Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems

Mohammed K Elghoul[1*], Sayed F. Bahgat[2], Ashraf S. Hussein[3], Safwat H. Hamad[4]
Scientific Computing Department-Faculty of Computer and Information Sciences, Ain-Shams University, Egypt[1, 2, 3, 4]
King Salman International University, South Sinai, Egypt[3]
Saint Mary's College of California, Moraga CA 94575, USA[4]

***Abstract*—Blockchain technology presents a promising solution to myriad challenges pervasive in the healthcare domain, particularly concerning the secure and efficient management of burgeoning health information technology (HIT) data. This paper delineates a novel blockchain-based approach to enhance various aspects of healthcare management, including data accuracy, drug prescriptions, pregnancy data, supply chain management, electronic health record (EHR) management, and risk data management, with a special emphasis on ensuring secure access, immutable record-keeping, and robust data sharing. We propose a solution focusing on leveraging blockchain technology, particularly utilizing a Hyperledger network within Amazon Web Services (AWS), to securely manage patients' medical records in the cloud. The implemented framework, housed within a Virtual Private Cloud (Amazon VPC) to ensure restricted access and cost-effective resource utilization, underscores advancements in data availability, security, traceability, and sharing, addressing key challenges within healthcare data management, and presenting a scalable, efficient, and secure approach to EHR management in contemporary healthcare contexts.**

***Keywords*—Security; blockchain; cloud; hyperledger**

I. Introduction

Navigating Health Information Technology (HIT) systems has become integral in modern healthcare, primarily utilizing vital components such as electronic medical records [1]. Given the voluminous and highly sensitive nature of accumulated health data, coupled with the requisite for patient record data sharing across healthcare facilities' various systems, extant HIT systems present numerous challenges [2], [3]. Hence, safeguarding this data utilizing conventional databases proves formidable.

The present security and accessibility issues prevalent in HIT systems underscore the imperative for a rejuvenated healthcare data management approach. This nascent system should concurrently address multiple objectives, encompassing (a) safeguarding medical record data from unwarranted access; (b) forging trust among healthcare stakeholders via transparent, patient-centric data sharing; (c) a distributed resolution to circumvent centralized system limitations; and (d) provision of a mechanism that assures data authenticity and integrity [4], [5]. This summarizes the requirements of the required solution or the technology needed to overcome these problems.

Blockchain, as an inventive, dispersed, and immutable ledger technology, is becoming pivotal in transmuting HIT systems. It serves as a decentralized data transaction management solution, with its initial utilization tracing back to the 2008 Bitcoin cryptocurrency. Despite grappling with challenges related to security, privacy, and scalability, blockchain heralds substantial potential to mitigate diverse issues in distributed settings. Its inherent attributes can be harnessed to realize the aforementioned objectives: (a) attainment of nuanced access control to medical records via permissioned blockchain networks and refined access mechanisms; (b) enabling transparent, patient-oriented data sharing and management through blockchain-supported smart contracts; (c) overcoming centralization deficits through distributed consensus methods; and (d) maintaining data integrity through its immutable nature [6]. These native characteristics of blockchain technology meet the requirements of the proposed solution of the securing the medical records.

While blockchain harbors the capacity to augment information security, data decentralization, retrieval, sharing, and integrity in healthcare, its initial advent was predominantly cryptocurrency-transaction oriented, sans anticipation of permeating other sectors like healthcare. Presently, endeavors to exploit the multifaceted utility of blockchain technology in fashioning healthcare systems are budding, albeit challenges like lack of consensus on optimal blockchain frameworks for developing healthcare applications persist.

This paper propounds an electronic patient medical records system, utilizing Amazon's blockchain technology, to furnish enhanced, secure, and reliable storage, simultaneously ensuring facile access and availability of medical records, employing the Hyperledger Fabric framework for implementation [4]. Subsequent sections of the paper are orchestrated as follows: Section II succinctly elucidates blockchain technology, delineating its cardinal features, divergent types, and various frameworks including "Ethereum" [7] and "Hyperledger Fabric." Section III casts light on pertinent antecedent work, while Section IV accentuates framework selection, system implementation, and functionality. Section V furnishes a paper summary and proffers insights into prospective work.

II. Background

Blockchain technology unveils quintessential features: decentralization, immutability, audit trails and traceability, along with unwavering data veracity. Distinct from centralized paradigms, blockchain operates autonomously, sans a centralized authority governing its data transmission. It leverages a spectrum of consensus algorithms, affirming data

validity within a peer-to-peer network framework. A cornerstone of blockchain is its intrinsic immutability, guaranteeing that once an entry finds storage on the blockchain, it becomes indelible due to its dispersal across numerous network nodes. Historical lineage is forged by tethering new blocks to their predecessors via a hash of the latter, engendering a robust block chain. Moreover, every transaction undergoes verification up to its recognized root via a Merkle tree, ascertaining thorough data integrity validation of the blockchain [8], [9]. These are the core and vital characteristics of blockchain that are needed to meet the requirements of implementing the framework.

Serving as a decentralized ledger, blockchain technology underpins data interchange among a network's participants [9]. Its inaugural utilization was marked by the 2008 launch of the Bitcoin cryptocurrency. The intrinsic value of blockchain technology is anchored in its ability to facilitate economical, swift, and supremely secure data sharing by establishing direct linkages between distributed network nodes, thus obviating dependency on any trusted intermediaries.

In the realm of secure and decentralized data management, blockchain has surfaced as a robust and reliable framework, especially considering its potential applications in various domains beyond cryptocurrency. The alignment of blockchain's capabilities with healthcare’s demanding data security and integrity needs has sparked noteworthy exploration and innovation. Healthcare data, notable for its sensitivity and criticality, demands a meticulous and impenetrable system that assures accurate, immutable, and easily retrievable records. Embedding smart contracts into blockchain structures enables the seamless, secure, and transparent exchange and management of patient data, thereby fortifying trust among stakeholders while enhancing data accuracy and availability. Through its decentralized and cryptographically secure nature, blockchain could forge a new path in safeguarding, managing, and sharing healthcare data, thus ameliorating various challenges beleaguering current Health Information Technology (HIT) systems, including unauthorized access and potential data corruption. Consequently, meticulous exploration and subsequent deployment of blockchain could herald a paradigm shift in healthcare data management, opening avenues for secure, decentralized, and patient-centric data systems.

A. Types of Blockchain

Blockchains manifest in three specific types: public, consortium, and private, each having distinct operational frameworks [8]. Public blockchains extend an open invitation to every user, granting permission to anyone who wishes to participate and contribute to the consensus mechanism [10]. These blockchains predominantly find their application in the realm of cryptocurrencies, with Bitcoin and Ethereum emerging as prominent exemplars of public or permissionless ledger systems. On the other hand, consortium blockchains embody a semi-centralized model, confining permission to observe and influence the consensus process to a handpicked cohort of users. Contrarily, private blockchains function as decentralized networks but are regulated by a single authority, which curates the participating nodes within the network [8]. Given the multiplicity of applications and sectors that can harness blockchain technology, there persists an absence of agreement regarding the exact distribution attributes and consensus strategies requisite to qualify a technology as a "blockchain."

B. Current Challenges in Healthcare

Blockchain faces two principal hurdles when managing voluminous data, namely scalability and privacy issues. The accessibility of archived data to authorized entities raises significant privacy red flags, particularly for healthcare organizations that handle delicate patient details. Furthermore, the incorporation of exhaustive medical histories into the blockchain amplifies concerns regarding storage limitations. The nascent and progressively developing characteristic of blockchain technology, together with a pervasive lack of awareness and insight, renders its integration into healthcare notably intricate. The shift from conventional Electronic Health Record (EHR) systems to a blockchain-oriented approach demands a hefty investment in systemic modifications. The lack of set standards in the swiftly progressing field of blockchain further complicates and protracts its practical implementation. Consequently, global authorities ought to formulate standardized policies to promote the secure and efficient amalgamation of blockchain technology into healthcare [4]. Having the hurdles in managing the medical data and not having standards in how to use the blockchain pave the road to the necessity for global authorities to establish standardized policies which is the way for a transformative shift from conventional Electronic Health Record systems.

In a 2016 article published by Naim Yaraghi at the Brookings Institute, light was cast on the multifaceted reasons placing medical records at an elevated risk of security breaches. Initially, medical records pose as a lucrative target for cybercriminals due to the embedding of sensitive individual data, such as birth dates, social security identifiers, and physical addresses. Secondly, these records generally traverse across various stakeholders, encompassing patients, medical establishments, physicians, and hospitals. Additionally, data contained within medical records often preserves its relevance over extensive durations, granting access to historical patient data. Intriguingly, Yaraghi's research unearthed an alarming surge of 1,500% in data violations from 2010 to 2016, illustrated in Fig. 1.

Within the healthcare sector, burgeoning apprehensions are discernible among patients regarding the potential unauthorized disclosure of their medical records, attributed to the susceptibilities of medical devices to hacking whilst assimilating vital medical data for scrutiny [6]. Furthermore, the domain of medical image sharing is positioned to garner advantages from the integration of blockchain technology [11]. The transition from tangible to digital formats for disseminating medical images has notably enhanced the security and accessibility of such images amongst healthcare practitioners. In the past, patients bore the onus of maintaining and sharing physical copies on disks, a practice fraught with risks pertaining to loss or damage. Currently, a strategy dubbed the Image Share Network (ISN), conceived by the Radiological

Society of North America (RSNA), provides a resolution to this challenge.

Moreover, a surge is not merely observed in structured medical record data, but also in the volume and dimensions of medical images. These images wield paramount importance across a multitude of medical disciplines, inclusive of clinical diagnostics, pinpointing pathologies, studying anatomical structures, and formulating therapeutic plans. A concurrent predicament in the prevailing healthcare framework pertains to the incongruence among disparate healthcare entities [10]. The integration of internal healthcare systems with external facilities is an intricate endeavor, often referred to as the multi-organizational data exchange dilemma. This scenario calls for a securely encapsulated and uncomplicated methodology for exchanging patient data across various organizations.

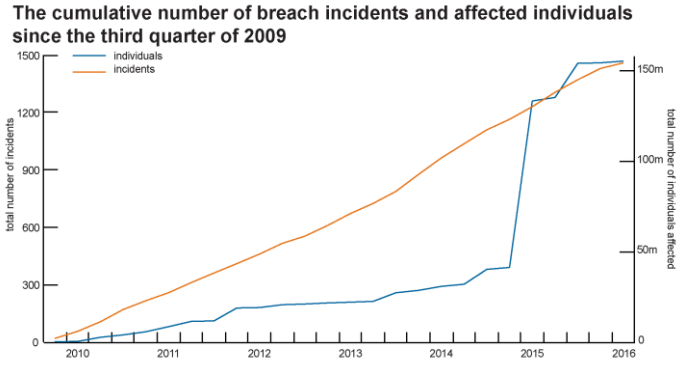

Fig. 1. Data breaches between 2010 and 2016 [4].

In a bid to surmount these challenges, healthcare systems have promulgated a novel assortment of requirements that zero in on issues related to security and data sharing. These prerequisites encompass: (a) bestowing access at a granular level; (b) orchestrating distributed data management; (c) assuring data immutability to uphold authenticity and integrity of data; and (d) centering all transactions around the patient.

III. Current Application and Related Work

Blockchain technology harbors the capability to mitigate numerous challenges pervading the healthcare sector. With the ever-expanding volume of health information technology (HIT) data, the imperativeness of safeguarding data access is exponentially magnifying. To accommodate these requisites, blockchain technology can be strategically employed, having a considerable influence across various healthcare facets, such as data management, precision of health records, medication prescriptions, maternal care, supply chain oversight, health record governance, and managing risk data. Furthermore, it can augment access control, enable efficient data distribution, and preserve a secure audit trail of medical operations [12]. Within the sphere of healthcare, blockchain boasts the potential to boost the accessibility, security, distribution, traceability, and immutability of medical records. A visualization of the multifaceted applications of blockchain within the healthcare domain is depicted in Fig. 2.

Blockchain technology permeates numerous applications throughout the entire expanse of data gathering, analysis, and research, presenting a myriad of possibilities. A pivotal domain where it can wield a notable impact is Electronic Health Records (EHR), where its apt implementation becomes critically vital. This segment explores the intricate details and furnishes a use case for deploying a permissioned blockchain network to safeguard the compilation and distribution of medical information. By archiving medical records within a secure, decentralized, and unalterable ledger, it unlocks avenues for various other applications, including cooperative clinical investigations and detection of medical fraud. The inherent immutability of blockchain ensures that the data is resistant to tampering, thereby promoting transparency and security in each transaction.

Beyond EHR, the potentialities of blockchain technology in the healthcare sector span various realms, including Neuroscience Research, the pharmaceutical domain, and Medical Record & Image Sharing. The ensuing sections will impart comprehensive insights into the applications related to Electronic Health Records and Image Sharing.

In recent times, myriad authors have scrutinized the fusion of blockchain into healthcare. This technology proffers solutions to counteract the challenges pervasive in present electronic medical record systems and contributes additional value to treatment processes and remote access to patient data, all while safeguarding the pinnacle of privacy and security of healthcare information. Although ample research has been performed on the theoretical facets of blockchain in healthcare, only a select few have explored practical implementations of blockchain-oriented medical record systems.

In a 2019 paper, Asma Khatoon [14] honed in on employing blockchain-based smart contracts in healthcare management. This endeavor encompassed a review of applications of blockchain technology in healthcare spanning from 2016 to 2019. Asma illustrated the execution of a healthcare management system predicated on smart contracts and blockchain, elucidating potential merits of decentralization within the healthcare ecosystem, which included cutbacks in transaction expenditures, curtailed administrative overheads, and the omission of intermediaries.

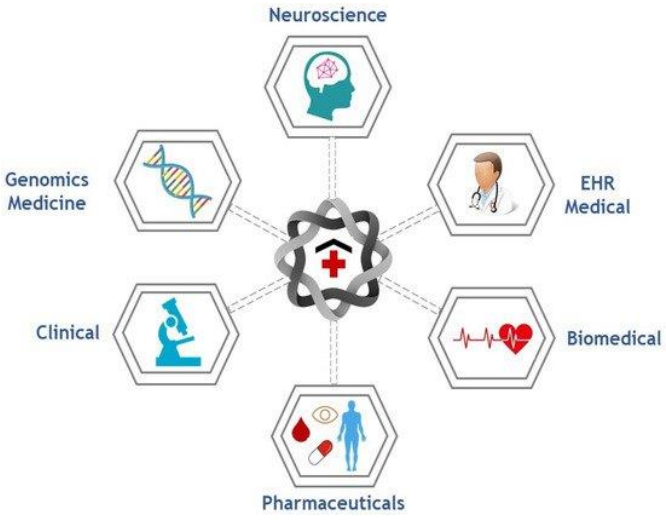

Fig. 2. Applications of blockchain in healthcare [2], [11].

In a distinct study, Daisuke et al. [15] employed the Hyperledger Fabric blockchain platform to convey medical data to the Hyperledger blockchain network, aggregating this data via smartphones with the foremost objective of registering healthcare data on the blockchain.

Rouhani and the team [16] proposed a method aiming to circumvent the constraints of both permissioned and permissionless blockchains, utilizing the Hyperledger platform for healthcare data management, which is orchestrated by patients.

Zhang et al. [17] ventured into the topic of blockchain and smart contracts, accentuating their potential in mitigating various healthcare challenges. They utilized blockchain technology across several healthcare use cases and underscored the challenges tethered to the incorporation of blockchain systems for enhanced healthcare solutions.

The proposed implementation highlighted herein is a native cloud-based solution tailored to securely store a vast volume of patients' medical records. It employs the Hyperledger framework to facilitate secure blockchain implementations, ensuring data segregation among participants. Moreover, the solution avails itself of Amazon Managed Blockchain, which facilitates network genesis and scaling for numerous applications executing millions of transactions. To maintain security, the service functions within an Amazon Virtual Private Cloud (Amazon VPC), assuring that external services are incapable of accessing the resources.

IV. Framework Implementation

A. Framework Selection and Architecture

Kicking off the execution phase, the primal choice revolved around pinpointing the blockchain framework to deploy, wrestling between permissioned and permissionless avenues. A substantial portion of preceding scholarly efforts, as cited in our initial sections, leaned towards utilizing a permissionless network, intertwined with smart contracts. Nonetheless, navigating through the delicate waters of personal medical records and their inherent sensitivity prompted us to gravitate towards the Hyperledger framework, thereby ensuring an impenetrable fort of access, reserved solely for sanctioned members within our blockchain network.

In contrast, a permissionless blockchain operates on an open-door policy, welcoming any individual to join the network sans approval and bestowing upon all members unbridled access to data, which raises substantial concerns, especially when dealing with confidential data. Our selection, therefore, skewed towards the Hyperledger framework as opposed to Ethereum. Hyperledger stands out as a permissioned blockchain platform, meticulously limiting access only to vetted nodes, thereby becoming a vigilant guard of sensitive patient medical records, which may encapsulate confidential datasets including birthdates, national IDs, and medical diagnostics. Within the landscape of a permissionless system, such data could potentially lay bare, exposed to unanticipated entities, thereby man dating bespoke protective solutions. Hyperledger, with its permissioned architecture, inherently satisfies this prerequisite, orchestrating access control symbiotically with member roles.

Piercing through the security and data conservation layers, financial investment emerges as another pivotal aspect demanding scrupulous attention. Ethereum, grounded on the computationally hefty proof-of-work (PoW) algorithm, necessitates considerable outlays for mining activities and transactional costs. Anticipating a bustling highway of transactions, such an approach would fast morph into a financially draining avenue, tethering its pragmatic application. Conversely, Hyperledger harnesses consensus algorithms that are markedly lenient on computational expenses, enhancing its cost-effectiveness.

Arvind et al. [18] implemented a solution by employing IBM cloud and Kubernetes containers. Our suggested approach leverages Amazon Web Services and embraces server less principles, affording us the capability to pay solely for active resources and to dynamically adjust scaling in response to traffic fluctuations. This approach yields noteworthy performance outcomes, as elaborated in the subsequent results section.

Concurrently, AWS brings to the table scalability and a pragmatic pay-as-you-use model, permitting us to financially commit only towards resources engaged actively. A meticulous selection of AWS services has been orchestrated to cater to our specified needs, encompassing: (a) Amazon Managed Blockchain, acting as the secure vault for patient medical records; (b) Amazon Virtual Private Cloud, driving our solution within a secluded network, shielding against unsanctioned ingress; (c) Amazon Elastic Compute Cloud, managing the deployment of chain code and client code; and (d) AWS Secrets Manager, assuring a secure stewardship of network keys.

B. System Architecture and Implementation

Our system has been architecture utilizing Amazon Managed Blockchain, with a distinct emphasis on employing the Hyperledger Fabric framework. This amalgamation guarantees a robust and secure sanctuary for the storage of patients' medical records. Depicted in Fig. 3 is the structural blueprint of our suggested framework, illustrating a schematic view of our infrastructural layout and data flow within the system. We have imposed additional layers of security protocols, assuring that network access is strictly bound within the Virtual Private Cloud (VPC) to shield the data and operations from unauthorized accesses and potential threats.

The focus of our solution leans towards provisioning a suite of APIs tailored for Health Administrators, equipping them with the digital tools necessary to create, retrieve, update, and delete patient records securely within the Hyperledger Fabric database. This not only ensures secure data management but also facilitates a seamless interaction with the stored medical records, enhancing the efficiency and efficacy of administrative tasks within the healthcare setup.

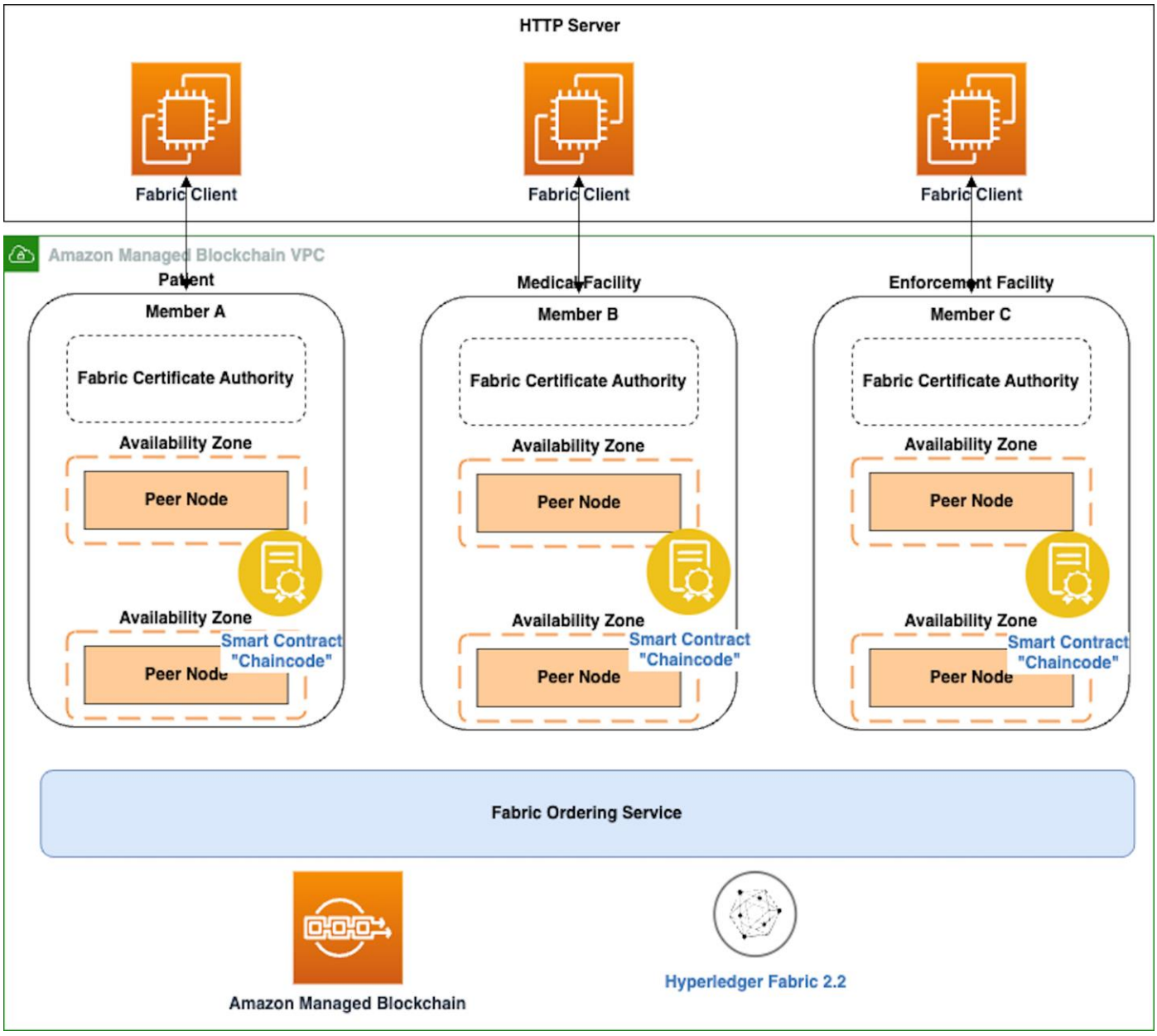

Fig. 3. High level system architecture diagram [1].

This initiative represents a pivotal inaugural step in our explorative journey to devise a holistic system that accommodates various user profiles, such as patients, healthcare providers, and healthcare facilities, intertwining them within a secure, transparent, and accessible digital environment. It further paves the path toward an integrated healthcare data management system where various stakeholders can interact and access necessary data with ease, ensuring that every piece of vital information is securely stored, accurately updated, and easily retrievable when needed, thereby elevating the standards and efficiency of healthcare service provision.

Within the framework of the Hyperledger blockchain network, the system meticulously assigns unique roles and permissions to its participants, facilitating judicious administration and regulated access to medical records. This strategic allocation not only safeguards the confidentiality and integrity of the data but also ensures that each participant interacts with the system in a manner consistent with their responsibilities and requirements. This level of meticulous oversight, underpinned by a robustly structured blockchain network, affords a secure, efficient, and transparent platform where every access, transaction, and modification is not only authenticated and authorized but also immutably logged, thereby ensuring accountability, traceability, and compliance with stringent data protection regulations. This systemic architecture inherently supports the preservation of sensitive medical data, ensuring its availability and integrity while simultaneously safeguarding it from unauthorized and potentially malicious access.

- Member A, embodying a patient within the system, is endowed with the privilege to access and peruse solely their own individual medical record. Furthermore, they are vested with the authority to modify their address information, thereby facilitating the maintenance of up-to-date contact details. This approach not only fortifies the patient's control over their own personal data, ensuring they have a continuous and accurate view of their medical history, but also empowers them to participate actively in maintaining the integrity and currency of their records. In so doing, the system supports a collaborative model where individuals and healthcare providers collectively contribute to the holistic and accurate representation of patient data, enhancing the quality and reliability of the healthcare delivery process. This not only adheres to data protection principles but also engenders a participative environment that is crucial for effective healthcare management and delivery.
- Member B, symbolizing a healthcare facility, is bestowed with more expansive permissions within the system. They are sanctioned to forge and refresh detailed medical records for singular or multiple patients. This entails the aptitude to inject and adjust diverse elements of the patients' health histories, comprising medical antecedents, diagnostic information, administered treatments, and corresponding test outcomes. Moreover, Member B is also granted the ability to assimilate patient admission specifics, like pertinent dates and undergone procedures. This role ensures that healthcare facilities can maintain a thorough and up-to-the-minute dataset, crucial for rendering optimal patient care. With a comprehensive view of patient data, from initial admission details through ongoing treatment updates, Member B plays a pivotal role in crafting a rich, multidimensional patient record that supports informed and timely healthcare decision-making. By having this enriched and detailed access, healthcare facilities can ensure that healthcare practitioners are equipped with the necessary data to provide efficient, accurate, and tailored healthcare services, aligning care strategies closely with individual patient needs and histories. Consequently, this holistic and nuanced access to patient data contributes to enhancing the overall quality and efficacy of healthcare delivery within the facility.
- Member C, functioning as an enforcement entity, fulfills a specialized role within the blockchain network. Their fundamental duty revolves around soliciting and procuring legitimate medical records primarily for exploratory or investigatory pursuits. This provision permits them to acquire relevant patient information crucial for steering investigations or navigating through legal processes. Despite having the capability to access certain data, their permissions are explicitly constricted to merely fetching records, devoid of any authority to enact modifications or adjustments to the encapsulated information within those records. Such controlled access safeguards the integrity of the medical data while ensuring that enforcement agencies can validate or corroborate details imperative to their work without compromising the confidentiality and accuracy of the stored patient information. Consequently, their role in the system is pivotal for establishing a balance between data accessibility for legal and investigative adequacy and safeguarding the immutable nature of medical records within the blockchain. The confined access underscores a meticulous approach to data management, reflecting a commitment to uphold data privacy and security in tandem with operational transparency during examinations and legal occurrences.

Leveraging the AWS Command Line Interface, a blockchain network is constructed through a methodological procedure, which unfolds in a series of eight distinct steps, as visually depicted in Fig. 4. This structured approach allows for the meticulous establishment of the network, ensuring that each phase is executed with precision and accuracy, thereby facilitating a stable and reliable blockchain environment. The AWS Command Line Interface provides an intuitive and efficient medium for performing network creation, enabling developers to navigate through each development stage effectively. Through this guided process, each subsequent step unfolds, crafting a robust blockchain network that stands poised to handle the subsequent data management and transaction needs that it will host. This procedural depiction in Fig. 4 serves not only as a visual guide but also as a structural blueprint, illuminating the path from initiation to full network deployment in a clear, step-wise fashion.

Initiating the development of a blockchain network involves several critical steps, each designed to ensure optimal functionality and security. The subsequent paragraphs elucidate these steps:

1) The inception of the network commences with its creation, during which the selection of the framework type is pivotal. For this instance, Hyperledger Fabric version 2.2 has been chosen as the preferred framework.

2) Subsequently, a member is formulated with a petite instance type, a strategy intended to maintain economical cost management during the preliminary setup phase.

3) Ensuring additional security, a virtual private cloud endpoint is configured for the network, thereby guaranteeing access exclusivity within this VPC.

4) Proceed to formulate a peer node. The nodes are quintessential for interaction, facilitating querying, updating, and maintaining a localized copy of the ledger by interacting with other members' peer nodes within the blockchain.

5) The creation of a client is imperative to streamline interaction within the network and to successfully deploy the chain code.

6) Administrative user enrollment within the certificate authority (CA) of the created member transpires subsequently. It is paramount to secure the user's password, a task aptly handled by Amazon Secrets Manager.

7) Utilizing the administrative client instance, a channel is inaugurated, fostering the sharing of the ledger across the

entirety of the network, providing that all members concur on a universal channel.

8) Looking towards future enhancements, the option to invite new members to affiliate with the network can be explored. Such augmentation facilitates the participation of varied user categories, including administrators and healthcare providers, thereby diversifying user participation.

Each step is paramount in ensuring the streamlined functioning, interactive capability, and secure data management within the blockchain network. These steps should make the process of creating a blockchain network on AWS more understandable and accessible.

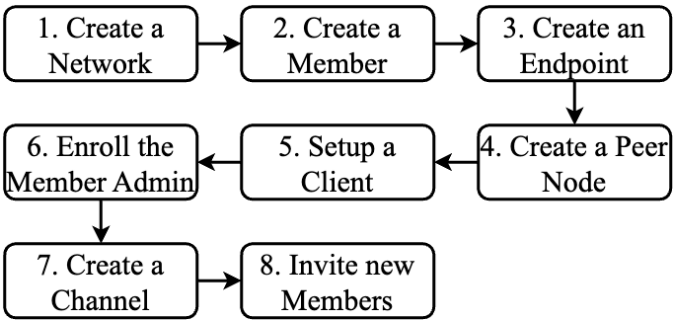

Fig. 4. Create blockchain network steps [4].

C. System Functionality

In the ensuing section, we demystify the findings and performance indicators derived from our experimental exertions. Our investigative ventures were coordinated employing a test dataset that is germane to patient healthcare records. Test automation and quality assurance play an important role in monitoring test results because they reduce human effort and cost and improve the accuracy of results [19]. For the enactment of these experiments, we utilized the open-source Gatling library, involving ourselves in executing concurrent operations which include, but are not limited to, the creation, retrieval, and updating of patient records, alongside obtaining historical data. The script was set into motion with an inaugural group of ten concurrent users and was systematically scaled to integrate up to 2,000 users over a span of 100 seconds. This method of scaling afforded us the ability to assess the system's performance while simultaneously accommodating up to 20 concurrent users for each of the four distinct operations.

The results indicated that the proposed solutions are effective and well-developed for addressing real-world needs. What distinguishes this platform is its effective utilization of Amazon web services. In brief, although the experimental outcomes emphasize the system's potential efficacy in situations with high demand, additional investigation is necessary to confirm its suitability in practical healthcare environments. This involves considering various technical, regulatory, and user experience factors that may impact its performance and acceptance.

The ensuing illustrations elucidate the results procured from the Gatling tool:

- Fig. 5 delineates the spectrum of Response times and the count of requests.
- Fig. 6 unveils the count of active users over the duration of the experiment, reaching an apogee of 1,706 active users at a particular juncture during the experimental phase.
- Fig. 7 sheds light on the dispersion of response times, illustrating the duration requisite to procure a response from the server.

Each diagram provides a visual representation that aids in comprehending the performance and response capabilities of the system during various levels of user load and interaction, offering valuable insights into its operational viability.

An essential consideration is the expense associated with infrastructure. Numerous current healthcare data management systems depend on expansive server farms and physical infrastructure, leading to substantial maintenance and upgrade costs. In comparison, our system utilizes the cost-effective 'Starter' edition of Amazon Managed Blockchain, lessening the financial strain on healthcare providers and enabling scalable expansion without requiring a substantial initial investment.

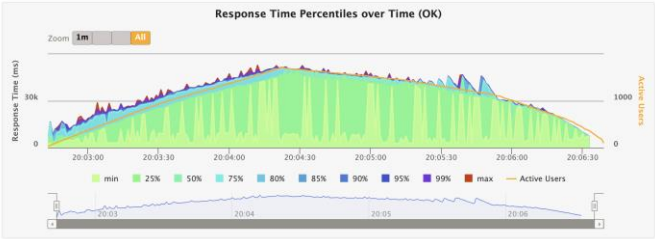

Fig. 5. Response time percentile over time for successful request.

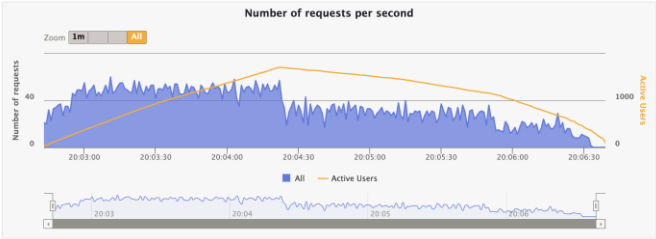

Fig. 6. Number of requests per second.

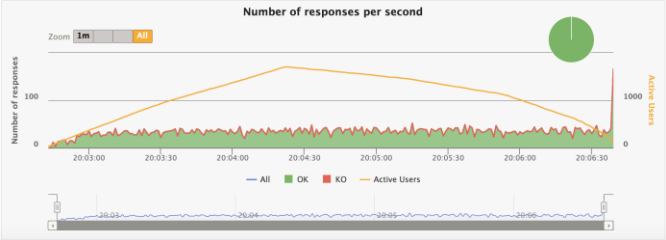

Fig. 7. Number of responses per second.

V. Conclusion and Future Work

This paper unveils a pioneering methodology toward devising a high-performance, cloud-centric solution for safeguarding and accessing medical records within a Hyperledger blockchain network. The implementation is proficient in adroitly managing the migration of historical data, including a magnitude of five million records, and can effectively administrate daily data influxes. The system's capability to accommodate concurrent users was tested utilizing the starter edition of Amazon Managed Blockchain machine type, thereby illustrating its scalability and cohesive integration with AWS services.

Moreover, the paper accentuates the crucial role of testing automation and quality assurance in authenticating experimental outcomes, diminishing human labor and financial expenditure while enhancing precision.

The suggested system is predominantly centered around data storage and analysis, laying a foundation for future enhancements and the integration of novel features to amplify functionality and security. This encompasses potential amalgamation with nascent technologies like artificial intelligence and machine learning to expedite diagnostic processes. Furthermore, enhancements such as multifaceted authentication to secure personal, confidential information and the option to scale to more substantial machine sizes for bolstered performance are contemplated. These prospective enhancements underscore the potential for ongoing system development to cater to the evolving demands of healthcare data management.

References

[1] M. K. Elghoul, S. F. Bahgat, A. S. Hussein, and S. H. Hamad, “Management of medical record data with multi-level security on Amazon Web Services,” SN Appl Sci, vol. 5, no. 11, p. 282, Nov. 2023, doi: 10.1007/s42452-023-05502-9.

[2] S. Elgayar, S. Hamad, and E.-S. El-Horbaty, “Revolutionizing Medical Imaging through Deep Learning Techniques:An Overview.,” International Journal of Intelligent Computing and Information Sciences, vol. 23, no. 3, pp. 59–72, Sep. 2023, doi: 10.21608/ijicis.2023.211266.1274.

[3] salma mostafa ahmed helmy, A. Mahmoud Amar, and E.-S. El-Horabty, “Internet of Things (IoT) based smart device for cardiac patients monitoring using Blynk App,” International Journal of Intelligent Computing and Information Sciences, vol. 0, no. 0, pp. 0–0, Dec. 2022, doi: 10.21608/ijicis.2022.139226.1182.

[4] M. K. Elghoul, S. F. Bahgat, A. S. Hussein, and S. H. Hamad, “Secured Cloud-based Framework for Electronic Medical Records using Hyperledger Blockchain Network,” Egyptian Computer Science Journal, vol. 46, no. 2, Sep. 2022.

[5] C. C. Agbo and Q. H. Mahmoud, “Comparison of blockchain frameworks for healthcare applications,” Internet Technology Letters, vol. 2, no. 5, Sep. 2019, doi: 10.1002/itl2.122.

[6] M. Elghoul, S. Bahgat, A. Hussein, and S. Hamad, “A Review of Leveraging Blockchain based Framework Landscape in Healthcare Systems,” International Journal of Intelligent Computing and Information Sciences, vol. 0, no. 0, pp. 1–13, Oct. 2021, doi: 10.21608/ijicis.2021.75531.1095.

[7] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” Digital Communications and Networks, vol. 6, no. 2, pp. 147–156, May 2020, doi: 10.1016/j.dcan.2019.01.005.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[9] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, “A Systematic Review of the Use of Blockchain in Healthcare,” Symmetry (Basel), vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[10] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, “Blockchain in healthcare and health sciences—A scoping review,” Int J Med Inform, vol. 134, p. 104040, Feb. 2020, doi: 10.1016/j.ijmedinf.2019.104040.

[11] V. Patel, “A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,” Health Informatics J, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[12] V. L. Lemieux, “Trusting records: is Blockchain technology the answer?,” Records Management Journal, vol. 26, no. 2, pp. 110–139, Jul. 2016, doi: 10.1108/RMJ-12-2015-0042.

[13] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives,” Cryptography, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/cryptography3010003.

[14] A. Khatoon, “A Blockchain-Based Smart Contract System for Healthcare Management,” Electronics (Basel), vol. 9, no. 1, p. 94, Jan. 2020, doi: 10.3390/electronics9010094.

[15] D. Ichikawa, M. Kashiyama, and T. Ueno, “Tamper-Resistant Mobile Health Using Blockchain Technology,” JMIR Mhealth Uhealth, vol. 5, no. 7, p. e111, Jul. 2017, doi: 10.2196/mhealth.7938.

[16] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, “MediChainTM: A Secure Decentralized Medical Data Asset Management System,” Jan. 2019, doi: 10.1109/Cybermatics_2018.2018.00258.

[17] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, “Design of Blockchain-Based Apps Using Familiar Software Patterns with a Healthcare Focus,” in Proceedings of the 24th Conference on Pattern Languages of Programs, in PLoP ’17. USA: The Hillside Group, 2017.

[18] A. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta, “A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake,” Comput Intell Neurosci, vol. 2022, pp. 1–19, Apr. 2022, doi: 10.1155/2022/3045107.

[19] A. Ali, H. Maghawry, and N. Badr, “Automation of Performance Testing: A Review,” International Journal of Intelligent Computing and Information Sciences, vol. 0, no. 0, pp. 1–16, Dec. 2022, doi: 10.21608/ijicis.2022.161846.1219.