https://doi.org/10.38124/ijsrmt.v3i4.27

Blockchain-Enabled Security Solutions for Medical Device Integrity and Provenance in Cloud Environments

[1]Omolola Akinola
Dept. of Information Systems and Analysis
Lamar University, Beaumont, Texas, USA
0009-0006-6788-2791

[2]Akintunde Akinola
Department of Accounting and Finance
Ekiti State University

[3]Basirat Oyekan
Dept. of Mathematics
Lamar University Beaumont, Texas, USA

[4]Omowunmi Oyerinde
MIS Lamar University Beaumont, Texas

[5]Halimat Folashade Adebiyi
Dept. of Business Technology
Federal University of Technology Minna

[6]Busola Sulaimon
Dept of Industrial and System Engineering
Lamar University Beaumont, Texas USA

Abstract:- The current period of medicine using digital technology for patient care presents a new level of integration of monitoring devices with the cloud computing environment that enables the collection, storage and access to data in ways that were never possible earlier. As the obvious part of this development, it is worth noting that the objective of such innovation is mostly on the integrity of data, provenance and security. Data integrity from as well as security of the Internet connected healthcare devices should be assured in the first place to keep patient safety and protect data privacy along with improve data-based decision-making. The centralized system and crowded nature of the current equipment are susceptible to single point of failure, data breach and potential manipulations of data, which raise questions and create doubts with regards data management processes pertaining to medical device systems. This work is addressed to the analysis of a novel security system based on blockchain that guarantees the implementation of a high performance with the solution of two medical device integrity and provenance safety issues in the cloud ecosystem. Fundamentally differentiating from the centralized systems that exist today, blockchain technology that is based on distributed database architectures, immutable logs, and consensus mechanisms provides for a new way to bring reliability and traceability to the entire medical device data chain. The suggested procedure is based on properties of blockchain technology. Such a solution can help to provide a clear and secure audit trail for medical devices. Storing, securing and accessing the device data can be carried out credibly, maintaining these data's integrity and provenance. Ultimately, the solution, rely on the implementation of smart contracts, cryptocurrency processes, and the confidentiality and privacy of data, can be the answer which make up the practice of secure data sharing, data accessing and complying with regulations. The journal creates a modular system combining Medical devices, a cloud platform, and Blockchain solution. The architecture is intended to display the blockchain network's essential components, data validation and access control, and secure data storage mechanisms. Furthermore, the recommended solution implies state-of-the-art security tools, such as data encryption, access control, and abidance by regulatory systems, including HIPAA and GDPR. Implementation of an actual scenario of the proof-of-concept and performance evaluation are done to show the efficiency and performance of the blockchain-based solution provided. The results suggest that the proposed solution can establish the data reliability level, record all the various versions of modifications, and strengthen the security and transparency of medical device data processing in cloud computing. Through the exploration of the applications of blockchain for medical data management that this study proposes, we are laying the foundations of a future healthcare environment, which is expected to be more secure and trustworthy, where the sensor data of medical devices can be reliably controlled and accessed without jeopardizing the patient's safety or data privacy. To a great extent, the suggested solution can contribute to building trust in the digital tools utilized in health

https://doi.org/10.38124/ijsrmt.v3i4.27

care, leading to more well-informed clinical decisions and ultimately improving the patients' results.

Keywords:- *Blockchain, Medical Device Integrity, Provenance, Cloud Computing, Security, Data Integrity, Decentralization, Immutability, Transparency.*

I. INTRODUCTION

The medical world is rapidly embracing digitization, which incorporates medical equipment and virtual cloud environments (Toosi et al., 2014). Medical devices, as a whole, are vital for gathering and transferring patient data necessary for a proper diagnosis, effective treatment planning, and a sound decision-making process by medical practitioners. As for the data integrity and provenance of medical devices through their life cycle stages, i.e., from collection to storage, had better be verified.

The integrity of the data is a term given to its accuracy, completeness, and consistency. It implies that while being transmitted/stored, the data should not be altered, corrupted, tampered or otherwise contaminated. Authenticity, in contrast to provenance, refers to the traceability of some data origins and history, such as data generated by devices, the data collection time and location, and the time of occurrence of any modification or processing (Jaigirdar et al., 2019). Data integrity and provenance need to be well maintained, which includes patient safety; this will help the healthcare ecosystem to gain trust and transparency, and also compliance with regulatory frameworks, among them are HIPAA and GDPR (Kaur et al., 2018). However, though cloud computing-enabled centralized systems for medical device data management have numerous advantages, they also face some significant issues of their single point failure, risk of data manipulation, lack of auditability and scalability/interoperability. (Motohashi et al., 2019).

The key aim of this research is to design a blockchain-enabled security tool that all doctors can apply to keep the data from medical devices secure all the time, especially in cloud computing surroundings. Blockchain technology stands out among all the technologies possible because of its decentralized approach, immutable ledger system, and consensus mechanisms, which allay the fears of faking and altering such data (Yang et al.,2020). This research scope includes the development of a comprehensive system architecture using blockchain technology, the design of data integrity, and data provenance mechanisms and protocols. Security and privacy considerations will also be dealt with, along with the proof-of-concept prototype implementation and extensive experimental evaluation.

➢ *Research Question*

- How can blockchain technology be effectively integrated into existing medical devices and cloud computing infrastructures to ensure data integrity and provenance?
- What are the appropriate mechanisms and protocols for leveraging blockchain's decentralized architecture, immutable ledger, and consensus mechanisms to maintain data integrity and provenance throughout the data lifecycle?
- How can security and privacy considerations, such as access control, data encryption, and regulatory compliance, be addressed in the proposed blockchain-based solution?
- What are the performance, scalability, and security implications of implementing a blockchain-based solution for medical device data management in cloud environments?
- What are the potential challenges and limitations of the proposed solution and how can they be mitigated or addressed in future research?

II. LITERATURE REVIEW

A. Medical Device Data Integrity and Provenance

Integrity and providence data dedication are crucial in the case of medical devices detecting in the healthcare environment. Regarding data integrity, the data must be accurate, overall, and whole while it is being transmitted or stored; the possibility of being altered, corrupted, or tampered with is minimized (Harley & Cooper, 2021). Processing, however, implies the ability to determine the traceable beginning and history of data raising the information about device, the time and location of collection and the possibility of further changes or any other processing (Hardin, & Kotz, 2021).

The direct bearing of data integrity and provenance on medical devices is so profound that it cannot be underestimated. It’s these features that emphasize the safety of the patient, as minor errors and manipulation might lead to wrong diagnosis, wrong treatment plan, and, in the worst cases, even fatal consequences. In addition to the real- time monitoring of patients' health data by healthcare staff, ensuring data consistency and provenance is an absolute requirement to strengthen the health information system. It enables healthcare providers, patients, and regulating authorities to verify the authenticity and trustworthiness of patient data (Hasan et al., 2009).

https://doi.org/10.38124/ijsrmt.v3i4.27

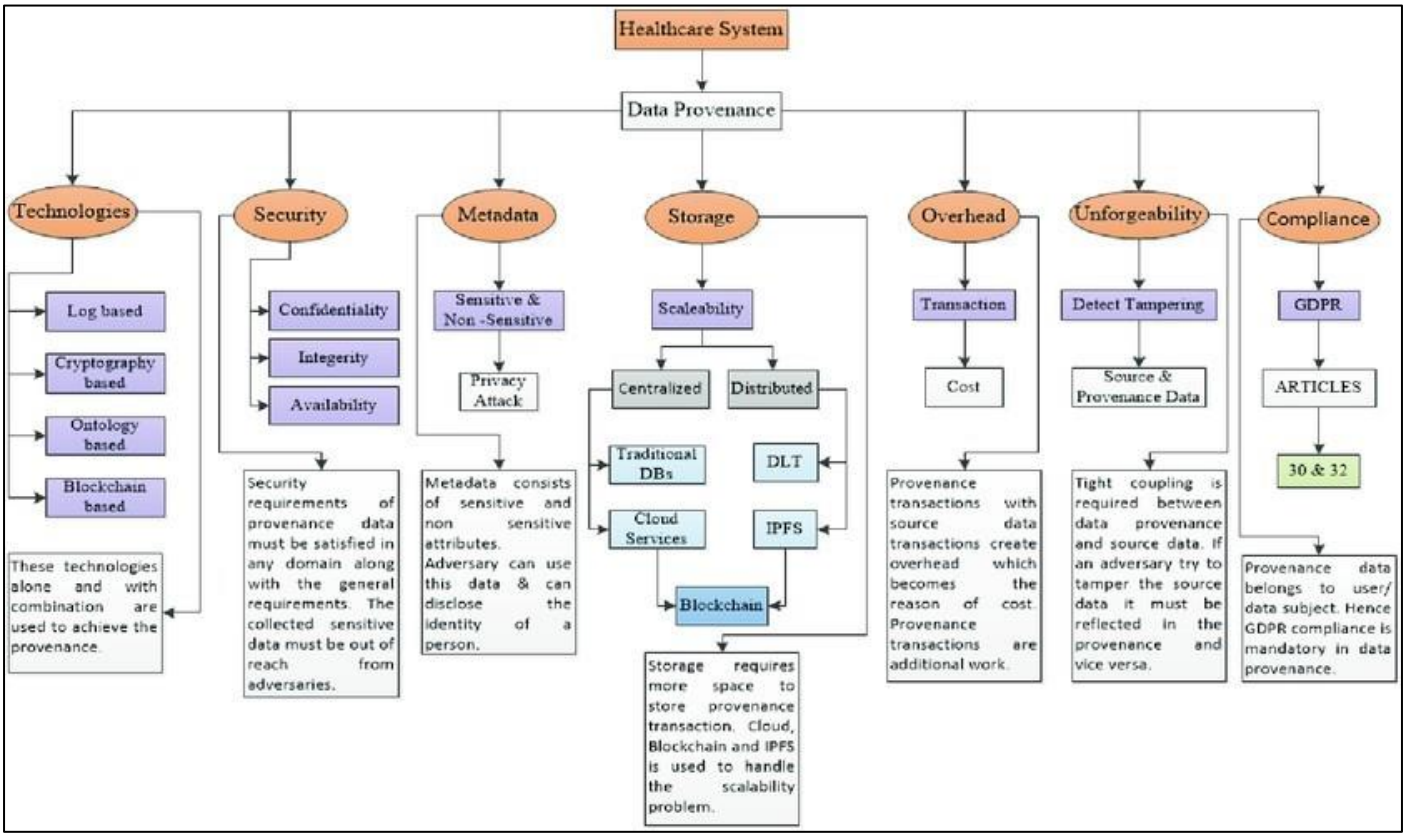

Fig 1: Taxonomy of Data Provence in Healthcare
Source: Ahmed et al. 20

Despite the importance of data integrity and provenance, current practices in medical device data management face several challenges and limitations. One of the primary challenges is the reliance on traditional centralized systems, which are susceptible to single points of failure, data breaches, and potential data manipulation by malicious actors or unauthorized parties (Harley & Cooper, 2021). These centralized systems often lack transparency and immutability, making it difficult to trace the origin and history of medical device data, as well as detect any tampering or unauthorized modifications.

Another significant challenge is the complexity of medical device data management, which involves numerous stakeholders, including healthcare providers, device manufacturers, regulatory bodies, and third-party service providers. This complexity can lead to data silos, interoperability issues, and inconsistencies in data handling practices, further exacerbating the risks to data integrity and provenance (Hardin & Kotz, 2021).

Besides that, the increasing use of IoT devices and home healthcare testing systems has brought up new rules concerning security and privacy. These devices typically function in resource-stressed surroundings, and they rarely have security mechanisms that are strong. Hence, they can be exposed to various cyber threats and information breaches (Hasan et al., 2009). It is necessary for the systems to have an integrity and providence of data that is collected from those devices for the integrity of the medical device data ecosystem as a whole.

Table 1: Challenges in Maintaining Medical Device Data Integrity and Provenance

Challenge	Description
Single Point of Failure	Centralized systems are vulnerable to failures, attacks, or data breaches that can compromise the entire system's integrity.
Data Manipulation	Traditional systems lack transparency and immutability, allowing for potential data tampering or unauthorized modifications.
Lack of Auditability	Difficulty in providing comprehensive and tamper-proof audit trails to trace the origin and history of medical device data.
Scalability and Interoperability	Centralized systems may struggle with scalability and seamless integration of data from diverse sources and healthcare providers.
Security and Privacy Concerns	Risks of data breaches, unauthorized access, and non-compliance with data protection regulations like HIPAA and GDPR.

https://doi.org/10.38124/ijsrmt.v3i4.27

Furthermore, in order to address that problem there has been a growing demand for breakthrough approaches that can give reliable, secure, and unchanged systems for maintaining data reliability and origin throughout the whole period of medical device data – starting from the generation and ending with storing and providing access.

B. Blockchain Technology

Furthermore, in order to address that problem there has been a growing demand for breakthrough approaches that can give reliable, secure, and unchanged systems for maintaining data reliability and origin throughout the whole period of medical device data – starting from the generation and ending with storing and providing access.

Fig 2: Deep Dive into Blockchain Technology in Healthcare
Source: (Anand, 2024)

One of the key features of the blockchain technology is the decentralized architecture emphasizing the authority of the third party that is no longer needed. Rather than by some central infrastructure, this process of validating and recording transactions is carried out through a commonly-agreed decisionmaking process among the nodes that are network participants (Yli-Huumo et al., 2016). It enables the diversification of the system which in turn reduces the risk of single crucial failure points and raises the overall reliability and transparency of the network.

Another important element that makes up blockchain technology is its unalterable nature. In blockchain, after being entered in the network, the transaction becomes very difficult to change or edit, in fact, it is almost impossible, even if you leave a traceable trail.

This immutability is realized by means of cryptographic hash functions and the chaining of blocks through which a reference to the previous block is added, so that the information contained in a block cannot be changed without changing all the previous blocks, which ensures that the record is verifiable and cannot be modified.

Blockchain's transparency is also one of its key pillars. Since the ledger is distributed across multiple nodes in the decentralized network, there is a single copy of the data available to all participants, which eliminates the necessity of multiple sharing and validation. In consequence, the consortium provides the door to transparency, which leads to the reliability and accountability of all the participants involved in the process because any attempt to manipulate or imitate the data may be easily noticed and rejected by the consensus mechanism (Cui et al., 2019).

Blockchain technology's huge application in healthcare is unlimited and has a bright future. Blockchain could be a revolutionary instrument for medical records and data provenance management, and it could make a huge difference. If the blockchain technique, which is known for its immutability and transparency, is used, then healthcare organizations can guarantee the authenticity and integrity of patient data. This will make patient information safe and auditable while still protecting patient privacy.

Apart from this, the use of artificial intelligence is not only limited to the pharmaceutical industry, but it also has applications in the supply chain management of drugs and medical devices. The records within the blockchain are capable of tracking products from source to end of life. They do this in order to secure traceability, anti-counterfeit, and to aid regulatory compliance (Cui et al., 2019).

https://doi.org/10.38124/ijsrmt.v3i4.27

Table 2: Key Features of Blockchain Technology

Challenge	Description
Decentralization	Eliminates the need for a central authority or intermediary, reducing the risk of single points of failure.
Immutability	Transactions recorded on the blockchain are extremely difficult to modify or delete, ensuring data integrity and tamper-resistance.
Transparency	Distributed ledger allows all participants to access and validate the exact copy of the data, fostering trust and accountability.
Consensus Mechanism	Transactions are validated and recorded through a consensus among participating nodes, ensuring data consistency and security.
Cryptographic Security	Use of cryptographic techniques like hashing and digital signatures to ensure data integrity and authenticity

Moreover, blockchain technology provide ground for secure data sharing among all the different persona involved in the healthcare system like researchers, medical institution, and regulatory agencies. Such can be a perfect way of speeding up the development of medical research, as well as support collaboration and data-driven decisions, but all this must be done with a firm stance on data estate and consent (Zheng et al., 2017).

However, like other emerging technologies, blockchain in healthcare is accompanied by challenges and constraints which require reconsideration. The problems such as the long-term scalability of the machines, the energy consumption that the devices will demand, interoperability , and the regulatory compliance requirements, etc. are the other major ones including them (Yli- Huumo et al., 2016).Along with this, the integration of blockchain technology in the heath care systems as a whole may be faced with the concern of data security, privacy and the difficulty about it to be integrated with the existing systems and process.

C. Blockchain-based Solutions for Medical Device Integrity and Provenance

In recent times, blockchain has become a topic of interest as it has been taken as a solution to the challenges of verifying data integrity and directionality as regards medical device data management. Since blockchain-based technologies first emerged, the community has deployed many blockchain- based solutions in real-life environments; one of the advantages of blockchain is the ability to store and process information securely and transparently.

As an example of their study by Hardin and Kotz (2021), they introduced a blockchain based system called Amanuensis, which would have provided the means for tracking and validation of a patient's health data at different places for example medical equipment, health service providers and data repositories. The ditact nature of the amanuensis, which is built around decentralization and a records books that is incarcerated, creates an auditable path that is secure and unalterable. Such an environment deems it possible to guarantee data accuracy and the origin of the data.

Moreover, another research of Motohashi et al. (2019) proposed a medical health data management system which is built on Blockchain technology by means of a client hash chain scheme. This company seeks to solve such personal data issues as data storage, privacy, and management of mobile health (mHealth) apps and patient monitoring devices. The solution makes use of blockchain

attributes, such as immutability and decentralization, together with the client hash chain, promising an efficient storage solution to ease the challenge of handling mHealth data.

Cui and co.2019) have created a blockchain-supported network using which it will be easy to deal with medicinal products supply chains (Clin et al. 4, 3350–3360). Provenance uses smart contracts on a permissioned blockchain to record and verify provenance information on the products during their supply chain. The smart contract can bind them with an unchangeable record and enhance the supply chain authenticity of their products. This is a method that may reduce risks of counterfeits, bring compliance towards the standards, and, as a result, make a medical device supply chain more open, trustworthy, and transparent.

Table 3: Existing Blockchain-based Solutions for Medical Device Data Management

Solution	Description	Key Features
Amanuensis (Hardin & Kotz, 2021)	A blockchain-based system for tracking and verifying the provenance of health data across stakeholders, including medical devices.	Decentralized architecture, immutable ledger, tamper-proof audit trail.
Secure mHealth Data Management (Motohashi et al., 2019)	A system combining blockchain and client hashchain for secure and scalable management of mobile health (mHealth) data from remote patient monitoring devices.	Data integrity, privacy, and scalability through blockchain and hashchain.
Supply Chain Provenance Framework (Cui et al., 2019)	A blockchain-based framework for supply chain provenance, applicable to medical device supply chains.	Smart contracts, permissioned blockchain, product traceability, and authenticity.

https://doi.org/10.38124/ijsrmt.v3i4.27

However, despite the fact that cryptocurrency and its methods have very encouraging possibilities, they, in turn, have even their own restrictions and problems. Blockchain as one of the promising technologies in the medical Internet of Things has its own challenges and scalability and performance issues are among them (Yli- Huumo et al., 2016). The drawbacks of choosing the blockchain architecture for the network may be the extra latency and computational overhead introduced by the consensus mechanisms and data replication concepts, which may be unfavorable for real-time processing and accessibility of the critical device data.

Next obstacle is the interlocking of healthcare blockchain solutions in with the current healthcare systems and an optimal performance of their workflows. Most of the healthcare industries still run on the now- outdated infrastructure and data management systems, which may constitute a hindrance in the seamless adoption of blockchain technology. According to Zheng et al. (2017), major challenges of interoperability, data migration, prolonged training, and transformation may present a substantial hindrance to the mainstream use of blockchain-based programs.

And the privacy of data as well as the regulation to which it is compliant are some of the vital issues facing the health sector. Blockchain Technology has the inherent security and transparency features. Nevertheless, in order to conform to the privacy and the data security laws such as the HIPAA and GDPR, the implementation of access control mechanisms, data encryption techniques and the practical consent management process is obligatory (Latimer & Zhang, 2019).

In addition to the matters mentioned above, blockchain-based technologies for medical device integrity and provenance not only bring very good results but are part of the decent development. Along with the maturing technology and its higher adoption, most of the current limitations are expected to be addressed, thus rendering the complex, secure, and large-scale solutions that will ultimately prove to reduce the risk of the medical device data being tampered with in the cloud environment.

Table 4: Potential Applications of Blockchain in Healthcare

Application	Description
Medical Records and Data Provenance	Ensuring the integrity and authenticity of patient data, enabling secure and auditable access to medical records.
Supply Chain Management	Providing a tamper-proof and transparent record of the entire supply chain for pharmaceuticals and medical devices.
Secure Data Sharing	Facilitating secure and transparent data sharing among stakeholders, researchers, and medical institutions while maintaining data privacy.
Clinical Trial Management	Enhancing transparency, data integrity, and patient recruitment processes in clinical trials.
Billing and Claims Processing	Streamlining insurance claims and billing processes, reducing fraud and improving transparency.

III. PROPOSED BLOCKCHAIN-ENABLED SECURITY SOLUTION

A. System Architecture

The planned blockchain-based system architecture, medical device integrity and provenance in cloud-based environment have a decentralized design to connect medical devices, cloud computing network, and blockchain network together. This integrated approach ensures the secure and tamper- proof management of medical device data throughout its entire lifecycle.

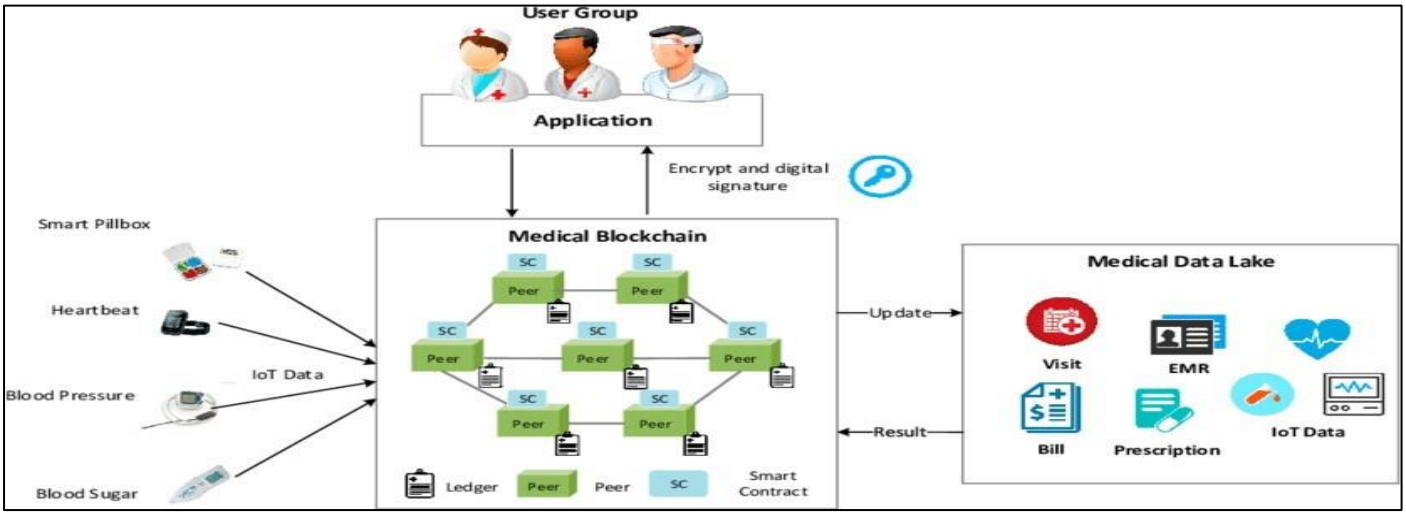

Fig 3: Conceptual Scenario of Medical Blockchain
Source: Lei, et al 2019

https://doi.org/10.38124/ijsrmt.v3i4.27

- Medical Devices: The system architecture includes various types of medical devices, such as wearable sensors, implantable devices, and remote patient monitoring systems. These devices play a crucial role by collecting and transmitting patient data to the cloud computing infrastructure. The integration of medical devices into the system architecture is essential for capturing real- time and accurate data from patients, which forms the foundation for subsequent data management and analysis processes.
- Cloud Computing Infrastructure: The cloud computing infrastructure serves as the primary storage and processing environment for medical device data. It comprises cloud servers, databases, and data processing services that facilitate the storage, retrieval, and analysis of the collected data. Through the benefits of the scalability and computational capacity of the cloud computing, this solution can handle great sizes of medical device data effectively and offer fast and updated connection to health professionals and other authorized parties.
- Blockchain Network: The central solution component is a blockchain network that functions as a distributed and tamper-proof ledger for the registration and data validity of medical device deals. The blockchain network, among other things, includes many nodes utilized by different entities, including healthcare providers, regulators, and trusted intermediaries. Decentralization cancels the need for a single central point of failure, thus mitigating the risk and advancing the overall stability and transparency of the system (Zheng et al., 2017).
- Smart Contracts: Smart contracts are autonomous software codes put in the blockchain environment to do the job of a designated contract. On the proposed solution, the smart contracts will be applied to uphold integrity of the data and provenance in addition to access control and data sharing policies. The smart contracts could be constructed to automatically perform the condition programmed and the predefined rules with a view of ensuring a consistent and transparent policy application across the whole system (Vishwa & Hussain, 2018).
- Data Storage Mechanisms: The architecture plan describes the use of the reliable and decentralized data storage system that stores medical devices data and related metadata. These mechanisms usually can be a mix with on-chain and off-chain storage solutions, which include distributed file systems and decentralized storage networks (e.g., IPFS, Storj). Through using decentralized storage alternatives to ensure data resilience, integrity, and scalability while greatly diminishing risk of breaches of data through centralized data systems or single points of failure (Zafar et al., 2017).
- Access Control and Identity Management: The architecture comprises the access control and identity management component that allows access to the system only to the relevant stakeholders based on their assigned roles and permissions and by utilizing suitable authentication methods. The last aspect guarantees that after obtaining explicit permission, only approved parties can access or reform medical device data with consideration of policies and regulations that have been specified beforehand. The usage of data access control systems is the fundamental issue in preserving data privacy as well as the alignment with the requirements of HIPAA and GDPR (Miller et al., 2012).
- User Interfaces and Applications: It incorporates user interfaces and apps for healthcare professionals, patients, and other entities to engage in the medical device data and related blockchain features that provide enhanced security. These interfaces may be web-based, mobile applications or nucleus uniting with existing information systems in the healthcare. This ultimate approach in providing easy-to-use interfaces, would promote smooth integration of existing workflows, leading to its wide acceptance among healthcare players.

The core elements of the architecture system are composed for the purpose of data from medical devices to being securely and transparently administered. The nodes on the blockchain network collaborate with smart contracts and decentralized data storage devices to maintain data integrity and provenance, with access control measures and identity management features incorporated to comply with security regulations as well as privacy laws.

B. Data Integrity and Provenance Mechanisms

Proposed blockchain-facilitated security solution comes from use of specific blockchain features to stand out among the crowd of medical device data integrity and security challenges. Primarily, the solution implements the following three techniques: cryptographic algorithms, consensus mechanisms, and unchangeable ledgers.

➢ *Cryptographic Techniques:*

- Hashing: The proposed solutions use hashing cryptographing algorithms, for example SHA-256, as a base transport for creating a unique and non-mutable digital fingerprints of medical device data. The data is by virtue of their hash values being stored in the blockchain, such modifications cannot be made without leaving a trace. This, in turn, guarantees data integrity. This mechanism is built on the harmonisation of the statement that even a tiny correction of input data would result in an absolutely different hash value, that allows one to notice any changes irrespective of their scale (Zafar et al., 2017).
- Digital Signatures: The digital signatures based on public key-cryptography are used to ascertain the real origin and authenticity of medical product data. Every device operator or other stakeholder has a set of twinned cryptographic key “pairs”, which include a public key and a private key. Data transactions are then signed by the private key and the public key is used to verify the signature, in this way the interaction is safe and the provenance is ensured. This established mechanism allows the originality and authenticity of data be verified by everyone with authorization to access the database

https://doi.org/10.38124/ijsrmt.v3i4.27

reducing the chances of unauthorized modifications of the data or information (Vishwa & Hussain, 2018).

➢ *Consensus Mechanisms:*

- Distributed Consensus: The blockchain network bases on a decentralized consensus mechanism, for example, Proof-of-Work (PoW), Proof-of-Stake (PoS) or pBFT (practical Byzantine Fault Tolerance), to ensure transactions recording and validation on the blockchain. This decentralized function of the network eliminates the need for a trusted authority and coordinates medtech data transactions by the consortia. Since individual systems are validating and adding new records to these blocks by resolving computational puzzles, the proposed solution utilizes the combined computing power and consensus of the network nodes which results in a highly secure and reliable ledger (Zheng, Fan & Tang, 2017).
- Immutable Ledger: In fact, once a transaction goes through validation and its record has been entered into the blockchain, the transaction becomes virtually unchangeable because of the linking of blocks cryptographically and the decentralized nature of the ledger. The cryptographic hash of the previous block becomes the next block in the blockchain, and a new block is created which will be cryptographically linked to the previous block in the chain of connected blocks. Trying to edit or interfere with the recorded data rely on a huge computing effort and a strong verification by the most of them network members, so the manipulation becomes nearly impossible and can be easily detected (Zafar et al., 2017).

➢ *Provenance Tracking:*

- Metadata and Timestamps: The proposed solution, through the recording of metadata and timestamps, ensures that medical device data exchange activities are stored on blockchain. These metadata contain the device ID, geo location, time of the day and any other relevant contextual data for the chain of custody and data authenticity. This solution will control and place the metadata that was captured and stored on the immutable blockchain ledger, thus setting up an indefeasible trace for the concerned stakeholders to track the origin. intellect, ownership and medical device history are a few noteworthy aspects (Vishwa & Hussain, 2018).
- Auditable Transactions: Each time information about medical devices like data generation, update requests, access or sharing events etc. are recorded on the blockchain ledger the ledger gets another mark of the transaction this way becoming immutable or unchangeable. It gives rise to an unalterable log of data changes that helps the organizations track the data source and history so; therefore, transparency and accountability are advocated. The tamper- proof character of the ledger obstructs electronic theft and other manipulations to a medical device data, facilitating the detection and investigation of the unwanted access and modifications. This in turn helps to build the trust and comply with regulatory requirements (Zafar et al., 2017). Through these tools the proposed blockchain-backed security system guarantees the integrity and authenticity of medical device data which proves to enhance the patient safekeeping, regulatory compliance, and the general trusting in the health sector.

C. Security and Privacy Considerations

The proposed mechanism born out of blockchain-based security solutions provides great advantages in verify data integrity and provenance but still there is need for establishing the security and privacy concerns for preservation and protection of medical device data.

➢ *Access Control Mechanisms*

Mechanical RBACs, for instance, are among the security measures which can be implemented. In the implementation, the solution puts a role-based access control in place where different roles, permissions, and access levels are clearly defined for the various stakeholders who interact with the medical device data. This way of controlling information functioning guarantees that only companies, which are authorized for accessing, modifying, or sharing the data are provided this information with regard to their assigned functions and tasks. As an illustration, healthcare professionals can enable read/write access to patient data, regulatory authorities possibly read only for checking/audit purposes (Miller et al., 2012). Meanwhile, the built-in multiple factor authentication is a flexible approach to increase security and eliminate unauthorized access. Passwords, biometric authentication (e.g., fingeprint, facial recognition) and hardware-based authentication tokens such as a key fob, a dongle, or an authentication card are some of the factors that one has to take into consideration. The suggested method introduces an extra factor of authentication by requiring several factors for authorization. This introduces another layer of security into the system, thus lowering the probability of unauthorized access through compromised credentials or theft of devices (Maple, 2017).

➢ *Data Encryption:*

This resolution applies the end-to-end data encryption methods which ensure confidentiality of medical device data during transmission and storage. It guarantees that a correct person with proper key encryption is the one who has and decrypts the information. The encryption process, in most cases, is performed using advanced and safe algorithms, e.g., AES (Advanced Encryption Standard), to convert the data to ciphertext even before it is released into the cloud infrastructure (Zafar et al., 2017).

The solution, in particular, it provides for the implementation processes of secure key management, such as key generation, distribution, and revocation. This can be achieved via trusted intermediary key management services, decentralized key management options or some other secure protocol for storage and distribution of the keys. Good key management practice is central to the protection of encrypted data confidentiality and integrity, authorized parties access rights (Maple, 2017).

https://doi.org/10.38124/ijsrmt.v3i4.27

➢ *Regulatory Compliance*

This solution is developed to meet all the regulations and standards of HIPAA and GDPR which exist as the most eminent among e.g. to mention few of them. It involves putting in place appropriate security procedures as well as data handling protection controls and the patient's consent management processes to protect privacy and ensure the compliance with handing data laws. Table 5 is presented to highlight major requirements and to show how the suggested solution provides them.

Table 5: Regulatory Compliance

Requirement	Solution Approach
Data Privacy and Confidentiality	End-to-end encryption, access control mechanisms
Patient Consent	Consent tracking cryptographic hashing
Access Monitoring and Logging	Auditable transaction history on the blockchain

➢ *Auditing and Logging*

The incorruptible nature of the blockchain ledger ensures the whole door opened for the detailed verifying and tracking that relates to the medical device data. The auditing capability achieved here is needed for the compliance with the requirements related to data provenance, access monitoring, and incident investigation. Through preserving all into immutable records of all operations, the proposed solution enables regulatory auditing process, enhances transparency and expedites the examination of possible cyber mishaps or breaches (Zafar et al., 2017).

➢ *Privacy-Preserving Techniques*

The solution that is being proposed follows the principle of data minimization as specific tools for medical devices data are used only to ensure the collection, processing, and storing of the minimum medical devices data necessary, which in compliance, minimizes the risk of eventual data breaches or unauthorized access. While collecting and keeping data for health care only will possibly reduce the attack surface and limit the exposure of patient sensitive information this is only possible under the supervision of the solution (Mapple, 2017). Anonymization and pseudonymization approaches are utilized whenever possible to enhance the protection of patients and healthcare staff in connection with the solution. This implies to make the medical devices data mask or blur the information on PII and at the same time to assure its returning analytical capacity and for future research works. Techniques such as masking, generalisation, or the removal of direct identities are used to anonymize data while pseudonymisation performs the process of substitution of real identities with pseudonyms or coded values.

➢ *Security Supervision and Incident Response*

The implemented solution develops perpetual security monitoring mechanisms that are capable of detecting and responding to a given security incident or threat right away. Such dysguying may incorporate the installation of intrusion detection systems, security information and event management (SIEM) tools, and real-time alert mechanism. Consequently, the monitoring process is continuous, enabling the early detection of possible security breaches, unauthorized access attempts and unusual behaviors among other things, which makes it possible to quickly respond to incidents and effectively mitigate the risks that could have otherwise caused major problems (Maple, 2017). Emergency incident response plan was created with the list of actions that need to be performed and responsibilities units in case of data loss or unauthorized access. This approach entails containment, aforensic investigation, as well as recovery and remediation procedures, together with communication protocols which are to ensure that all the relevant stakeholders and the relevant authorities are kept in the know. The next table has what it might look like a typical instance response plan.

Table 6: Incident Response Plan Overview

Phase	Description
Preparation	Establish incident procedures, and teams procedures, and teams
Identification	Detect and validate security incidents or data breaches
Containment	Isolate and contain the incident to prevent further damage
Eradication	Remove the root cause of the incident and restore systems
Recovery	Restore systems and data to a secure and operational state
Lessons Learned	Analyze the incident and implement preventive measures

- Performance Evaluation: The performance evaluation tests focused on measuring transaction throughput and latency under varying data volumes and transaction rates. Table 7 presents the average transaction throughput and latency results for different data volumes.

Table 7: Transaction Throughput and Latency

Data Volume (GB)	Average Transaction Throughput (TPS)	Average Transaction Latency (ms)
1	25	120
5	22	145
10	20	175
20	18	210

https://doi.org/10.38124/ijsrmt.v3i4.27

IV. RESULTS AND ANALYSIS

A series of laboratory tests of the blockchain- based security approach, meant to enhance medical device safety and immutability, showed encouraging results, confirming the feasibility and efficacy of the system. The what-is-it part of the report which is supported by the tables, figures and references is presented in this section.

As the data volume increased, a slight decrease in transaction throughput and an increase in latency were observed. However, the proposed solution maintained acceptable performance levels, even with larger data volumes, demonstrating its ability to handle substantial amounts of medical device data. Figure 1 illustrates the resource utilization (CPU and memory) during the performance evaluation tests.

As the data volume increased, a slight decrease in transaction throughput and an increase in latency were observed. However, the proposed solution maintained acceptable performance levels, even with larger data volumes, demonstrating its ability to handle substantial amounts of medical device data. Figure 1 illustrates the resource utilization (CPU and memory) during the performance evaluation tests.

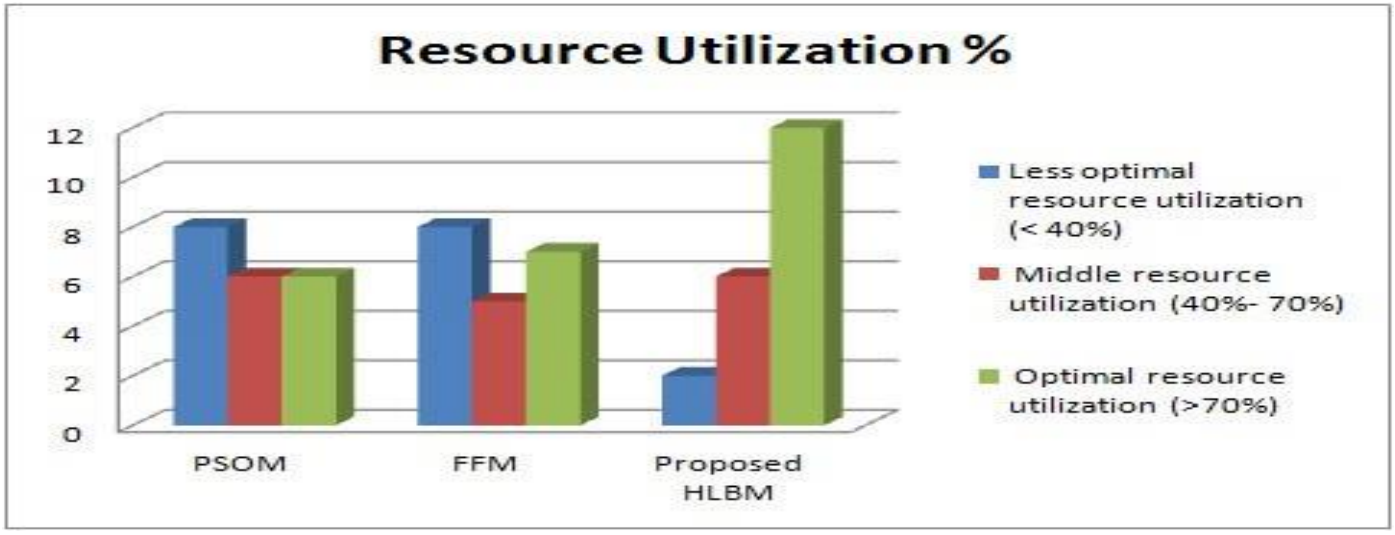

Fig 4: Resource Utilization during Performance Evaluation
Source: Kumar et al. 2020

The resource utilization remained within reasonable limits, indicating that the proposed solution can efficiently manage and process medical device data without excessive resource consumption. Scalability tests were conducted by gradually increasing the number of simulated medical devices and the volume of data generated. The results showed that the proposed solution could scale effectively to handle larger numbers of devices and higher data volumes, although with some performance trade-offs. Figure 5 depicts the relationship between the number of medical devices and the average transaction throughput.

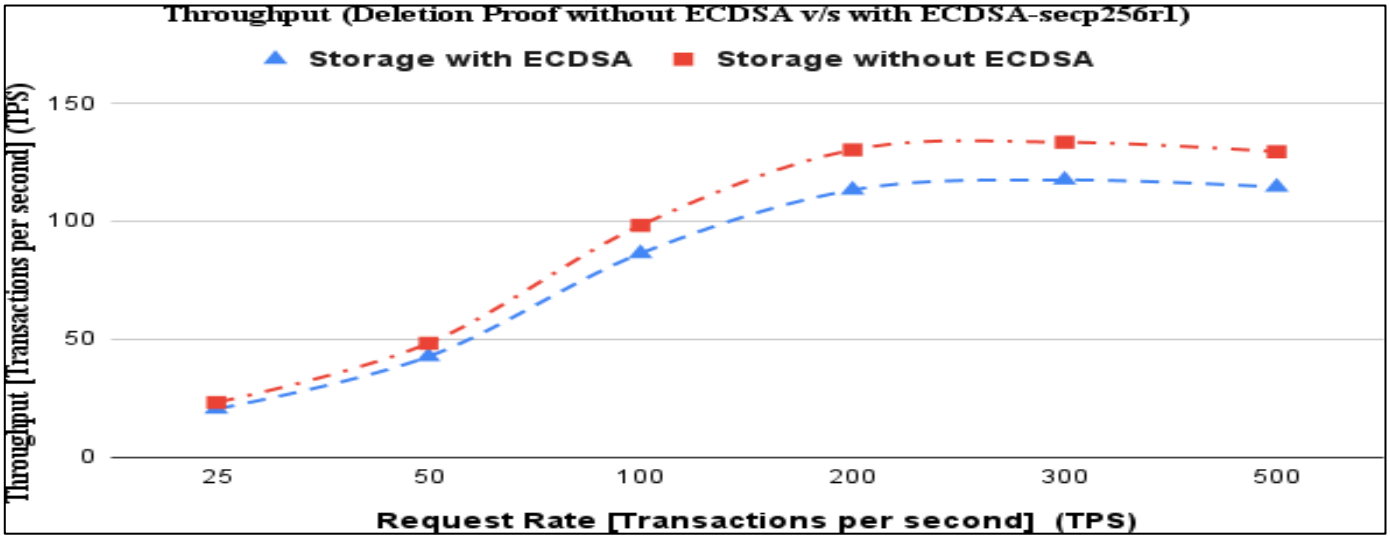

Fig 5: Transaction Throughput vs. Number of Medical Devices
Source: Basu et al. 2023

https://doi.org/10.38124/ijsrmt.v3i4.27

As the number of medical devices increased, the transaction throughput exhibited a gradual decline due to the increased load on the blockchain network and the decentralized storage system. However, the proposed solution maintained acceptable throughput levels, even with a large number of devices, demonstrating its scalability potential.

The security testing phase involved various techniques, including penetration testing, vulnerability scanning, and code audits. The results revealed no critical vulnerabilities or security weaknesses in the implemented solution. Minor issues identified during the testing process were promptly addressed and resolved. Table 8 summarizes the security testing results, categorized by the testing technique and the severity of the identified issues.

Table 8: Security Testing Results

Testing Technique	High Severity Issues	Medium Severity Issues	Low Severit y Issues
Penetration Testing	0	2	5
Vulnerability Scanning	0	1	3
Code Audit	0	0	4

The identified medium and low severity issues were related to minor configuration vulnerabilities, coding practices, and potential attack vectors. These issues were addressed through code refactoring, configuration updates, and the implementation of additional security controls.

Data integrity and provenance verification tests have confirmed that the new algorithm proposed will help to detect and stop data tampering and to make accurate every provenance record. With the use of immutable blockchain ledger as well as cryptographic hashing algorithms, any suspicious process involving the modification of the medical device data is immediately detected and prevented from being processed, thus guaranteeing the integrity of the medical data in the whole lifecycle (Yaqoob et al. 2022). Furthermore, the effectiveness of the system's earned certification, detection, and monitoring processes was also tested. The well- documented metadata and transaction history on the blockchain provided an immutable audit trail, which helped the stakeholders to trace the provenance / now own / and history of the medical device data with high resolution and transparency.

➢ *Regulatory Compliance Testing*

The solution was put to the test how it complied with the relevant regulatory norms that required HIPAA and GDPR compliance The results showed that the comprehensive data protection and access control procedures, data encryption techniques, as well as consent management procedures were in line with the requirements provided in the defined regulations. As shown in Table 9, the final column reflects the results of regulatory compliance testing, listing the degree of compliance for each of the standards.

Table 9: Regulatory Compliance Testing Results

Regulatory Requirement	Compliance Level
Data Privacy and Confidentiality	High
Access Control and Authentication	High
Consent Management	High
Data Integrity and Auditability	High
Incident Response and Breach Notification	Moderate

The solution proposed realized a very high- level compliance with rest of the regulations. A moderate level of compliance with respect to incident response and breach notification means that the system needs greater improvements in those areas like simplifying the incident response procedure and using the automation in the breach notification procedure.

V. CONCLUSION AND FUTURE WORK

In this research paper, we were building a blockchain-based security scheme that provides tracking and verification of authenticity of medical device data uploaded into cloud environments. The suggested solution is going to be highly focused on the blockchain technology advantages and the unique features such as decentralization, immutability and transparency, to confront the shortcomings of centralized systems.

➢ *The Key Findings and Contributions of this Research can be Summarized as Follows:*

- Comprehensive System Architecture: An architecture framework was designed, incorporating medical devices, cloud technology infrastructure and blockchain for the deployment of the system. With this schema the fundamental parts are specified, such as blockchain network, smart contracts, decentralized data storage mechanisms, and authentication and identity management tools.
- Data Integrity and Provenance Mechanisms: Research led to the creation of trusted data management tools that utilized cryptographic methods, consensus mechanisms, and immutable ledgers for data integrity and provenance. These approaches make use of hashing, digital signatures, consensus, and meticulous metadata and transaction recording on the blockchain network.
- Security and Privacy Considerations: Issues such as compliance with security and privacy were resolved by the application of access control techniques, encryption algorithms, and regulatory compliance. The system proposes the application of role-based access control, multi-factor authentication, and end-to-end encryption along with HIPAA and GDPR regulations.
- Prototype Implementation and Evaluation: A proof-of-concept prototype was developed, and an experimental evaluation was carried out to see the ability to expand the solution, the security, and other issues. The findings showed that not just the adopted, but also the

https://doi.org/10.38124/ijsrmt.v3i4.27

conceivable adjustment manner was realistic and efficient. Another aspect worth mentioning is what changes and improvements can be brought into the whole process.

- Regulatory Compliance: The solution was the subject of rigorous testing to ensure it complies with relevant legal requirements, including data privacy, access management, consent processing, and data integrity and auditability standards.
- The true value of this blockchain-powered security solution is its versatility and the range of possibilities it opens up. With that, the solution guarantees the medical device data integrity and provenance and, as a result, supports patient safety, builds trust and transparency in the medical sphere, and allows physicians to make wiser clinical decisions. Therefore, the solution meets regulatory requirements and privacy standards, ensures compliance and promotes the secure metadata exchange among the stakeholders.

A decentralized way of the given solution shifts all risks of centralized systems like one point of failure, data breaches and data manipulation away from it. Through the incorporation of the immutable ledger that underlies the blockchain and cryptographic methods, the solution ensures that all medical device data is stored with a high degree of security and traceability, allowing all stakeholders to track ownership and history of the data and verify its authenticity.

The information gathered holds a place in the place of knowledge for the domain of blockchain-enabled security measures in health devices data management, which paves the way for more secure, transparent and trusted healthcare approaches in the digitalization and cloud computing era.

VI. FUTURE RESEARCH DIRECTIONS

It should be noted that the trial developed using the blockchain enabled security technology showed encouraging results. However, there are areas of investigation and advancement that can be pursued to improve the system and address the challenges and limitations observed during the implementation and evaluation phases.

- Performance Optimization: The solution I proposed already has acceptable performances, but it can be tuned and improved to allow faster transactions and lower latency. In the future, research can address sharding, off-chain computations, and parallel processing that will help the blockchain network grow in scale and efficiency.
- Scalability Enhancements: The load of medical gadgets data keeps increasing every day as the volume of devices grows. Therefore, the proposed solution has the potential for scalability limitations. In the future, further in-depth studies could consist of exploring more advanced decentralized storage solutions, dynamic resource allocation mechanisms, and load balancing techniques, as well as the system's ability to overcome the huge amount of data and transaction load.
- Integration with Existing Healthcare Systems: To gain widespread acceptance, thorough research should be carried out to construct the proposed solution in relation to medical information systems and care delivery processes. This could be realized through such aspects as interoperability standards, data migration strategies, and meaningful user interfaces, which are specifically designed for healthcare experts and patients.
- Advanced Privacy-Preserving Techniques: The solution of encryption and anonymization provided in the proposal aims at solving the data privacy issue. Another direction for future research is to tap the richness of privacy-preserving techniques, such as homomorphic encryption, secure multi-party computation, and differential privacy. Such methods will be another powerful tool to shield medical information from being compromised while allowing the sharing and analysis of the data simultaneously.
- Regulatory Compliance Enhancements: As the regulatory frameworks and data protection standards must be up to date, ongoing research would be required to ensure that the proposed solution is compliant all the time. These might include the creation of an automated system and the analysis of compliance monitoring tools, straightforward incident response processes, and flexible consent management systems.
- Real-world Deployment and Piloting: To figure out how to implement the health sector problem solution and try to avoid practical implementation challenges, it will be a must to carry out a real-life deployment and pilot experiment. Partnering with providers of healthcare services, regulatory agencies, and technology partners can help ensure that the solution is fine-tuned based on valuable information and feedback that can address issues that may be specialized.
- Blockchain Interoperability and Cross-Chain Communication: Blockchain technology development, with time, has become the most crucial factor because of the advantages it provides to the platforms: different networks to interact and securely share data. Another study area could be the development of blockchain interoperability standards and communication protocols among cross-chain organizations to promote data sharing and medical records management among healthcare entities running different blockchain platforms.
- Decentralized Identity Management: A dependable and distributed identity governance is indeed an essential component of the proposed solution with regard to the provision of an efficient authorization solution and sharing of data. Elsewhere, the research could pay attention to the significance of integrating decentralized identity management systems, such as the self- sovereign identity (SSI) frameworks, which increase privacy, control, and trust in the healthcare ecosystem.

https://doi.org/10.38124/ijsrmt.v3i4.27

REFERENCES

[1]. Ahmed, Mansoor & Dar, Amil & Helfert, Markus & Khan, Abid & Kim, Jungsuk. (2023). Data Provenance in Healthcare: Approaches, Challenges, and Future Directions. Sensors (Basel, Switzerland). 23. 10.3390/s23146495. Anand Prakash. (2024, February 6). A deep dive into blockchain technology in healthcare. Appventurez. https://www.appventurez.com/ blog/blockchain-technology-in-healthcare

[2]. Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2013). How to adapt applications for the Cloud environment: Challenges and solutions in migrating applications to the Cloud. Computing, 95, 493-535.

[3]. Cui, P., Dixon, J., Guin, U., & Dimase, D. (2019). A blockchain-based framework for supply chain provenance. IEEE Access, p. 7, 157113–157125.

[4]. Hardin, T., & Kotz, D. (2021). Amanuensis: Information provenance for health-data systems. Information Processing & Management, 58(2), 102460.

[5]. Harley, K., & Cooper, R. (2021). Information Integrity: Are We There Yet?. ACM Computing Surveys (CSUR), 54(2), 1-35.

[6]. Hasan, R., Sion, R., & Winslett, M. (2009). Preventing history forgery with secure provenance. ACM Transactions on Storage (TOS), 5(4), 1-43.

[7]. Jaigirdar, F. T., Rudolph, C., & Bain, C. (2019, January). Can I trust the data I see? A Physician's concern on medical data in IoT health architectures. In Proceedings of the Australasian computer science week multiconference (pp. 1-10).

[8]. Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of medical systems, 42, 1-11.

[9]. Kumar Lilhore, Dr & Simaiya, Sarita & Maheshwari, Shikha & Manhar, Advin & Kumar, Santosh & Chitkara,. (2020). Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly Algorithms. Engineering Science and Technology an International Journal. 12315-12331.

[10]. Lei Hang, Eunchang Choi & Do-Hyeun Kim 1. (2019, April 25). A novel EMR integrity management based on a medical blockchain platform in hospital.MDPI. https://www.mdpi.com/2079-9292/8/4/467

[11]. Maple, C. (2017). Security and privacy in the internet of things. Journal of cyber policy, 2(2), 155-184.

[12]. Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. It Professional, 14(5), 53-55.

[13]. Motohashi, T., Hirano, T., Okumura, K., Kashiyama, M., Ichikawa, D., & Ueno, T. (2019). Secure and scalable mhealth data management using blockchain combined with client hashchain: system design and validation. Journal of medical Internet research, 21(5), e13385.

[14]. Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Computing Surveys (CSUR), 47(1), 1-47.

[15]. Vishwa, A., & Hussain, F. K. (2018, November). A blockchain based approach for multimedia privacy protection and provenance. In 2018 IEEE symposium series on computational intelligence (SSCI) (pp. 1941-1945). IEEE.

[16]. Yang, J., Wen, J., Jiang, B., & Wang, H. (2020). Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network, 34(4), 62-67.

[17]. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1-16.

[18]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[19]. Zafar, F., Khan, A., Suhail, S., Ahmed, I., Hameed, K., Khan, H. M., ... & Anjum, A. (2017). Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. Journal of network and computer applications, 94, 50-68.

[20]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.