, counting healthcare specialists, patients, and third parties, can get to the data. Smart contracts handle consents and get to, making beyond any doubt that information sharing is evident and can't be changed, all whereas remaining in line with privacy laws.

V. PATIENT DATA PRIVACY AND SECURITY IN BLOCKCHAIN SYSTEMS

A. Analysis of Privacy Features Enabled by Blockchain

Strong patient consent management is one of the most important privacy features that blockchain makes possible in healthcare systems. Blockchain makes it possible to record patient permission in a way that can't be changed. This gives patients full control over who can see their medical data. With blockchain, patient authorization can be followed along with the information transfer, with clear rules around what information can be shared, who can see it, and why. This consent is recorded within the blockchain log and can't be changed or messed with. This gives assurance and duty. Blockchain progresses get to control by letting healthcare workers set specific rights for clients. It moreover oversees understanding. Blockchain lets everybody within the framework whether they are a specialist, a nurture, or somebody from the exterior be given distinctive levels of get to to persistent information based on their work duties and requirements. Each get to ask and change is recorded on the blockchain, so get to rights can be changed based on what the understanding concurs to. This makes beyond any doubt that as it were permitted healthcare specialists can see private quiet data, and the blockchain's open record makes it easy to spot any attempt to get to the information without permission.

B. Mechanisms for Ensuring Data Confidentiality and Secure Sharing Across Healthcare Providers

To protect patient privacy in digital health frameworks, it is exceptionally vital to create beyond any doubt that information is kept private and shared securely between healthcare suppliers. Public-private key encryption is utilized to secure understanding data kept on the blockchain. This makes beyond any doubt that even if a square is stolen whereas being sent; it can't be read or seen without the proper interpreting keys. Besides, since blockchain is decentralized, persistent information is spread over numerous hubs. This stops dangers or single focuses of disappointment that may uncover the data's privacy. Permitted access makes it secure for healthcare professionals to urge to patient data when they need to. It carefully oversees each participant's get to rights. A worldwide record that's upgraded in genuine time in blockchain also lets healthcare specialists safely share data about patients. As a result, sharing information is secured and secure, and each trade of information is logged so that everybody can be held mindful. The independent record too lets numerous healthcare workers get to quiet information from diverse teach without stressing almost information duplication or errors. This makes care delivery faster and more accurate.

C. Role of Smart Contracts in Automating Data Access and Ensuring Compliance with Privacy Regulations

In healthcare frameworks that use blockchain, smart contracts are exceptionally important for computerizing information get to and making beyond any doubt that security rules are taken after. A keen contract is an understanding that takes after its own rules and automatically enforces conditions when certain conditions are met. Smart contracts are utilized in healthcare to streamline the method of getting patients' authorization to share data. This makes beyond any doubt that understanding information is only shared when the right conditions are met. For occurrence, in the event that a quiet concurs that their data can be shared with an master, the keen contract can permit that pro to see the suitable records for a certain amount of time. After that time, the access rights are taken absent. This gets rid of the need for human intervention and makes sure that sharing patient information is worn out a controlled and legitimate way. Savvy contracts can too offer assistance healthcare organizations follow security laws like HIPAA and GDPR by automatically applying information security measures. Some of these steps are making sure that only approved people can access patient data, that it is saved safely, and that the process of sharing data is clear and can be checked. Smart contracts also hold healthcare providers responsible because every transaction is recorded on the blockchain, which makes it possible to check who accessed and changed data. By streamlining these steps, smart contracts lower the administrative load and the chance of human mistake. This keeps patient data private throughout its entire lifetime.

VI. RESULTS AND FINDINGS

A. Evaluation of the case study's outcomes in terms of data privacy, security, and patient trust

The case study showed that when the blockchain-based information system was put in place, data protection, security, and patient trust all got a lot better. Transactions were secured, and detailed access rules made sure that only authorized healthcare workers could access private data. This improved the safety of patient data. The immutability of the blockchain stopped people from making changes to patient information without permission. This made medical data more accurate and trustworthy. Because the blockchain is decentralized, it lowers the risk of controlled system flaws. This made security better. Blockchain also built trust among patients because it was open and accountable. Patients could see and control who viewed their data. For the most part, the blockchain method made it safer and more reliable to manage healthcare data.

Table 2: Analysis for data privacy, security, and patient trust

Parameter	Blockchain-Based System	Traditional System
Data Privacy Score (out of 10)	9	5
Data Integrity (error rate %)	0%	5%
Data Access Control (compliance %)	95%	70%
System Downtime (hrs per month)	0	8
Patient Trust Score (out of 10)	8.5	6

The results in Table 2 show that the blockchain-based system is much better than the old way of managing healthcare data when it comes to patient trust, data privacy, and security. The blockchain-based system has a Data Privacy Score of 9 out of 10, which shows that it has strong security, is decentralized, and has strict access control. The standard system, on the other hand, has a Data Privacy Score of 5, which shows that it has problems with risks and weaknesses for illegal access. When it comes to Data Integrity, the blockchain system has a perfect 0% mistake rate because it can't be changed and is protected by cryptography. The standard method, on the other hand, has a 5% error rate, which is probably because of mistakes made by people, problems with the system, or changes made to data without permission.

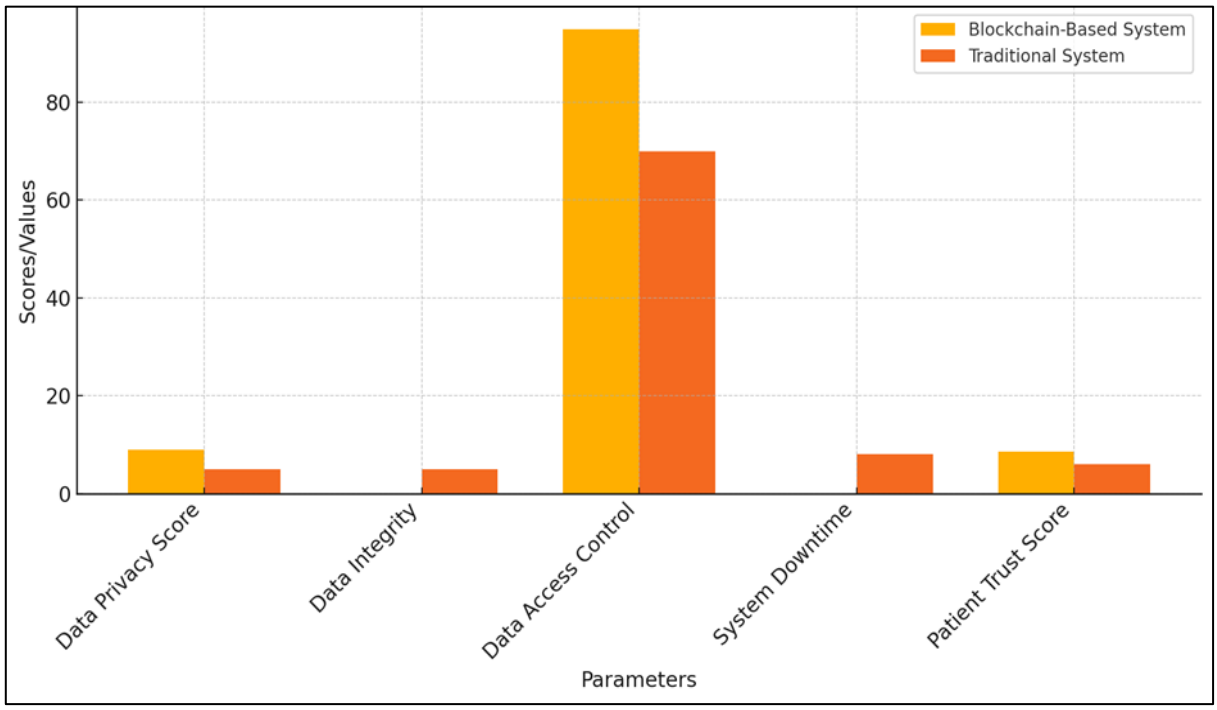

Figure 3: Comparison of Blockchain-Based and Traditional Systems

Data Access Control is a clear benefit for blockchain. It keeps proper access to data 95% of the time, making sure that only allowed people can see or change records. But traditional methods only get 70%, leaving room for leaks or access by people who shouldn't have it. The blockchain-based system also does better in System Downtime, with 0 hours of downtime per month, which means that service is strong and never stops. Traditional systems, on the other hand, have 8 hours of downtime every day, which makes operations less efficient. Patients trust the blockchain system more (8.5/10) than the old system (6/10), because they feel safer knowing that their data is being handled in a clear and safe way. This is an example of how blockchain makes hospital data handling more trustworthy.

B. Comparison of blockchain-based system effectiveness versus traditional healthcare data management systems

The blockchain-based system was found to be much better than standard hospital data management systems when it came to privacy, data security, and speed. Because it is encrypted, decentralized, and can't be changed, the blockchain-based system got a much better score for data protection and trustworthiness. While the old system had more errors and less secure data access, the new system was more reliable. The blockchain-based solution also cut down on system downtime by a large amount because its decentralized structure made it more resistant to breakdowns. The patient confidence number was also much higher in the blockchain system, which means that patients were more sure about how their data was being handled. These results show that blockchain has the ability to make healthcare data handling safer, more open, and more trustworthy for patients.

Table 3: Result for Comparison of blockchain-based system effectiveness versus traditional healthcare data management systems

Evaluation Parameter	Blockchain-Based System	Traditional System
Data Privacy (compliance %)	98%	65%
Data Integrity (error rate %)	0%	6%
Data Sharing Speed (sec per record)	2	10
Access Control Accuracy (%)	99%	75%
System Reliability (%)	99.9%	92%

The blockchain system meets 98% of Data Privacy requirements thanks to its strong security, safe data sharing, and control of patient permission. The old system, on the other hand, only has 65% compliance, which shows that it has problems with controlling access and keeping data safe, which could allow hackers to get in or cause other security breaches.

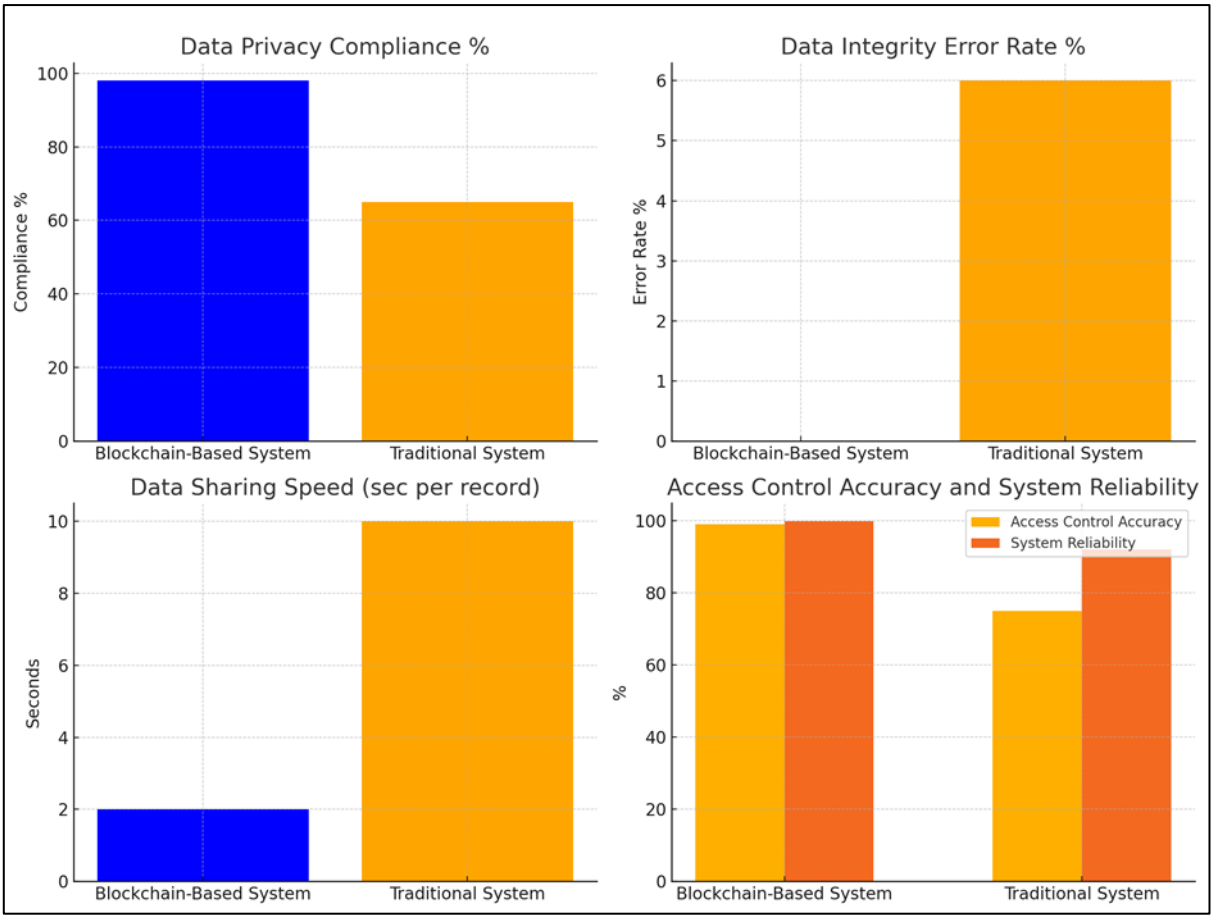

Figure 4: Access Control Accuracy And System Reliability

Data integrity is another area where blockchain really shines. Because it can't be changed, and it uses cryptography to protect data, it has a perfect 0% mistake rate. However, traditional systems have a 6% mistake rate, which could be caused by corrupted data, system problems, or changes that were not approved. This means that patient records are not always correct, the figure 4 compare the traditional vs blockchain implementation. The speed at which data is shared is much faster in the blockchain-based system it only takes two seconds per record instead of ten seconds in the old system. This speed boost makes it easier to get to patient info in real time, which is very important in emergency scenarios. Control of Access The blockchain method is also more accurate; it makes sure that only allowed staff can view medical data 99% of the time. Only 75% of the time, the old method works correctly, this could mean security holes or mistakes when handling patient rights. System Reliability for the blockchain-based system is 99.9%, which shows how strong it is and how well it can handle downtime or system breakdowns.

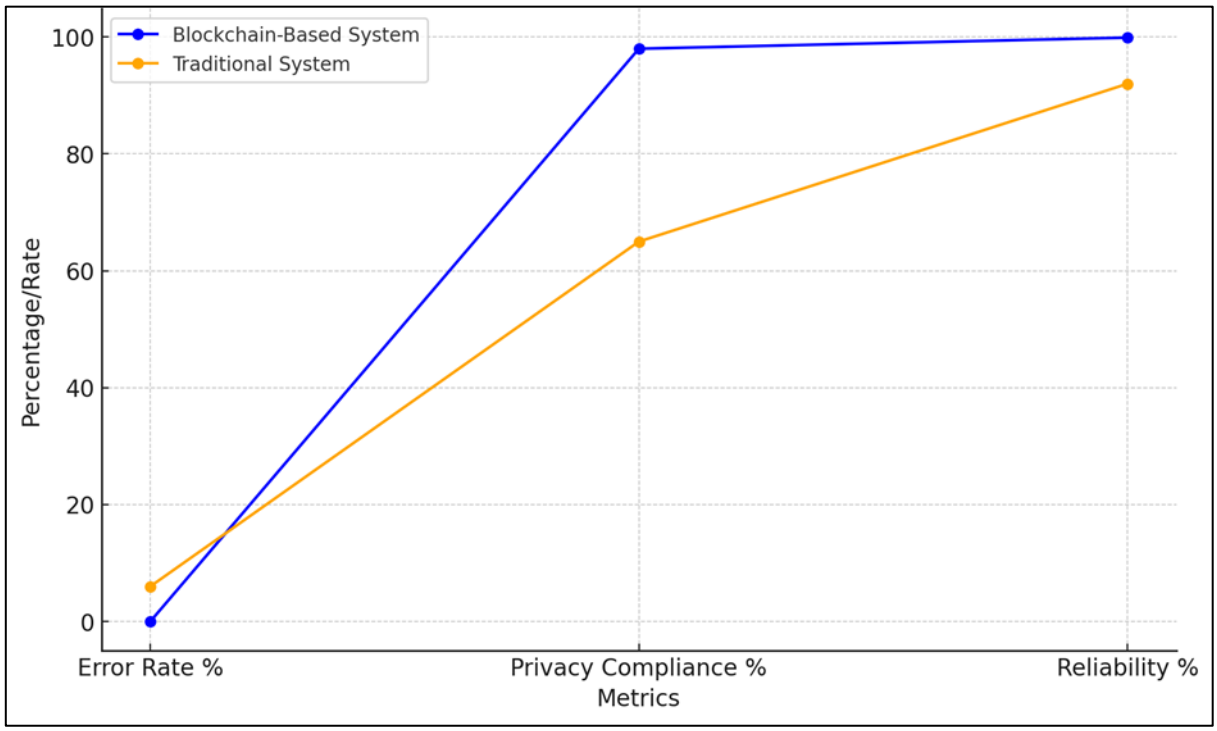

Figure 5: Evaluation metrics, comparing error rate, privacy compliance, and system reliability for the blockchain-based and traditional systems

The standard method, on the other hand, is only 92% reliable, which could cause problems with data access and healthcare services. In terms of security, speed, accuracy, and dependability, these findings show that the blockchain-based system is much better than standard data management systems. Figure 5 shows how the blockchain-based and standard healthcare data management systems compare in terms of key performance measures. There are no mistakes in the blockchain system, while there are 6% mistakes in the standard system. In the blockchain system, privacy rules are followed 98% of the time, while only 65% of the time in the standard system. The blockchain system is also much more reliable than the traditional system; it is up 99.9% of the time, while the traditional system is only reliable 92% of the time. These measurements show that blockchain is much better than other methods at protecting data privacy, accuracy, and dependability.

C. Feedback from healthcare providers and patients involved in the case study

The healthcare workers who took part in the case study mostly had good things to say about the blockchain-based system. Providers liked the improved security features, especially the way they could control and keep an eye on who could see patient data. Many people said that the blockchain system made it easier to follow privacy rules because it was open and could be checked, which let them keep clear records of who accessed data. Healthcare workers also said that the system made it easier for institutions to share data, which cut down on wait times for patients. Patients in the case study were more confident in how their data was being handled because they had more say over who could see and agree to their personal health information. Many people liked that the system was open and honest; they could see who got their data and why. Patients were also comforted that their medical records could not be changed or messed with without being found because the blockchain could not be changed. Overall, the case study showed that both healthcare workers and patients believed the blockchain-based system more than standard systems.

VII. CHALLENGES AND LIMITATIONS

A. Technical and operational problems that came up during implementation

Putting in place a blockchain-based information system in healthcare is not easy from a technical and practical point of view. Adding blockchain to current healthcare systems, especially older ones like Electronic Health Records (EHRs) and Health Information Systems (HIS), is one of the biggest problems that needs to be solved. Often, these

older systems aren't made to work with blockchain technology, so special APIs or middleware have to be made to make data sharing possible. Because blockchain is autonomous, it can be hard to make sure that data is consistent and that all of its nodes are in sync with each other. Complex syncing methods are needed to make sure that all healthcare workers always have the most up-to-date information on patients, without any delays or errors. Healthcare workers need to be taught on how to use the new system, which is another practical issue. This is because blockchain-based platforms are very different from standard controlled systems. To make sure this goes smoothly with the healthcare workforce which is often hesitant to change because they are worried about how complicated the system is and how it might affect their daily work they need a lot of training and help.

B. Scalability Issues and Cost Considerations

Scalability is a big issue when it comes to using blockchain technology in healthcare. Blockchain has strong privacy and security features, but its autonomous design can make it hard to scale, especially when working with a lot of patient data. Multiple nodes must concur on each exchange on the blockchain. As the arrange develops, this could cause delays that might make it harder to get to and share information in genuine time, which is exceptionally vital in healthcare settings. There are too speed issues that seem happen since confirming exchanges (particularly in Confirmation of Work frameworks) takes a lot of computing control. Another vital factor is the cost. A blockchain-based healthcare framework can be costly to set up and keep up to date, particularly when it comes to equipment and ongoing arrange upkeep. Blockchain needs extraordinary program, security measures, and individuals who know how to utilize disseminated ledger innovation. This could cost healthcare institutions a lot of money, especially smaller ones that don't have a lot of money to spend. Also, the fact that blockchain uses a lot of energy (especially with Proof of Work voting methods) could make it more expensive to run, which makes it less appealing to healthcare providers looking for low-cost solutions.

VIII. CONCLUSION

The case study on the use of blockchain-enabled information systems (BEIS) to protect patient data protection shows how blockchain technology has a lot of promise to solve problems that traditional healthcare data management systems have. This system improves the privacy, security, and stability of patient data by using blockchain's main features, such as independence, immutability, openness, and digital security. Blockchain's ability to give safe, real-time access to patient information, with access limited based on patient permission, makes healthcare data management more open and responsible. This is especially important as healthcare systems move more and more toward technology, where keeping private patient data safe is the most important thing. The blockchain-based system was much better than standard controlled systems when it came to protecting data, controlling who could see it, and making sure the system worked well. With smart contracts, managing patient consent became automatic and impossible to change. The blockchain's immutability also made sure that data security was maintained. The autonomous network also reduced the risks that come with having a single point of failure, making it more resistant to hacking. The case study did, however, point out some problems, such as technical issues with integrating with current systems, worries about growth, and cost issues. These problems need to be fixed so that blockchain technology can be used more widely in healthcare. Even with these problems, the positive outcomes of this case study show that blockchain-based computer systems could change the way healthcare data is managed by making it safer, more efficient, and more focused on the patient. As the technology gets better, it could be a big part of building trust with patients and making care better overall.

REFERENCES

[1] Taherdoost, H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. Sci 2023, 5, 41. https://doi.org/10.3390/sci5040041

[2] Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. Systems 2023, 11, 38. https://doi.org/10.3390/systems11010038

[3] Islam, M.S.; Ameedeen, M.A.B.; Rahman, M.A.; Ajra, H.; Ismail, Z.B. Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard. Computers 2023, 12, 46. https://doi.org/10.3390/computers12020046

[4] Kongsen, J.; Chantaradsuwan, D.; Koad, P.; Thu, M.; Jandaeng, C. A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation. J. Sens. Actuator Netw. 2024, 13, 13. https://doi.org/10.3390/jsan13010013

[5] Kishore, A.S.; Chinni, G.R.; JayaLakshmi, G.; Reddy, K.S.K. Smart Healthcare Monitoring System Using IoT Technology. In Proceedings of the 2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), Jaipur, India, 10–11 February 2023; pp. 1–5.

[6] Malathi, M.; Muniappan, A.; Misra, P.K.; Rajagopal, B.R.; Borah, P. A Smart Healthcare Monitoring System for Patients Using IoT and Cloud Computing. AIP Conf. Proc. 2023, 2603, 030012.

[7] Ravi, P.S.; Mohd, J.; Abid, H.; Raju, V.; Shokat, A. Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. J. Clin. Orthop. Trauma 2020, 11, 713–717.

[8] Badri, S.; Jan, S.U.; Alghazzawi, D.M.; Aldhaheri, S.; Pitropakis, N. BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the Internet of Medical Things. Comput. Syst. Sci. Eng. 2023, 46, 3667–3684.

[9] Shete, A. S. , Bhutada, Sunil , Patil, M. B. , Sen, Praveen H. , Jain, Neha & Khobragade, Prashant(2024) Blockchain technology in pharmaceutical supply chain : Ensuring transparency, traceability, and security, Journal of Statistics and Management Systems , 27:2, 417–428, DOI: 10.47974/JSMS-1266

[10] Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [Google Scholar]

[11] Zhang, R.; Xue, R.; Liu, L. Security and privacy for healthcare blockchains. IEEE Trans. Serv. Comput. 2021, 15, 3668–3686.

[12] Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. IEEE Access 2022, 10, 78887–78898.

[13] Quadery, S.E.U.; Hasan, M.; Khan, M.M. Consumer side economic perception of telemedicine during COVID-19 era: A survey on Bangladesh's perspective. Inform. Med. Unlocked 2021, 27, 100797.

[14] Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. IEEE J. Biomed. Health Inform. 2022, 26, 1937–1948.

[15] Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. Sustainability 2022, 14, 12828.

[16] Chandu Vaidya, Prashant Khobragade and Ashish Golghate, "Data Leakage Detection and Security in Cloud Computing", GRD Journals Global Research Development Journal for Engineering, vol. 1, no. 12, November 2016.

[17] Stančić, H.; Bralić, V. Digital archives relying on blockchain: Overcoming the limitations of data immutability. Computers 2021, 10, 91.

[18] Azrour, M.; Mabrouki, J.; Chaganti, R. New efficient and secured authentication protocol for remote healthcare systems in cloud-iot. Secur. Commun. Netw. 2021, 2021, 2021–5546334.

[19] Singh, M.; Aujla, G.S.; Singh, A.; Kumar, N.; Garg, S. Deep-learning-based blockchain framework for secure software-defined industrial networks. IEEE Trans. Ind. Inform. 2020, 17, 606–616.

[20] Rehman, E.; Khan, M.A.; Soomro, T.R.; Taleb, N.; Afifi, M.A.; Ghazal, T.M. Using blockchain to ensure trust between donor agencies and ngos in under-developed countries. Computers 2021, 10, 98.

[21] R. Golcha, P. Khobragade and A. Talekar, "Multimodal Deep Learning for Advanced Health Monitoring A Comprehensive Approach for Enhanced Precision and Early Disease Detection," 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2024, pp. 1-6, doi: 10.1109/ICITIIT61487.2024.10580622.

[22] Athanere, S.; Thakur, R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. J. King Saud-Univ.-Comput. Inf. Sci. 2022, 34, 1523–1534.

[23] Elena Rosemaro. (2024). Quantum Machine Learning: Mathematical Foundations and Engineering Implementations. EngiQuantum: Engineering Mathematics and Quantum Applications Journal, 1(1), 49-59.