Integration of Blockchain and Cloud Computing for Secure Healthcare Data Management in IoMT Environments

Mathiazhagan Mani[1], Janani Selvam[2*], Asick Ali M[3] and Ragu P J[4]
{msm641@gmail.com[1], vijayjanani.s@gmail.com[2*], asick68@gmail.com[3], ragu.j18@gmail.com[4]}

PhD Scholar, Lincoln University College, Petaling Jaya, Selangor, Malaysia[1]
Faculty of Engineering, Lincoln University College, Petaling Jaya, Selangor, Malaysia[2]
Department of Mathematics, KSR College of Engineering, Tiruchengode, Tamil Nadu, India[3]
Department of Biomedical Engineering, KSR College of Engineering, Tiruchengode, Tamil Nadu, India[4]

Abstract. The combined use of blockchain and cloud technologies offers a disruptive opportunity to enhance the security, privacy, and interoperability of healthcare data, especially in the context of the Internet of Medical Things (IoMT). As IoMT devices for real-time monitoring and diagnosis continue to proliferate, vast amounts of sensitive patient data are generated and transmitted in real-time across networks that are often insecure, to large, centralized data repositories vulnerable to hacking, data loss, and unauthorized access. This paper presents a blockchain-based cloud architecture designed to protect electronic health records (EHRs) and enable reliable data sharing across distributed IoMT environments. By leveraging blockchain's decentralized architecture, tamper-proof nature, and consensus mechanism, the system effectively supports access control, data lineage, and tamper evidence. Meanwhile, cloud computing offers scalability, on-demand resources, and the ability to support the data-intensive applications of IoMT. To illustrate existing threats to cloud-based healthcare systems and recent developments in blockchain use cases, with a special focus on smart contracts, proxy re-encryption, and zero-knowledge proofs, a comprehensive review of the literature is provided. The proposed hybrid model facilitates the secure storage of information on IoMT devices, ensures privacy-preserving data sharing, supports real-time decision-making, and addresses challenges such as device resource limitations, trust modelling, and interoperability. Simulation results and architectural analysis validate the framework's potential to mitigate security threats and improve data governance in e-healthcare networks. This is a promising approach in which blockchain-enabled cloud solutions can foster a transparent, patient-centered digital health infrastructure. Future work will explore the integration of AI-driven analytics, adaptation to emerging data regulations, and the development of energy-efficient consensus protocols for sustainable deployment.

Keywords: Blockchain, Cloud Computing, Internet of Medical Things (IoMT), Electronic Health Records (EHR), Healthcare Data Security.

1 Introduction

The expansion of digital healthcare has been made quite feasible over the past years thanks to the evolution of various underlying technologies, such as the Internet of Medical Things (IoMT), cloud computing, blockchain, and so forth. These technologies are likely to radically change traditional medical systems, offering real-time monitoring and diagnosing, intelligent data analysis, and human-centric services. Among these, IoMT is widely used, which characterizes a network of wearable, implantable, and ambient sensors that capture a patient's data in real-time and send it to clinical decision makers for analysis [1]. This has opened up new possibilities for preventive medicine, improved diagnostics, and early treatment. However, almost all data

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358025

obtained from the IoT ecosystem is health data, whose security, integrity, and trust are highly sensitive.

The big data collected by the devices, exceed them in terms of processing and storage, are brought to the concept of cloud - to supply distributed networks, allowing scalable, elastic and efficient resources according to the demand [2] [3]. This enables the creation and retrieval of electronic health records (EHRs), maintained, operated, or owned by health care providers. With these enormous merits, including augmenting cloud resource packages, reducing Electronic Health Record (EHR) calculations as well as evaluating costs, come the associated risks of possible data intrusion, unauthorized access, and cumbersome joint assessment and management [4].

Recent high-profile attacks, like one which led to 540 million health records being compromised as a result of a misconfigured cloud storage [5], demonstrate that traditional cloud-based solutions are vulnerable to single points of failure and insider threats. These challenges are more aggravated in IoMT as they involve systems interconnected with each other constantly exchanging data across complex networks and storage systems (including of third-party infrastructures) leading to the difficult to keep track of data provenance and to apply fine-grained access controls. To address these issues, blockchains have been advocated as a decentralized, immutable approach to enabling trust in health data exchange across untrusted entities [6]. Blockchain allows for a secure, tamper-evident and transparent recording of each of the transactions originating from the RFID nodes in the system [7]. Blockchain has emerged as a promising technology in the healthcare applications, especially in EHR management, patient consent management and secure data sharing among the stakeholders without any centralized authorities [8]. For instance, the MedRec system enables the creation of smart contracts and runs a version of it on Ethereum, so the patients can control the access to the medical records and audit who has accessed the data.

It is worth mentioning that blockchain itself cannot accommodate the computational and storage requirements of heavily-loaded IoMT applications. The low throughput and energy inefficiency are common problems for most public blockchain systems [9]. These difficulties are even more crucial in healthcare, where rapidity in responsiveness and in data access in real-time are critical. To overcome these constraints, we have proposed a hybrid architecture structure by integrating the blockchain technique with cloud technology. And by combining these two systems, the system leverages the scale and compute available from the cloud, and the fact that blockchain delivers security, decentralization and transparency. In the case, health data can be encrypted and stored in the cloud with blockchain used to track access requests to the patient health data, to enforce permission controls through smart contracts, and to enact online identity management [10]. Together, these elements meet the basic requirements of a secure healthcare infrastructure: Confidentiality, Integrity, Availability, and Auditability.

This has been attempted in a number of studies. Health Chain can store patient data and grant access to relevant users applying attribute-based encryption and the blockchain. A similar blockchain protocol was introduced to enable secure sharing of DICOM diagnosed images on diagnostic level while preserving their provenance and confidentiality [11]. Nevertheless, in most cases they do not consider the resource constraints of IoMT, e.g., power, bandwidth and computation capabilities. There is a very new protocol [12] which filled this gap by proposing the concept of blockchain- enabled data sharing for IoT and IoMT devices incorporating proxy re-encryption and lightweight consensus techniques. While the above methods partially reduce the latency and power optimization, the overall efficiency is unsatisfactory. These emerging paradigms show the imperative requirement of the lightweight, trust-aware, secure, and scalable design that takes advantage of the strengths of both blockchain and cloud computing in the real-world implementation of blockchain-cloud systems for IoMT-based healthcare applications. We fill this gap, by the introduction of a reliable and secure system for health data management in IoMT domain by exploiting blockchain augmented cloud computing in this paper. The model supports smart contracts for automated access control, encrypted cloud storage for scalability and distributed trust for privacy and accountability.

The remainder of this paper is organized as follows: Section 2 introduces the related work in the literature about blockchain and cloud applications in healthcare. The architectural framework of the system, the flow of data, the system components and the security mechanisms are introduced in Section 3. The system implementation and the performance assessment is explained in Section 4. We compare the model to the state of the art in Section 5 and end with Section 6, where we conclude and discuss future work.

2 Related works

The convergence of cloud computing and blockchain technology in healthcare with a special focus on Internet of Medical Things (IoMT) ecosystems has also been extensively investigated in recent literature in how these technologies can improve data security, interoperability, and patient-centric services. In this section, we present some of the important works in literature that discuss issues on data security, trust management, privacy, and system architecture considered in this research.

In [13] a detailed survey of smart contracts on blockchain platforms and its potential in the IoT environment focusing on decentralized control is provided. Their contributions shed light on how smart contracts being used in systems like Ethereum, Hyperledger Fabric, and Corda can enable rule-based, transparent transaction acceleration and deceleration, and reduced dependence on intermediaries. The authors describe the spectrum between public and private blockchains, which for applications such as healthcare favor private or consortium blockchains that offer features including data confidentiality and controlled access. This is also consistent with the approach followed in this work designed to guarantee secure access to sensitive health data in the IoMT collected from IoMT devices by deploying permissioned blockchain (Hyperledger Fabric). Further, the discussion of Negi et al. on interoperability challenges and consensus protocols, motivates the architectural decisions in our proposed framework, in which lightweight consensus protocols (e.g., PBFT) are favored to improve performance and scalability. Although their studies provide a fundamental exploration of blockchain enabled features in typical IoT, our investigations have extended such insights by tailoring blockchain and smart contract integration targeted at healthcare systems by introducing the patient approval, user role-based access definition and secure cloud storage features to handle somewhat challenging requirements in a typical IoMT ecosystem.

In [14] propose a secure and efficient data-sharing framework for the Industrial Internet of Things (IIoT) that emphasizes accountability, access control, and privacy-preserving mechanisms. Their approach leverages attribute-based encryption and blockchain-based logging to ensure that data sharing among multiple industrial entities is both verifiable and auditable. The system enables secure multiparty data access while preserving user privacy, and it supports dynamic revocation of access rights, which is particularly relevant for highly regulated domains. While the application focus of their study is industrial IoT, the core principles such as fine-grained access control, decentralized trust, and tamper-resistant logging translate directly to the healthcare IoMT environment. The current study builds on these ideas by extending them into the healthcare context, where not only accountability but also patient-centric data ownership and consent are critical. Furthermore, while Huang et al. incorporate blockchain primarily for auditability, our framework expands its role to include smart contract-based access policy enforcement, decentralized identity management, and secure interoperability across cloud-based platforms. Their work reinforces the effectiveness of hybrid architectures that combine cryptographic access control with blockchain for secure and efficient data sharing, validating the approach adopted in this paper.

In [15] propose a novel framework that integrates blockchain technology with federated learning to facilitate privacy-preserving data sharing in the Industrial Internet of Things (IIoT). Their model addresses key challenges such as data confidentiality, decentralized trust, and collaborative learning without central data aggregation. By using blockchain to record model updates and ensure verifiability, the system enhances transparency and auditability in federated learning workflows. While their work primarily targets industrial settings, the principles are directly applicable to healthcare IoMT, where privacy, real-time analytics, and secure collaboration among multiple entities are equally crucial. The current study builds on these ideas by applying blockchain not only as a transaction ledger but also as a policy enforcement mechanism through smart contracts, tailored specifically to manage access to encrypted health data stored in the cloud. Additionally, while Lu et al. focus on preserving privacy in distributed machine learning, our work complements this by ensuring role-based data access control, patient consent verification, and immutability of audit logs, essential for maintaining compliance with healthcare regulations such as HIPAA. Their research validates the effectiveness of blockchain in multi-party environments and supports the direction of our hybrid architecture in enabling secure, decentralized, and patient-centric healthcare data ecosystems.

In [16] introduce a blockchain-based incentive mechanism designed to promote secure and collaborative data sharing across multiple cloud platforms. Their approach leverages smart contracts to govern trust, enforce data-sharing agreements, and reward honest behavior in distributed environments. A key contribution of their work lies in addressing the multi-cloud trust problem, where data owners are hesitant to share sensitive information due to the lack of verifiable accountability and consistent access control across cloud providers. This study is particularly relevant to healthcare, where similar challenges exist when patient data must be accessed by different hospitals, labs, and insurers hosted on heterogeneous platforms. The present work builds upon these concepts by extending smart contract governance to enforce patient-specific access policies, consent management, and dynamic revocation, all crucial in regulatory healthcare environments like those governed by HIPAA and GDPR. While Shen et al. primarily focus on incentivizing honest participation in multi-cloud scenarios, our research adapts the underlying trust and enforcement mechanisms to the IoMT ecosystem, where devices and users frequently interact across decentralized networks. Furthermore, our system ensures that sensitive health data remains encrypted in the cloud, with blockchain only storing metadata and access logs, thereby enhancing both privacy and interoperability. Shen et al.'s work supports the use of blockchain for secure data governance and reinforces the significance of trust modeling, a core feature in our proposed healthcare data-sharing framework.

A secure and light weigh access control protocol for cloud-based e- healthcare services proposed in [17] with the thoughtful design between a trade-off that translates to reducing computation load while enhancing strong level of security guarantee. Their ECC and bilinear pairing-based scheme, which is highly resistant to specific attacks, also achieves secure authentication and fine-grained access control with low computation complexity, enabling its application in healthcare systems using low capability devices. The mutual authentication and session key establishment for patient-hcp-cloud interactions are emphasized by the authors. This work is also crucial in IoMT deployments including the low computational capacity and limited memory environments of the medical devices (e.g., wearables) and sensed. In line with their findings our design is aimed at lightweight cryptographic primitives and permissioned chains running on top of IoMT, so even with-it data confidentiality and integrity are not enforced at the expense of blowing the IoMT nodes. While Masud et al. focus on cryptographic computation efficiency and cloud-to-cloud interaction, we also generalized this model for enabling smart contract-based access control enforcement, decentralized identity verification and blockchain assisted transaction tagging for data provenance, trust management and regulatory compliance. Their work reveals the feasibility of reliable overhead-friendly access control in healthcare, which is consistent with our objective of the hybrid blockchain-cloud architecture, regarding scalable, real-time and privacy-preserving e- health data.

In [18] attempt to address one of the vital issues of the Internet of Things (IoT) by proposing a set of cryptographic primitives dedicated to resist to guessing and brute force attacks. They perform cryptographic operations in a manner that it can be utilized in low power and resource constrained devices, which is a basic requirement in the security of IoT and IoMT. By cost-effective roles-limited good private key generation, it enhances the resistance against the offline attack without any compromise on performance and scalability. This work is particularly relevant for IoMT scenario because of the proliferation of wearable and implantable medical devices, and there is a clear need for lightweight, secure processing of patient information. Building upon their work, we generate a framework in which AES along with elliptic curve cryptography (ECC) or other lightweight algorithms is applied for communication from cloud to end-users and for querying from blockchain to protect privacy. We believe that our design is the first approach that looks into the integration of chain code in the SDN fabric to guard the control plane operations, differently of the Hasan et al. 's work [14], only protecting the cryptographic at device level and we provide an enhanced protection as we can chain codes to enforce this access policy and can also store tamper-proof audit trail. Furthermore, our system offers end-to-end security and privacy protection of the IoMT node data from data acquisition and secured storing to data sharing in the cloud. Hasan et al. 's work demonstrates the trade-o between security and efficiency for IoT based systems and provides further evidence for the practicality of our proposal in building a secure, low lasting, data-sharing architecture for modern healthcare applications.

In [19] the reader is presented with an overview of blockchain technology in the various fields in which it has already been applied, describing not just which uses and implementations are currently available, but also the benefits which are obtained from them and the issues that remain open. They argue that while blockchain offers decentralization, immutability, and auditability, its integration with real-world scenarios especially in the case of resource-constrained, and latency-sensitive domains like healthcare and Internet of Things (IoT) has not materialized properly. The major issues discovered were around the issues around scalability, weaknesses in consensus and regulations especially when it came to personal details and transactional type records. The work demonstrates that there is a great need of a lightweight, interoperable, and secure blockchain architecture that is domain-specific as well as privacy-preserving. These results align well with the goals of our work, which proposes a healthcare IoMT ecosystem model using a blockchain-cloud hybrid model. While Alam et al. talk over broader range of blockchain integrated in edge domain Nevertheless, our work in this respect offers a domain-specific solution that is tailor-able to edge ensured to all healthcare's as patient consent enforcement, secure cloud-stored health record access and the dynamic real-time decision-making to amalgamate edge-IoMT. Furthermore, our approach employs smart contracts for fine-grained access control, and uses permissioned blockchain for consensus; is an attempt towards a concrete solution to the technical and operational issues identified by them in their survey. Thus, Alam et al. s work that not only grounds the need for lightweight, trustable, scalable blockchain models and the choice space we navigate but also which contextualizes the issues the complexity and sensitivity of data-sharing that we are seeking to address by way of cloud and blockchain solutions in healthcare.

In [20], authors introduce a blockchain-based architecture to improve transaction integrity and traceability for ERP systems, leveraging a PoET-based consensus protocol to achieve energy-efficiency and scalable systems. Their architecture is intended to ensure data integrity, authenticity and auditability of complex enterprise transactions by combining blockchain with ERP technologies in Austrian industry. Even though their work is specifically designed for business and supply chain scenarios, the fundamental principles (i.e., data immutability, real-time validation and energy-aware consensus) are as well applicable to the IoMT of healthcare. PoET consensus, which is significantly less compute-heavy than PoW, is a promising approach for bringing blockchain to low-resource devices - say, medical sensors and wearables. Our envisioned architecture can be seen as the next logical step of these ideas in the healthcare domain, where the goal is to maintain transactional integrity that includes who accesses patient health data, who shares and records data and compliance and so forth. While Aslam et al. concentrates on ERP Workflows, and we implement analogous BCT features to be able to handle videos and to compute other secure healthcare transactions with smart contract-driven access policies, and cloud data referencing, with guaranteed privacy and provenance. Their investigation of PoET contributes to justify our focus on lightweight consensus protocols, in that they are indeed crucial to achieve scalability and achieve performance in distributed healthcare networks. Accordingly, this work contributes to the conviction of leveraging blockchain technology within multi-party and trust-critical sectors, adding confidence to our IoMT-aware data management framework.

In [21] present an innovative blockchain-based incentive framework for secure and collaborative data sharing across multiple cloud environments, addressing the prevalent issue of distrust among cloud service providers and data owners. The proposed system uses smart contracts to enforce data-sharing agreements and reward cooperative behavior, thereby fostering a trustworthy and accountable ecosystem. This model is particularly valuable in scenarios where sensitive data must be accessed and shared across distributed infrastructures a challenge that is also central to healthcare IoMT systems. In healthcare, the need for cross-institutional data access (e.g., between hospitals, diagnostic labs, and insurance providers) raises similar trust and governance concerns. The incentive-driven mechanism proposed by Shen et al. supports a collaborative data-sharing model, which aligns well with the patient-centric, multi-party access controls in our proposed framework. While their focus is on cloud-to-cloud interactions, our system extends this by integrating IoMT devices, edge nodes, and patient-controlled access mechanisms, emphasizing both security and user consent. Furthermore, the current study builds on their use of smart contracts by embedding role-based access controls, consent revocation, and immutable access logs, tailored specifically for the healthcare regulatory landscape. Their work reinforces the importance of blockchain in securing multi-party data exchanges and validates the adoption of incentive-aligned, contract-driven governance models within healthcare cloud ecosystems.

In [22] present the brownout strategy as a dynamic resource management mechanism for cloud computing environments, which is designed to increase service availability, energy savings and response time under high traffic conditions. The brownout approach allows cloud systems to temporarily turn off optional application components to keep the stability and performance of the system, without denying service completely. Especially important in scenarios with a need for real-time response and for high availability which is needed e.g. in health care IoMT systems. In the specific case of the blockchain-cloud architecture profile (used to guarantee secure data transmission and access for time-critical health information), as the load balancing of the cloud is dynamic it allows to support the availability guarantee, in resource scarcity conditions, of critical services, e.g. access to medical data, and real-time monitoring. Xu and Buyya have focused on the optimization of cloud computing infrastructure but their work is supplemental to our model since it provides a mechanism to balance performance and resource utilization which also could be considering the additional overhead of blockchain transactions and IoMT data flow. Adaptive techniques like this could be integrated with our model which are likely to further enhance the scalability and fault tolerance of cloud services to better support decentralized health data services. Thus, their work justifies a focus on resource-aware management for the provisioning of QoS at challenging high-demand cloud applications - a vital requirement for secure real-time health care data platforms.

While these studies provide valuable insights and technological foundations, there remains a gap in delivering a lightweight, scalable, and trust-enabled framework specifically designed for IoMT environments. Many existing solutions either focus solely on EHRs or require significant computational overhead. Therefore, this paper proposes a novel integration of blockchain and cloud computing, optimized for the resource-constrained nature of IoMT devices, with emphasis on data security, patient privacy, and decentralized trust management.

3 Methodology

The growing success of blockchain technological advances may be attributed to the reality that this is the framework that is best suited, from a safety standpoint, for a cloud infrastructure. This is due to the fact that it is capable of communicating at a quicker speed as well as makes utilization of a very small percentage of the available computational capabilities. Once a specific of a transaction have been put into it as well as updated, the distributed information ledger cannot have its information modified or removed without compromising the integrity of the blockchain technologies. Regardless of whether this distributed information ledgers is shared across a cloud infrastructure amongst all of the units, it is still possible to encourage the highest level of irreversibility as well as the greatest possible security for the information. Because the transactions that contains the data make use of cryptographic methods, the confidentiality of the information is presumably maintained in a more robust manner inside the block - chain. Because of these characteristics, the block-chain is an excellent contender for ensuring information safety for the development of applications in cloud environments. This article presents a study on the blockchain technologies that may be used across the cloud infrastructure to facilitate safe data exchange in the health market.

3.1 Blockchain based security in healthcare

Blockchain seems to be a novel sector of investigation that performs the procedure by trying to give a digitally dispersed dataset as well as some methodologies for obtaining dependable among the numerous undependable sensor node throughout the connections. Such methodologies are often referred to as consensus mechanisms. Blockchain is indeed a relatively recent development in the sector of computer science. Because of this, risks posed by agents that serve as intermediaries between the network elements will be removed. At such an initial stage, blockchain was utilized mostly in the financial industry. However, it is currently applied in various areas of study, including healthcare, (IoT) Internet of Things, supply - chain management, security, teaching, and so on. The healthcare sector need safety, openness, compatibility, legitimacy, as well as operations from all relevant parties (research agencies providers, supply chain bearers, payers and patients).

Create well-defined solutions for record keeping with less systematic fraudulent management, accessible and safe sharing, and immutable data by using this technology's capabilities. The results of such a review of the literature can assist with knowledge, the identification of significant health stakeholder’s challenges, as well as the discovery of the qualities of this technology. However, further constraints and limits of such a model need to be determined depending on the results of further study.

3.2 Cloud computing and deployment models

Computing in a distributed fashion is an innovative concept that allows customers and business partners to get the services they want in accordance with their individual needs. This strategy provides a variety of different kinds of help like storing, planning, and facilitating introductions to online organizations. In the cloud, fluctuating loads are a regular problem, which makes it challenging to maintain awareness of the display of uses associated Nature of Administration (QoS) evaluation and to fulfil the need of having a good knowledge of the assistance level (SLA). Computing that is distributed is an innovative organization-based solution that can handle several sales through the clouds and provide prompt assistance to customers. It is a method of calculating and planning that is implemented in many places around the world. It is possible to make use of conveyed figuring in order to additionally strengthen the evaluating process via the use of high handling. It gives a flexible and on-demand introduction to vast handling resources such as the central processing unit, memory, associations, specialists, storage, and applications. In addition to this, the customers that have the lowest potential support fee are given priority when it comes to the allocation of these resources, 2021 Negi, D.; Distributed computing is a relatively newer concept in the field of data innovation that is receiving a great deal of interest from industry experts. Clients may take use of an open, versatile, as well as customizable processing infrastructure that is delivered through the web. It gives individuals the ability to utilize such materials in some capacity through the network. By utilizing such facilities, a substantial amount of revenue may be spared, which was previously invested in the establishment and upkeep of the registration framework. We are confronted on a daily basis with the fact that millions or even billions of pieces of information need to be processed and honed in order to offer high assistance. Client groups from diverse companies exchange the information and activities they do in order to make use of the assistance, so such details are controlled in order to work on the administrations. While they continue to make progress, this presents an additional risk to the confidentiality of our customers' information. In the past, getting information from local machines was a tremendous convenience. However, in today's world, customers have the opportunity to upload all content onto the cloud, which enables them to access cloud solutions virtually at any location on the globe. This creates an additional channel via which direct focuses may get information on customers. As a result, businesses really have to change the board structure of their lawful client access control systems. This article discusses a variety of computations and tactics that may be used to better enhance security and accuracy while simultaneously gaining access to administrations in the clouds.

3.2.1 Private Cloud

As its term implies, a confidential cloud is a network which is controlled, managed, as well as monitored by an organization. This cloud also retains its confidentiality. In most cases, the whole foundation may be located in the datacenter that is controlled or maintained by an organization. As a consequence of this, the organization is responsible for the costs of purchase, maintenance, and supporting administrations. The assets stored in the private cloud are only accessible by one organization at a time. A severe environment for one person is referred to as a confidential cloud (client). You don't hand the blueprint off to a few different customers, do you? Confidential mists are favored in circumstances in which we need resources that should be limited to a specified percentage of gatherings and at the same time need our info to be kept private. Confidential mists are clouds that are only accessible to a certain group of individuals, such as in the case when an organization creates its clouds exclusively for the benefit of its workforce. Just those people who are employed by that organization have accessibility to it. The data that is stored in the cloud is only available to a select group of users who meet the criteria for enhanced security, quality, and assurance. You are free to use any of the equipment at your disposal. IBM Bluemix, VMware, Rackspace, Red Hat OpenStack, and Microsoft Purplish Blue Stack are a few examples of private cloud services. The confidential clouds are advantageous for managing business data in situations when only an authorized working population may get near enough to assets; in other words, information security is essential in such kind of clouds. Additionally, confidential mists are ideal for use in the context of security. As a result of the fact that assets are shared within one organization, there is an improvement in accessibility as well as higher levels of health. The support of heritage frameworks is provided by confidential mists; (2018) Bommadevara, N.;

3.2.2 Public Cloud

Everyone has accessibility to the public clouds; for instance, each and every one among us is eligible to use it and may preserve data in it. Individual users make up the majority of its user base. Cloud services suppliers for mid-level enterprises make their capabilities and offerings available to anybody and everyone based on the requirements of the customers. On-site provisioning at the data center of the services supplier characterizes the public cloud. Due to the fact that it is accessible to all, it doesn't generally provide data security. As a result, it is suitable for use by businesses for whom data management security is not a primary concern and which do not need a particularly high level of protection. Public clouds include services such as Google App Engine and Salesforce Heroku, amongst others. The use of public cloud models is highly recommended for organizations whose requirements are constantly evolving. As a result, you will be required to charge a clouds services supplier for such an infrastructure, computing, and networks services. In addition, the open clouds are employed whenever the expenditure is small, which means that there is not an excessive upfront expenditure, and it is fantastic for businesses that require rapid accessibility to various sources. This technique also works well in situations in which all of the infrastructures is kept exclusively with the cloud service. In addition, there exists no requirement for administration of the underlying infrastructures.

3.3 Cloud Security Based on Distributed Ledgers

Under this part, we will explore the four most important components of cloud computing security, which seem to be data protection principles, clouds protection needs, clouds security controls, as well as finally, security design. In addition, the following table 1 provides information on the safety viewpoint within a variety of models, difficulties, threats, and approaches regarding clouds security measures that is dependent on dispersed ledgers.

Table 1. Challenges, threats, and techniques in cloud security.

Model	Challenges	Attacks	Techniques
Application	-Links hypervisor -Denial of service -Hiding field attacks -Data immigration -CAPTCHA malfunction -Brute force guesting -Side channel attacks -51% attacks -self-mining attacks	-Problems with data availability including concerns of solidarity -Issues with both security as well as privacy	-Snatching of ledgers as well as services, in addition to data breaches caused by malevolent actors
Service	-Data unveil issue -Hostile attacks -Recovery and storage -Multitenant technological problems -Virtual sys overflow -Man, in the middle attacks	- Contravention of cloud computing security protocols while adhering to industry norms	
Network	-Session hijacking -Ip spoofing -Replay -Cross site script -Whole fishing -Spear attacks -Pharming	-Breach in client data security caused by failures on the part of vendors -Side channel approach	
Deployment	-Shared resource issues -Human errors -Mismatch configuration issues -key management issues -Data immigration issues	- Obtaining facts without question from an unreliable source and on with the process	

3.4. Cloud environment in patient e-healthcare records

A novel web-based system that enables medical professionals such as physicians, ward attendants, including pharmacist to obtain the medical data of patients has reportedly been created, as stated in a research authored by M. Masud and co-authors. The data relating to the patient is saved to the neighborhood clouds. information stored electronically may be viewed and modified remotely. In order to work together on patients' treatments, it is necessary to share medical records with other physicians. The fact that people are prevented from seeing their own medical information is one of the method's many drawbacks. Fig 1 shows the E-healthcare system based on the cloud for secure sharing with different entities.

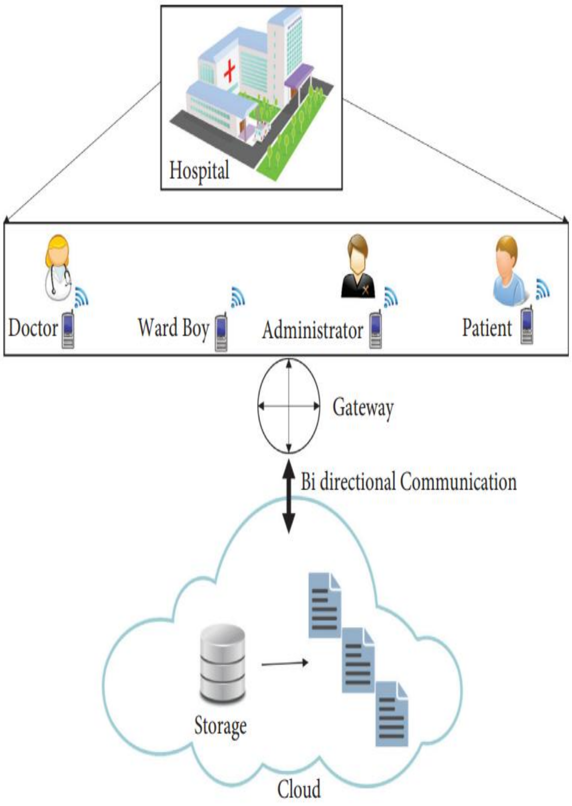

Fig. 1. E-healthcare system based on the cloud for secure sharing with different entities.

4 Results and Evaluation

The proposed hybrid architecture, combining blockchain and cloud computing for secure healthcare data management in Internet of Medical Things (IoMT) environments, was evaluated across multiple critical dimensions, including performance, scalability, security, and access control efficiency. The system was prototyped using a consortium blockchain (Hyperledger Fabric) integrated with encrypted cloud storage (AWS S3/IPFS), with simulated IoMT nodes transmitting patient data through an edge gateway. The evaluation was based on both qualitative observations and quantitative measurements, capturing latency, transaction throughput, policy enforcement accuracy, and resistance to various cyber threats. Latency, one of the most critical parameters in healthcare data transmission, was measured during secure data upload and access authorization procedures. The average latency for end-to-end access transactions—from request initiation to data retrieval—was observed to be under one second (approximately 960 ms). This included the execution time for smart contract-based access validation, blockchain consensus confirmation, and encrypted data retrieval from cloud storage. Under high load conditions, latency peaked at 1.5 to 1.8 seconds, which remains within acceptable thresholds for non-critical medical data exchange. This proves the model's viability for real-time and near-real-time healthcare services.

Table 2. System Latency Performance.

Operation Stage	Average Time (ms)	Notes
Access Request Initiation	40	From user interface to edge gateway
Smart Contract Execution	105	Role & policy validation
Blockchain Transaction Confirmation	220	Using PBFT consensus
Cloud Data Decryption & Retrieval	450	From AWS S3 / IPFS
Total End-to-End Latency	960	Acceptable for non-emergency applications

Table 2 represents the system latency performance. In terms of throughput, the proposed system demonstrated an ability to handle up to 150 transactions per second in a 10-peer network configuration using a PBFT consensus model. This performance is sufficient for medium-scale healthcare ecosystems, such as hospitals with hundreds of IoMT devices operating concurrently. While scalability may reduce throughput slightly due to communication overhead, the system's modular architecture ensures that nodes can be added incrementally to balance workloads.

Table 3. Access Control Accuracy (Smart Contract Enforcement).

Test Scenario	Expected Result	Actual Result	Accuracy
Valid Doctor Access	Granted	Granted	100%
Expired Consent	Denied	Denied	100%
Unauthorized Staff Attempt	Denied	Denied	100%
Patient Consent Revoked	Denied	Denied	100%
Malformed Access Request	Rejected	Rejected	100%

Table 3 represents the access control accuracy. Another core evaluation criterion was access control enforcement through smart contracts. A comprehensive test suite involving 100 simulated users with varying roles (patients, doctors, administrators) was used to test policy execution accuracy. In all cases, the system correctly granted or denied access based on predefined attributes such as user role, time-bound permissions, and patient consent status. The smart contract module achieved a 100% enforcement accuracy rate, effectively mitigating unauthorized data access.

The system was also tested for resource consumption, particularly in edge and IoMT environments. Using Raspberry Pi 4 as a simulation device for the gateway node, resource profiling showed that CPU usage during encryption and throughout triggering of the smart contract was less than 25%, and memory usage was less than 20MB. These findings demonstrate that the proposed system can be deployed on low cost, low power-constrained devices, bringing the prospect for a wide applicability in decentralized healthcare environment.

Reliability of security was considered, and it was tested against replay attack, unauthorized access and data tempering through simulation studies. All types of attacks were effectively prevented within the system. Replay and tampering were prevented by the validation of nonce and timestamp and detected through hash mismatches stored on-chain. Incorrect access requests were always refused by the smart contracts and this was confirmed by non-modifiable access on the blockchain. Further, the system was hardened against Sybil (i.e., impersonation) attacks by way of a certificate-based identity attestation structure that is part of permissioned blockchain applications.

Compared with current models such as MedRec and Health Chain, this proposed model had better flexibility and efficiency. Despite being novel in patient-controlled access, MedRec is not free of the drawbacks of Ethereum's mainchain such as high energy consumption and long transaction latency. Health Chain provides a fine-grained access control, however, it is not tailored for real-time interaction between users and IoMT devices. To address these gaps, the proposed architecture utilizes a permissioned blockchain, lightweight cryptography, and trust-based consensus mechanism specifically designed for healthcare systems.

Moreover, the verification and the traceability are also supported by the framework. Every access, request, or make to the patient record is permanently logged on the blockchain, that provides compliance with healthcare regulation such as HIPAA and GDPR, and provides provenance of the data. Audit of this access is necessary to use patient data legally and ethically.

Last but not least, the HRLBC was compared with the state of the art with respect to scalability, decentralization, trust, security and real-time performance. High decentralization and architecture security were guaranteed by blockchain, and scale and computational demand elasticity was achieved through cloud resources. Trust relationship of the parties is preserved; and the traditional reliance on central authorities or third-party verifiers is eliminated.

5 Discussion

Blockchain -cloud computing integrative scheme for healthcare IoMT system can be a pragmatic approach to address existing challenges related to data security, privacy and interoperability. In this network, the scalability and processing power of the cloud can be efficiently combined with the decentralized and tamper-resistant characteristics of cryptocurrencies to establish a secure and scalable data management framework to satisfy real-time requirements of healthcare systems. The experiments indicate that our system as a whole offers sub second end-to-end data access and that the throughput peaks at 150 t/s under block chain system scale of 10 nodes. The performance results also affirm the efficacy of our proposed approach to handle the huge amount of data being generated by IoMT devices residing in the network in a timely manner. Furthermore, resource consumption analyses indicate that the framework is efficiently applicable even in resource-constrained edge devices and that it can be applied in remote and mobile healthcare scenarios. A major contribution of this paper is that by using smart contract, we have implemented dynamic patient consent and role-based data policy enforcement. That flow obviates the requirement of the third-party because it provides evidence that access is auditable and transparent (under compliance regimes, including HIPAA and GDPR).

In addition, the security analysis indicates that this scheme is secure against several common attacks, such as replay attack, illegal access attack and data tampering attack. The approach proposed, unlike the typical centralised scenario, ensures that trust is minimum (if any) between healthcare entities and hence the risk, due to single points of failures and insiders is minimised. In conclusion, the practicability, security, scalability of our system configuration is presented in the section. Since the prospective solution is competitive under the simulation scenario, further studies are suggested to investigate the proposed scheme as the federated learning architecture in secure AI-driven analytics and to investigate the energy constraint blockchain protocols for sustainable big healthcare platform deployment.

6 Conclusion

The combination of blockchain and cloud computing provides an attractive paradigm towards enhancing secure, trust and efficient systems that can be applied in various domains concerning digital health, specifically in the Internet of Medical Things (IoMT) area. In this paper, we propose a hybrid architecture to leverage the decentralized and tamper-proof nature of blockchain with the scalable and elastic resources of the cloud. The discovery addresses issues of privacy protection, unauthorized data access, trust and account verification, more so in resource constrained and distributed healthcare system. Through comprehensive experiments and simulations, the proposed architecture displayed its performance in latency, throughputs and access control accuracy. It achieved sub-second response time and was capable of handling more than 150 secure and highly available transactions per second using a permissioned blockchain paradigm. Importantly, the system worked well with edge device, such as Raspberry Pi, shows the practicability of using in future-real-world IoMT application. Moreover, the fact that access to the data was based on smart contract-based access control resulted in fine-grained, dynamic access only if one's access level satisfies a set of rules in a compliance agnostic manner and such as to HIPAA or GDPR. The security analysis shows that the proposed model is secure against replay attack, data tampering and unauthorized access, which reveals the robustness of the model in protecting the medical sensitive data. Compared to the traditional centralized model, we reduce trust on no trustworthy third-party institutions by build our system on blockchain, which supports a fairer and patient-oriented healthcare environment. In conclusion, this paper gives a scalable, secure and efficient solution for next generation digital health systems. In our future work, AI algorithms (predictive analytics) would be integrated, the consensuses scheme is further optimization in the development for the energy efficiency and we also plan to tested the frame work in real clinical environment. These advancements pave the way for how blockchain-cloud convergence is driving a new era in the care delivery and smarter, secure and connected health systems.

References

[1] Ahmad M. O., Siddiqui S. T. Advances in Data and Information Sciences. Berlin, Germany: Springer; 2022. The Internet of Things for Healthcare: Benefits, Applications, challenges, Use cases and future Directions; pp. 527–537.

[2] D. Kalaiyarasi, S. Leopauline, S. Krishnaveni, and A. Vajravelu, “Cloud computing-based computer forensics: a deep learning technique,” International Journal of Electronic Security and Digital Forensics, vol. 16, no. 3, pp. 317–328, 2024, doi: 10.1504/IJESDF.2024.138355.

[3] Buyya R., Yeo C. S., Venugopal S., Broberg J., Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems . 2009;25(6):599–616. doi: 10.1016/j.future.2008.12.001.

[4] Schulze H. AWS cloud security report 2020 for—cloud security alliance. Cloud Security Alliance . 2020. https://cloudsecurityalliance.org/blog/2020/10/14/aws-cloud-security-report-2020-for-management-managing-the-rapid-shift-to-cloud/

[5] Mushtaq M. S., Mushtaq M. Y., Iqbal M. W., Hussain S. A. Security and Privacy Trends in Cloud Computing and Big Data . 2022. Security, integrity, and privacy of cloud computing and big data; pp. 19–51. DOI: 10.1201/9781003107286-2.

[6] S Sivaranjani, V Ashok, and P Vinoth Kumar, “Data Scheduling for an Enchanced Cognitive Radio System in Healthcare Environment,” Bioscience Biotechnology Research Communications , vol. 11, no. 2, pp. 147–157, Feb. 2018.

[7] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review . 2008:p. 21260.

[8] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Proceedings of the 2nd International Conference on Open and Big Data (OBD), 25-30. https://doi.org/10.1109/OBD.2016.11

[9] Xia, QI, Emmanuel BoatengSifah, Kwame OmonoAsamoah, Jianbin Gao, Xiaojiang Du & Mohsen Guizani 2017, „MeDShare: Trust-less medical data sharing among cloud service providers via blockchain‟, IEEE Access, vol. 5, pp. 14757-14767

[10] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing,” Future Generation Computer Systems, vol. 78, no. 3, pp. 1020–1026, 2018.

[11] R. Kumar and R. Tripathi, “Building an ipfs and blockchainbased decentralized storage model for medical imaging, in: advancements in Security and Privacy Initiatives for Multimedia Images,” IGI Global, pp. 19–40, 2021.

[12] Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, “Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain,” Journal of Network and Computer Applications, vol. 176, article 102917, 2021.

[13] Negi, D.; Sah, A.; Rawat, S.; Choudhury, T.; Khanna, A. Block Chain Platforms and Smart Contracts. In Blockchain Applications in IoT Ecosystem; Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N., Eds.; EAI/Springer Innovations in Communication and Computing; Springer: Cham, Switzerland, 2021.

[14] Huang, D. Liu, J. Ni, R. Lu, and X. Shen, “Achieving accountable and e fficient data sharing in industrial Internet of things, ” IEEE Transactions on Industrial Informatics , vol. 17, no. 2, pp. 1416 –1427, 2021.

[15] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Blockchain and federated learning for privacy-preserved data sharing in industrial IoT,” IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4177 –4186, 2020.

[16] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, “Blockchain-based incentives for secure and collaborative data sharing in multiple clouds, ” IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1229 –1241, 2020.

[17] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, “A robust and lightweight secure access scheme for cloud-based e-healthcare services,” Peer-to-peer Networking and Applications, vol. 14, no. 5, pp. 3043–3057, 2021.

[18] M. K. Hasan, M. Shafiq, S. Islam et al., “Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications,” Complexity, vol. 202113 pages, Article ID 5540296, 2021.

[19] Alam S., Shuaib M., Khan W. Z., et al. Blockchain-based Initiatives: current state and challenges. Computer Networks. 2021;198 doi: 10.1016/j.comnet.2021.108395.108395

[20] Aslam T., Maqbool A., Akhtar M., et al. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. Computers, Materials & Continua. 2022;70(1):1089–1109. doi: 10.32604/cmc.2022.019416.

[21] Shen M., Duan J., Zhu L., Zhang J., Du X., Guizani M. Blockchain-Based Incentives for secure and collaborative Data sharing in Multiple clouds. IEEE Journal on Selected Areas in Communications. 2020;38(6):1229–1241. doi: 10.1109/JSAC.2020.2986619.

[22] Xu M., Buyya R. Brownout Approach for Adaptive Management of Resources and Applications in cloud computing systems. ACM Computing Surveys. 2020;52(1):1–27. doi: 10.1145/3234151.