An Investigation of Scalability in EHRs using Healthcare 4.0 and Blockchain

Ahmad Fayyaz Madni[1], Munam Ali Shah[2], Muhammad Al-Naeem[3]
Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan[1]
Department of Computer Networks and Communications, College of Computer Science and Information Technology,
King Faisal University, Al-Ahsa, Kingdom of Saudi Arabia[2, 3]

Abstract—**In the past decade, Electronic Health Records (EHRs) based on clouds have become popular in empowering remote patient monitoring. The rise of Health 4.0, which includes using system elements and cloud services to access health records remotely, has gained highest attention of the experts. Healthcare 4.0 requires the consistent collection, combination, transmission, exchange, and storage of medical information related to the patients. Because patient information is a private data, it might be challenging to keep hackers out of the reach. As a result, secure cloud storage, access, and exchange of patient medical information is critical in ensuring that the information is not exposed in any unauthorized manner. Security mechanisms that employ Blockchain technology have become popular in recent years since they can provide robust data sharing amongst large number of users and provide storage protection with low computing costs. Researchers have now shifted their focus to using Blockchain to protect healthcare information administration. This work presents an architecture to investigate the scalability of the Healthcare 4.0 systems that use Blockchain. The investigations are carried out under different test scenarios and are evaluated under numerous circumstances, including varying user and data volumes, while also considering the presence of cyber threats. The results demonstrate interesting findings related to the efficiency and effectiveness of deploying Healthcare 4.0 and Blockchain in EHRs.**

Keywords—EHRs; secure cloud; Healthcare 4.0; Blockchain; scalability; cyber threats; medical information; security

I. INTRODUCTION

Business and engineering sectors, such as computing, automotive, electronics, aerospace, and military, have been significantly impacted by the latest innovations like Machine Learning (ML), the Internet of Things (IoT), the Artificial Intelligence (AI) and Blockchain etc. Similarly, healthcare providers such as hospitals and health practitioners have also adopted healthcare systems that utilize these technologies. They have become more robust and more practical over time [1].

Healthcare facilities and practitioners utilize a variety of systems that make them more robust and more helpful over time. Modern systems have also improved their capacity to deal with vast amounts of information instantly, and allowing earlier disease diagnosis, treatment, and automatic treatment solutions. Current healthcare systems have substantially changed the well-being of medical professionals and patients. These healthcare platforms are equipped with several applications installed on consumer devices to gather patient physiological data and provide automated sensing and monitoring of patients' vitals [2].

For instance, smartwatches can display unique pulse patterns, and cell phones can monitor work and sleeping cycles. The glucose sensors can regulate sugar levels by injecting insulin into patients automatically. The advancements in the healthcare sector can potentially enhance and save lives by keeping EHRs, prescribing medications, monitoring health conditions, and providing telemedicine services even remotely and across borders. Patients are becoming more dependent on mobile applications for managing their shared health and treatment information, and these applications are linked to the Internet of Medical Things (IoMT) through telehealth and telemedicine. These technological innovations are some of the examples of how innovations in the healthcare sector can improve the lives of individuals [3]. Similarly, the IoMT devices plays a crucial role in collecting and transmitting health information, however, IoMT is vulnerable to numerous cyber-attacks, including denial of service attack, information leakage, sensor attacks, and different malware threats and attacks [4].

A. Emergence of Healthcare 4.0

Several developments have occurred in the healthcare sector from Generation 1.0 to Generation 4.0. In the initial stages (Generation 1.0), the health sector was primarily focused on doctors and professionals maintaining written records of the patient's medical information. Similarly, under healthcare 2.0, written documents began to be replaced with digital ones. Wearable devices were introduced in Healthcare 3.0 to collect and monitor patient medical information instantaneously [5]. Subsequently, an EHR framework was established, enabling the electronic storage of patient data in an archive that is globally accessible.

Additionally, in the current era, maintaining security of the patient data is essential in guaranteeing data credibility. This is the reason, the concept of Industry 4.0 has emerged which emphasizes the use of high-tech, high-touch systems. These modern solutions have given birth to a more advanced and sophisticated version of the healthcare systems i.e., Healthcare 4.0 which combines AI, IoT, robotics, and cloud computing with numerous healthcare services. Recently, Blockchains are used along with Healthcare 4.0 to ensure secure, credible and easy accessible patients' healthcare information to the practitioners and health service providers [6]. Another goal of these advancements in the field of healthcare is to improve virtualization, which will allow for real-time, personalized medical treatment. Today, there is a need to focus on convergence, coherence, and collaboration of EHR in conjunction with the advancement of healthcare 4.0. The benefits of using Healthcare 4.0 and other modern solutions are numerous but the big challenge to address is that the data is being updated continuously and is being made accessible across various healthcare databases and platforms. The capacity of healthcare systems to scale in line with Healthcare 4.0 has become crucial for broad system adoption while preserving efficacy and efficiency.

The graphical representation in Fig. 1 illustrates various aspects of Healthcare 4.0, emphasizing its foundation in intelligent and digital technology. These characteristics are essential to support healthcare institutions effectively. The approach primarily involves the utilization of cloud computing and data-driven engineering concepts, leading to improved patient care by seamlessly integrating traditional and modern components of Healthcare 4.0. Incorporating fundamental concepts and intelligent artificial intelligence analysis further enhances the healthcare 4.0 culture, ensuring comprehensive patient care. The effectiveness of healthcare 4.0 technology is further elevated by integrating Internet of Things elements [53, 54], resulting in focused and meaningful outcomes for patients and healthcare organizations.

One of the most important and rapidly expanding areas in the global economy is Healthcare 4.0. This firm has met significant social challenges in various countries during the last decade. Numerous researchers have examined how Blockchain technology influences [7] Industry 4.0 in the healthcare sector. [8–10] have focused on how Blockchain technology has dramatically enhanced data communication, anonymity, and privacy.

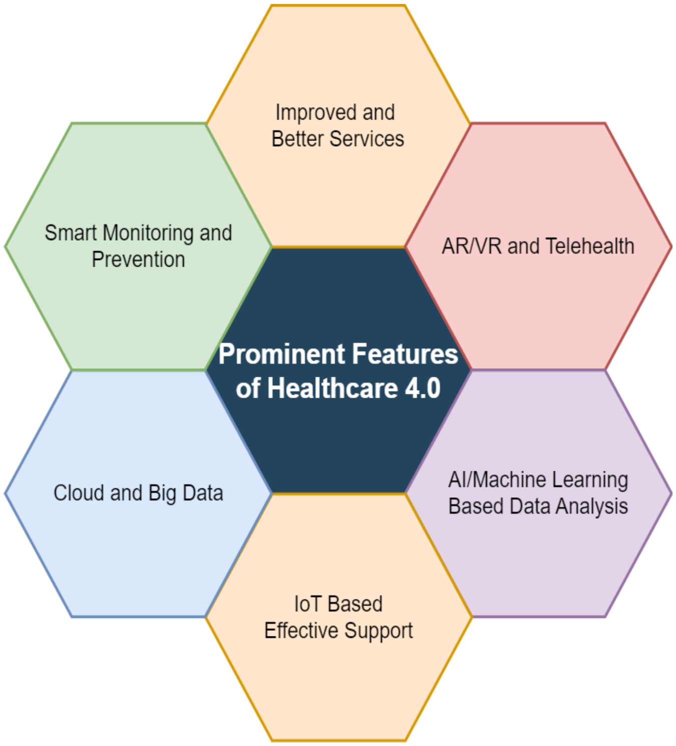

Fig. 1. Some prominent characteristics of Healthcare 4.0.

B. Blockchain in Healthcare

The healthcare sector can benefit from adopting Blockchain as a viable solution for EHR and data transfer, considering its capacity to provide a secure and decentralized infrastructure supporting regulated patient data transmission. It is a distributed platform with consecutive linkages connecting each block [11]. Different healthcare sector stakeholders, including physicians, patients, and insurance agents, might collaborate to support specific Blockchain-based healthcare systems. An EHR contains a patient's medical and operational outcomes from interactions with a provider (i.e., a physician, a nurse, or a mobile emergency nurse) for treatment. The most crucial factors in healthcare are scalability, privacy, and security [12].

As Blockchain enables individuals' complete control over information and security without a single point of control, it is a particularly cost-effective and efficient way to design applications for transmitting EHR data. Healthcare systems are changing in the digital age due to the advent of new advancements [13]. As health information grows exponentially, it is imperative to ensure that EHR systems are scalable. Here, the concepts of "Healthcare 4.0" and Blockchain technology are applied to solve scalability issues.

C. Healthcare Based on Cloud

Blockchain and cloud-based healthcare solutions are revolutionizing the exchange, storage, and access of medical data. Compared to traditional paper-based systems, these innovations improve interoperability, productivity, and safety in healthcare environments. The idea of substituting paper-based medical information with digital ones has been around for a long. Early use of EHRs was prompted by the need for more efficient data storage and retrieval [14]. However, the initial systems needed help with security, compatibility, and data fragmentation. As technology evolved, cloud computing emerged as a novel EHR solution. Cloud computing enhances data sharing among different participating entities but also raises security requirements [15].

Fig. 2 illustrates the storage and retrieval of medical data in cloud-based EHRs. These systems utilize the internet and distant servers, allowing healthcare practitioners to access patient information anytime and from any location. Cloud storage's scalability, flexibility, and cost-effectiveness eliminate the need for regional infrastructure, facilitating informed collaboration among healthcare professionals.

Cloud-based healthcare systems employ remote servers and the Internet for keeping and retrieving medical data [16]. Healthcare professionals may access patient information from anywhere anytime because of the cloud's scalability, flexibility, and affordability. As a result, regional infrastructure is unnecessary, and healthcare professionals can easily collaborate. Some of the benefits of uploading the medical data on the cloud are ease of access of the data to both the patient and the doctors. Ultimately, this helps in better decision-making and better patient care [17]. Moreover, cloud offers access to different services such as use of AI, data mining etc. which makes the cloud a better choice and a secure option. These services allow organizations to utilize the latest innovations without significant investments in their infrastructure or employees [18]. Application programming interfaces (APIs) and integration tools are also included in cloud platforms, allowing companies to easily connect their currently deployed systems and apps with cloud services.

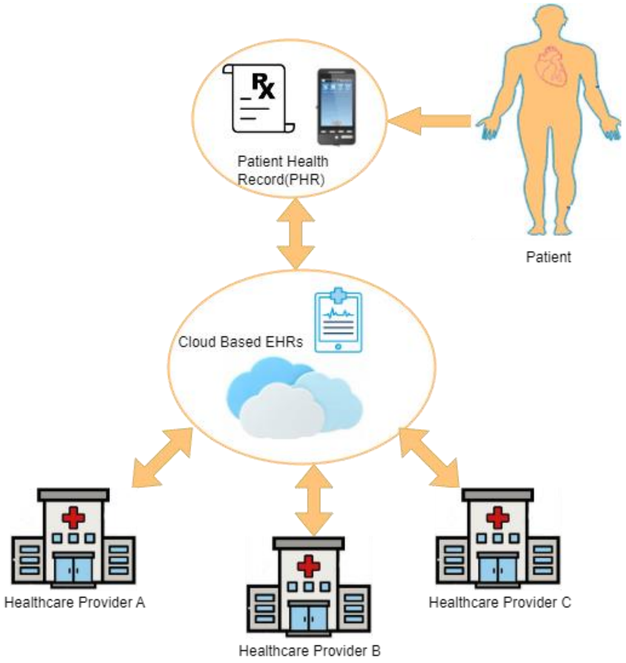

Fig. 2. Cloud based healthcare systems.

The healthcare industry can benefit from integrating Blockchain technology and the cloud. Healthcare organizations employ cloud platforms to handle computational requirements for Blockchain-based networks, including cryptography and consensus schemes. Because computational tasks are delegated to the cloud, Blockchain networks may concentrate on handling information and verification, increasing overall system scalability [19]. Blockchain-based healthcare systems' storage capacity is further increased via cloud computing. The Healthcare sector can utilize cloud storage services to store data, ensuring efficient and affordable data management. Cloud computing allows several healthcare organizations to interact and exchange data. Cloud-based EHR solutions provide rapid, secure access and sharing of patient data across medical practitioners, labs, pharmacies, and other stakeholders, enhancing collaboration and elevating the standard of treatment.

D. Research Problem

Regarding EHRs in Healthcare 4.0, the scalability is crucial challenge to address. The reason is that the healthcare sector creates and analyzes tremendous amounts of patient data, only the scalable EHR systems can manage rapidly expanding volumes of data, facilitate seamless integration, provide real-time analytics, and enhance patient care. With its built-in scalability, Blockchain technology can help EHR systems overcome their scaling issues by offering a decentralized, safe, and scalable architecture.

Different solutions for securing EHRs using Blockchain and Healthcare 4.0 have been proposed, however, the approaches proposed are insufficient to deal with the demands of large-scale deployments without compromising the usability of the system. There is a need to propose a system that can investigate the impact of implementing EHRs using Blockchain and Healthcare 4.0 at a large scale to measure efficiency and effectiveness.

The rest of the paper is prepared as follows: Related Works are presented in Section II. The system model and the proposed methodology are described in Section III. Section IV demonstrates the simulation results of our proposed scheme. Finally, this work's findings and future directions are presented in Section V.

II. Related Work

We focused mainly on the scalability of the healthcare sector that leverages Blockchain and Industry 4.0 concepts while maintaining efficiency and protecting against illegitimate access and data breaches. The most recent Blockchain-based healthcare systems are discussed in this section.

The growing number of internet-connected devices and the massive amount of data generated and gathered online make security and scalability the two most essential concerns for Industry 4.0 [22-23]. A Blockchain is an innovative approach that is a potential way to overcome the restrictions of current networks by preserving and transmitting data in a protected, tamper-proof manner [24-28].

The potential of Blockchain technology in healthcare was investigated in [29] from 2020 and was published in the International Journal of Medical Informatics. In recent years, Blockchain has proven to be a wise option that offers multiple features to the medical data at the same time. For example, it offers security, privacy and integrity of the data. The only limitation in adopting the Blockchain technology in the field of medical and healthcare is that the regulatory requirements are yet to be formulated.

The privacy of the medical records on cloud servers have been recently investigated in study [30]. In this paper, the authors have devised a mechanism that uses Blockchain technology for the health-related data. The authors claim that with their proposed mechanism, any tempering to the data can be easily spotted and the data remains accurate and verified. Moreover, the Ethereum Blockchain enhances the security of the data on the cloud servers.

In another paper [31], the authors have proposed a Personal Health Record (PHR) system which also uses Blockchain. Any unauthorized modification to the data will be observed by their proposed system.

A Blockchain based framework called as MedSBA has been proposed in [32]. This research aims to provide security, privacy and transparency to the patients' data and to the healthcare systems. A Blockchain based IoT system is proposed in [33] which handle the multimedia information such as x-ray images etc. The proposed system is evaluated for efficient data processing and resource usage.

The confidentiality and integrity of the medical data while exchanging it amongst medical professionals have been investigated in [36]. This research uses distributed ledger network and investigates security of data related to both the patients and the medical professionals.

Along with prominent developments in the healthcare system, a strategy needs to catch up when it comes to scalability. "MedChain" is a Blockchain-based medical information exchange solution proposed in [34]. The architecture addresses the healthcare sector's security, privacy, and data interoperability. Smart contracts are implemented with the proposed data fragmentation and exchange approach to improve productivity and offer a controlled and secure way to access medical information. As far as limitations are concerned, the proposed system is complex and needs to be more stable.

Similar research for securing electronic medical records (EMRs) has been proposed in [35]. This research uses three different technologies i.e., Blockchain, smart contracts and modern cryptographic algorithms and provides three different features i.e., data security, anonymity, and access control in any healthcare ssystem. Because the study does not particularly present results from experiments or performance assessments, the proposed architecture and its potential applications in securing EHR systems are explained in detail.

Alhayani et al. [37] suggested and evaluated a Blockchain-based framework to secure medical data stored on cloud servers. Their suggested approach used Blockchain for easily accessible encryption of EHRs. Through complex logic expressions stored in the Blockchain, users could search EHR information using index searches. Utilizing Blockchain ensures traceability, integrity, and protection against tampering with stored information. To evaluate its effectiveness, document IDs from Ethereum were compared with innovative contract transactions derived from EHRs. In 2020, Al-Hayani et al. [38] proposed a novel approach addressing scalability and security in health data. They emphasized four critical phases in the suggested approach, leveraging Blockchain technology to facilitate the exchange of medical information. At first, they explored the requirements for information technology in healthcare and how Blockchain-based frameworks can assist in meeting those demands. Secondly, they developed an FHIR Chain approach intended to meet these requirements. Finally, they demonstrated how to verify the FHIR Chain using health data identifiers. In conclusion, they provided an overview of a case study that facilitated their methodology. Alhayani et al. [39] suggested a Blockchain-enabled approach for healthcare systems. They discussed the opportunities, risks, and potential outcomes of employing the geospatial Blockchain in healthcare systems and the way forward. Blockchain is a decentralized, tamper-proof, trustless, transparent, and immutable append-only database that is now one of the critical instruments of Industry 4.0 [40- 43].

Yahya et al. [44] developed a solution to address the challenges associated with controlling access to sensitive medical information in cloud storage, using inherent features of Blockchain technology such as the ability of Blockchain ledger to remain unchanged and built-in independence. Also, the authors utilized advanced cryptographic techniques to ensure efficient access control for shared data pools by implementing a permission Blockchain. Additionally, they built a framework for Blockchain-based sharing data, which enables data users to get electronic medical reports from a centralized repository relying on user identities and authorized cryptographic keys.

Although Cloud based Health 4.0 are relatively new concepts, little work that utilizes both Cloud based and Healthcare 4.0 has been proposed in [20,21] to improve the security and privacy of cloud-based Healthcare solutions.

The authors in [20] suggest a framework that integrates fog computing, the Internet of Things (IoT), and Blockchain in the context of Health 4.0 to enhance health care services. The system is intended to handle both critical and non-critical patient data, using a clustered fog layer. Critical patients receive a rapid response, while Blockchain secures the health records of non-critical patients, ensuring privacy. The approach demonstrates improved performance in terms of privacy protection, reduced response time and cost savings compared to benchmarks. However, challenges related to scalability and resource limitations require further consideration.

The authors in study [21] also uses Blockchain in EHR system to secure healthcare data and also considers the standards of the Healthcare 4.0. In summary, it can inferred that the security and the privacy of the medical data using Blockchain has been extensively investigated in the research, however, the impact of the scalability by using Blockchain for medical records and EHR is an area which needs further investigations and research.

The authors in study [45] delved into utilizing Blockchain to share securely and store EMRs. With the progression of healthcare data digitization, ensuring the security and privacy of patient information becomes increasingly critical. Due to its decentralized and immutable nature, Blockchain offers potential solutions to these challenges. The focus is developing and implementing a Blockchain-powered system specifically designed to store and exchange EMRs. Additionally, they propose a distributed framework harnessing Blockchain technology's security and transparency features. Access control measures are implemented through a permissioned Blockchain to restrict access and modifications to EMR data, ensuring only authorized users can interact.

Hossein et al. endorse that all involved entities in healthcare, i.e., patients, doctors, etc., must adhere to standardized EHR protocols when recording healthcare information. They also propose using cloud databases to store extensive EHR information, reserve Blockchain storage for identity information, and ensure the integrity of data stored in the cloud [57].

Table I summarizes and simplifies information regarding other relevant works for quick access and comprehension. Table II shows a comparison of the most recent existing research with the proposed system.

As observed, the existing EHR approaches are mainly focused on either Blockchain, cryptographic solutions and cloud based secure solutions, however these approaches have limited or no discussion about the emerging issues of large-scale implementations, so there is a need to introduce a scalable and efficient solution which integrates the benefits of Blockchain and Health 4.0 and address the issue of scalability while maintaining its own efficiency and effectiveness.

TABLE I. COMPARATIVE ANALYSIS OF RELATED WORK

Prominent Features	Results	Evaluation	Limitations
[20] A Fog-enabled Blockchain based architecture to enhance healthcare services in the context of Healthcare 4.0 .	Response time, drop rate, throughput, and utilization of fog and cloud resources	Simulation using Proteus, Packet Tracer, and LabVIEW.	Interoperability and Scalability
[21] Blockchain enabled e-Healthcare system aimed at healthcare 4.0, which address the problems of data safety, privacy.	Average latency and throughput with transaction rate.	Simulation using Hyperledger caliper.	Challenges with the adoption due to complexity.
[45] A permissioned Blockchain to maintain and distribute electronic medical records securely, also address the issues of security, privacy.	Statical analysis	Simulation using web application.	Significant technical expertise and resources required to develop and maintain.
[46] BSF-EHR: Blockchain based Security Framework aimed at e-Health Records that address the problems of security, privacy.	Access time of Health Records in Blockchain and centralized storage.	Simulation using Java.	The proposed framework is technically complex.
[47] TP-EHR Temper Proof E-Health Record, a Blockchain and cloud based secure E-Health system.	Communication overhead with number of patients/doctors and computation overhead with no. of patients	Simulation based on C language.	No discussion on the scalability
[48] A secure Blockchain enabled architecture for storing and distributing e-health records.	Computation time with number of verifiers	Simulation based on PyCrypto.	Scalability and performance limitations.
[49] Blockchain with cloud-based framework for securely maintaining and distributing medical data.	Statical analysis.	Statical analysis is used	No discussion on scalability
[50] A consortium Blockchain and cloud-enabled framework for securing and sharing EHRs, with conditional proxy re-encryption and keyword searchable encryption.	Communication and Computation overhead.	Simulation based on JavaScript	Trust issues may arise.
[51] A Blockchain enabled secure architecture for healthcare-data Sharing.	Performance analysis on configuration and throughput.	Simulation on node.js	Limited analysis
[52] Health Block: A Blockchain enabled framework for secure and efficient management of healthcare data.	Transaction latency, transaction, throughput.	Simulation based on Hyperledger Caliper	Complex to implement.
[53] LB4HC: A light weight secure Blockchain enabled framework for low computational and storage requirements.	Number of blocks with amount of data.	Simulation based on NS3.	Security risks due lightweight Blockchain

TABLE II. COMPARISON OF EXISTING RESEARCH WITH PROPOSED ARCHITECTURE

Author	Health 4.0	Blockchain	Scalable
Adeel et al. [20]	✓	✓	x
Tanwar et al. [21]	✓	x	x
Abunadi et al. [47]	x	✓	x
Sheng et al. [48]	x	✓	x
Proposed	✓	✓	✓

III. SYSTEM MODEL AND PROPOSED METHODOLOGY

This section thoroughly explores the framework's various entities. i.e., patients, healthcare professionals, and Blockchain databases are examples of these entities. Each entity in the ecosystem serves a distinct purpose, adding to the overall functionality and advantages of the suggested framework.

Healthcare organizations should be aware of scalability concerns and possible Blockchain bottlenecks in healthcare systems. This paper allows these organizations to understand how efficiently the proposed system can handle varying volumes of data and user interactions while ensuring sufficient performance and security. This information may be helpful in decision-making, guiding infrastructures and system design choices, and ultimately facilitating the successful implementation of scalable Healthcare 4.0 solutions using Blockchain technology. Our proposed methodology is divided into three sections. These sections and entities are graphically depicted in Fig. 3 and elaborated in this section.

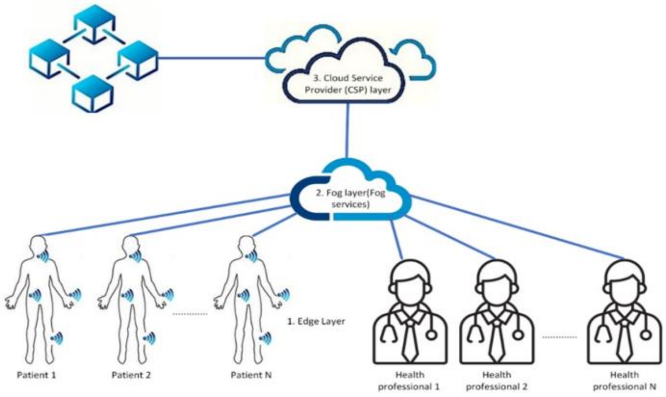

Fig. 3. Proposed system model.

A. Participating Entities

1) Patients and healthcare professionals: In the proposed design, the patient generates his/her medical information, and the owner of the generated health data. The distributed storage constantly receives copies of the patient's health information to facilitate resource sharing. At the same time, healthcare professionals can perform necessary operations on patient data by pre-defined permissions. After that, this information can be uploaded to a cloud-based EHR system. To facilitate patients and the ability to keep track of their health information and make well-informed treatment decisions, patients may also access and analyze their data at any time. Along with having access to all platform functions, which includes reviewing health information, healthcare professionals can register with the system. This ensures detailed diagnosis and treatment strategies by providing them an accurate representation of the patients past health and present state.

Patients and healthcare professionals required to register with the system to access the relevant information. Upon registration, both can access all platform features, including reviewing health information as per the permission defined. Additionally, Healthcare providers have access to and can examine the relevant patient health data. The EHR system based on Health 4.0 can include medical records, test results, treatment plans, and other pertinent data.

2) Blockchain database: The purpose of this architecture is to keep patient medical information on a secure, decentralized Blockchain. In this case, the data integrity and secrecy is guaranteed. Another important feature of Blockchain Database is that the patients have complete control on their data. In addition to improving data security and transparency, this system allows patients to manage their health information, which helps healthcare providers make better decisions and provide better treatment.

B. Components of the Proposed Model

1) Edge layer: A Secure Healthcare Information Gateway: The suggested architecture prioritizes the Edge layer, a starting point of contact, and a layer where information enters the proposed system. This layer deals with wearable sensors, end users, and medical providers, gathering and securing their data before sending it to the Fog layer, which is the layer next to it. Edge layer operations involve the following:

- Information gathering: Acts as the gateway, data gathering from a variety of sources (i.e., body sensors) within the scope of healthcare.
- Data protection: Encrypts sensitive data during transmission to avoid unauthorized access and modification.
- Data cleaning minimizes the quantity of redundant details sent to higher levels by evaluating and reducing information at the edge.
- Reduced latency allows for quicker analysis and processing by just sending secure, pertinent data.

The Edge Layer offers several advantages, few of which are mentioned below:

- Improved Protection: It protects the data against unauthorized access and modifications.
- Improved Efficiency: It removes data redundancy and offers fast processing and filteration of the information on the edge.

2) Fog layer: Orchestrating Healthcare Information: This layer serves as a bridge between the Edge layer and Cloud Service Provider (CSP) layer. In this layer, information collected from edge nodes undergoes verification and indexing. The layer is also responsible creation of logs and metadata Some advantages of this layer are:

- Information verification: The information gathered by the edge nodes is verified
- Data indexing: The data is indexed for processing and retrieval.
- Metadata Generation: Meta data is used for better analysis.
- Information orchestration: The data is better organized between the edge nodes and the CSP.
- Information orchestration makes sure effective data organization by coordinating data flow between the Edge and CSP levels.

3) CSP layer: The Healthcare Data Secure Vault: This layer is responsible for data storage, availability and accessibility of the data. It uses some indexing for efficient data management. Some of the salient features of this layer are:

- Use Data storage: Stores huge amount of data safely and securely.
- Data indexing: Indexes the data for better management and retrieval.
- Access Management: Monitors and controls the data access.
- Blockchain Integration: Uses distributed private Blockchain.

The Inter-planetary File System (IPFS), and Amazon S3 [56] uses the Blockchain technology for distributed data storage. Following are some of the advantages of this approach:

- Improved Security: The data is scattered in a decentralized fashion which provides better security.
- Enhanced Availability: Data replication is used which ensures continuous availability.
- Added Trust: The users are granted direct control to their data which enhances the trust.

The distributed private Blockchain offers an extra layer of security, making it resilient against security threats to the stored medical information.

C. Core Transations in the Proposed System

The proposed framework relies on two essential transactions to deliver a secure and transparent medical record service.

1) Inserting an EHR: In the proposed framework a particular EHR is generated after a patient visits the medical facility. This record contains information related to medications, treatment schedules, and other important data. This record also serves as a patient’s digital account with healthcare system every time the patient visits. Access logs and other metadata are also maintained for achieving the security of the HER. Moreover, the EHR is added with a unique hash value for verification to provide data integrity.

2) Retrieving an EHR: In the proposed framework, Blockchain and IPFS technologies are used to secure and efficiently manage patient EHRs. When an EHR is requested to be retrieved, the system checks the Blockchain for the corresponding transaction and retrieves the hash value of the desired EHR.

D. Evaluation Measures

In this proposed work, we have evaluated the scalability with efficiency of using Blockchain in EHR. Firstly, we evaluated the scalability by taking into account the number of edge nodes and the latency alongside the number of transactions. We have considered multiple scenarios such as one healthcare professional accessing data of one patient; and/or multiple healthcare professionals accessing data of one patient; and/or multiple healthcare professionals accessing data of multiple patients.

To evaluate the effectiveness of the proposed model, we have considered the number of transactions, the CPU usage and the average latency against the number of transactions per minute. The proposed system takes patient datasets as input and executes all Healthcare 4.0 functions and also integrates the Blockchain on these datasets. As the size of patients’ datasets gradually increases, the system will analyze and assess its performance. Lastly, we have investigated the performance of the proposed system on centralized storage.

IV. Simulation Results and Discussions

In this section, we provide the details of the simulations that have been carried out to show the efficiency and effectiveness of our proposed system. For our experiments, we have considered data size, efficiency with different numbers of edge nodes, and potential cyber risks. The experimental results show that the proposed system is scalable and maintains the security of the data.

We have also compared the performance of the proposed system with existing approaches. The comparative results show that our system is effective and the problem of the lack of scalability. The proposed system offers the security, privacy and scalability and is very suitable to be used in healthcare industry. We can increase its resistance and ensure data protection by implementing security measures and testing the system under various cyberattack scenarios. This study also plays a crucial role in mitigating potential risks, thereby fostering user trust in the system's overall security.

A. Enviorment Setup

To simulate a Blockchain network, we used Python as a programming language with Flask Framework, Visual Studio Code as a compiler, and Postman application to make requests to interact with our assumed Blockchain. A Computer System with a sufficient amount of storage is utilized during simulation. The Python code used in simulations along with its complete guide is accessible at the following link: https://github.com/ahmfz/Health4.0 (Accessed on 18th March 2024). Our assumed Blockchain network gets two patient attributes to store those details on the network. After that, the owner can verify the legitimacy of the stored data, and the Authenticity of the network can be determined by using some mechanisms. As we are concerned with the proposed framework's efficiency and effectiveness, we simulate this in terms of varying data sizes with latency and the number of users with latency.

B. For Efficiency

We prioritize attaining scalability while maintaining efficiency, as previously explained. To address this, we examined how access times were affected by the number of users, especially patients. The visual representation of the delay encountered by varying user counts is presented in Fig. 4. We evaluate the system performance at different user volumes and identify the best scaling techniques by examining this data. It is possible to create strategies that optimize the effectiveness of the suggested framework and support a growing user base by comprehending the connection between latency and the number of concurrent users. The goal is to strike a healthy balance between efficiency and scalability so each user can have a flawless experience.

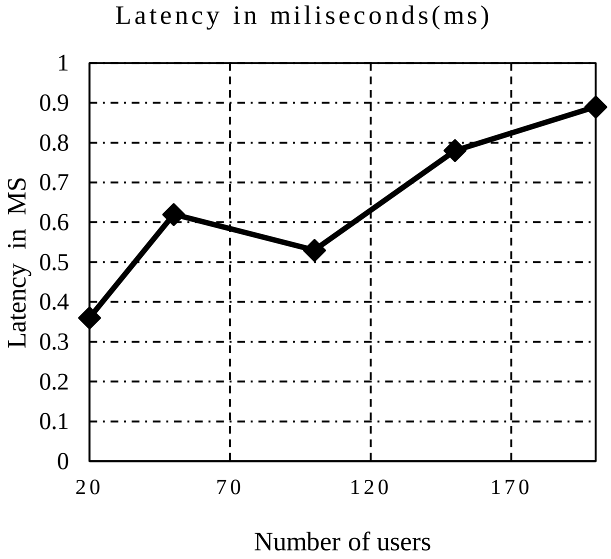

Fig. 4. Latency with varying number of users.

Table III shows the detailed statics of the varying number of users and latency.

TABLE III. LATENCY WITH VARING NUMBER OF USERS

Number of Users	***Latency in ms***
20	0.36
50	0.62
100	0.53
150	0.79
200	0.89

The intricate link between user count and system latency, measured in milliseconds, is depicted in Table III. With an increasing user count, latency varies without a clear upward or decreasing trend. This shows that several variables influence latency, including network congestion and resource availability. An easy user experience and performance optimization are achieved by analyzing these metrics.

Along with the factors discussed above, we also consider several transitions under various scenarios, including when one healthcare professional accesses one patient's data simultaneously. Two healthcare professional access one patient's data, two patients' data, and so on; Fig. 5 depicts the number of transitions concerning time.

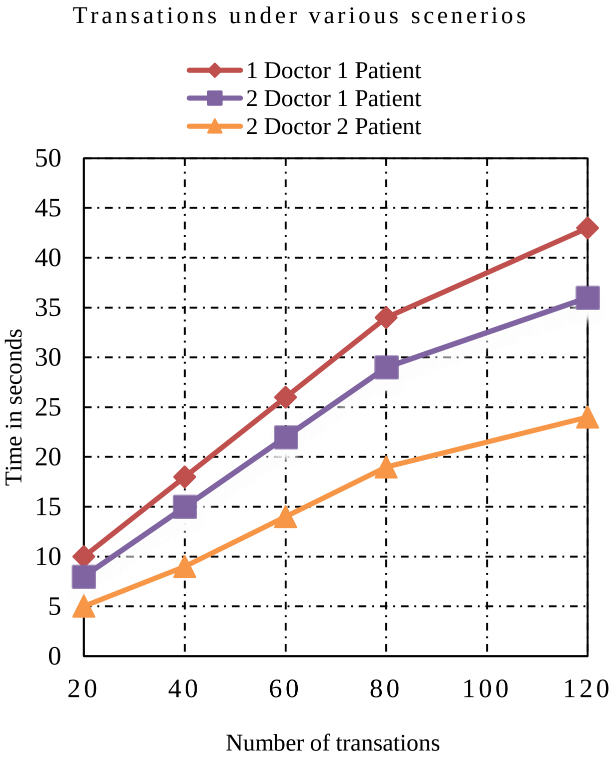

Fig. 5. Number of transitions under various scenarios.

Fig. 5 shows the total amount of transactions recorded across various periods for three scenarios: one doctor and one patient, two doctors and two patients, and two doctors and two patients. The statistics show a positive relationship between time and the number of transactions, with a linear growth in each scenario. Table IV depicts a detailed, relevant overview.

TABLE IV. NUMBER OF TRANSACTIONS WITH VARYING SCENARIOS

Time in Sec	***One Doc with one Patient***	***Two Doc with one Patient***	***Two Doc with Two Patients***
20	10	8	5
40	18	15	9
60	26	22	14
80	34	29	19
120	43	36	24

C. *For Effectiveness*

The initial problem description states that attaining scalability while preserving effectiveness is our core objective. To alleviate this concern, we have considered a scenario with varying numbers of transactions and their corresponding CPU utilization.

By analyzing the impact of different transaction numbers on CPU use Fig. 6, we expect to understand our system's scalability potential. Scalability is the capacity of an infrastructure to accommodate growing demands and alterations in demands. As the number of transactions rises, we are especially curious about how the system performs in this scenario.

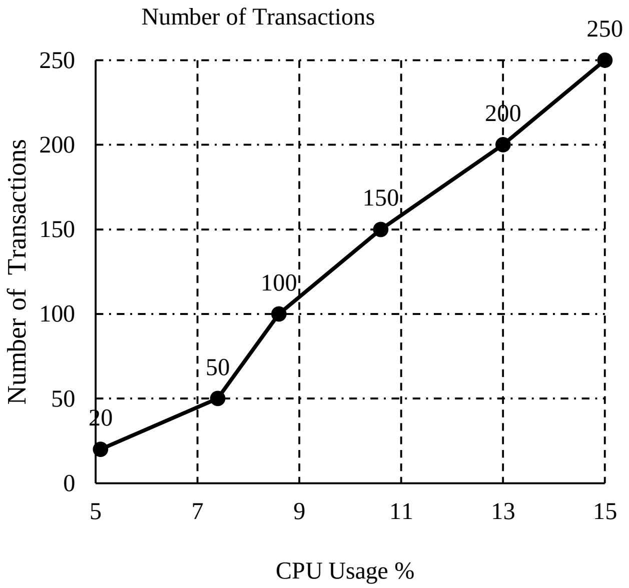

Fig. 6. CPU usage with varying number of transactions.

When we analyze this information, we see that as transaction volume increases, so does CPU utilization. This data helps analyze system scalability, detect possible performance bottlenecks, and optimize resource allocation to ensure efficient and effective system transaction processing.

The data size and latency trends are shown in Table V. Larger volumes and more significant latencies (particularly in the last row) may lead to apparent delays. They impact the overall efficiency, even if the system manages data effectively despite delays. Computational needs, distance, and network congestion probably cause these variances.

TABLE V. CPU USAGE WITH VARYING NUMBER OF TRANSACTIONS

CPU Usage	*Number of Transactions*
5.1	20
7.4	50
8.6	100
13	150
15	200

Average transactional latency is determined by continuously varying the transaction send rate to the outsourced EHRs from 50 to 300 transactions per minute. Fig. 7 shows the typical transaction delay of the suggested EHR storage Blockchain technology.

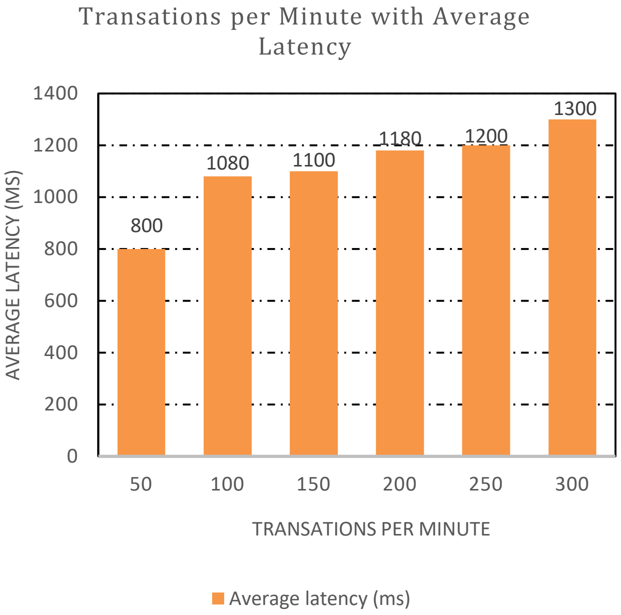

Fig. 7. The suggested algorithms average transaction latency.

Based on the statistics, average latency and the number of transactions delivered tend to rise. For instance, the average latency is 800 ms whenever 50 transactions are delivered. The average latency rises to 1080 ms when the number of transactions in-creases to 100. This trend persists as the number of transactions transmitted rises to 150, 200, 250, and 300, with average latencies of 1100, 1180, 1200, and 1300 ms, respectively.

D. Comparison with other Schemes

In this section, we compare the time it takes to obtain EHRs to a centralized storage system to assess how well the suggested Healthcare 4.0 architecture performs. Fig. 8 illustrates this evaluation.

The ease of handling various-sized EHRs using the suggested framework and centralized storage is compared in Fig. 8. With increasing EHR size, processing times improve, and the suggested design routinely beats centralized storage. That is 50% quicker for an EHR of 200 KB, enhancing scalability and offering advantages to patients and healthcare providers. Performance factors are essential when selecting an EHR storage strategy, and the suggested architecture stands out as a viable option. Table VI depicts these details.

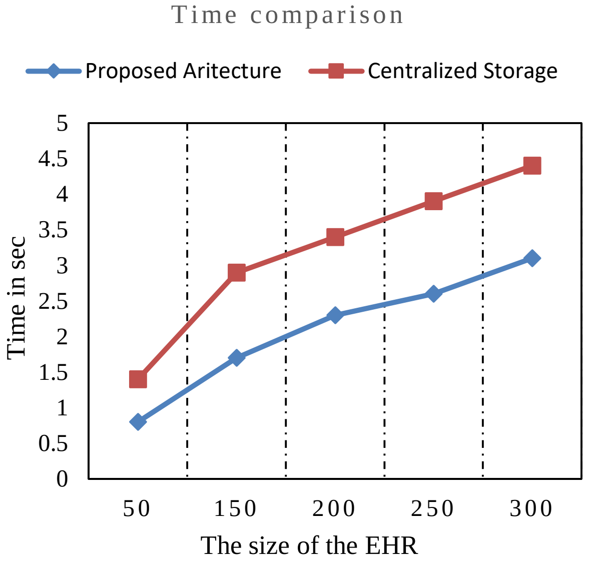

Fig. 8. Comparison with the centralized storage.

TABLE VI. LATENCY WITH VARING NUMBER OF USERS

Data Size in KB	*Time for Centralize storage*	*Time for proposed Architecture*
50	1.4	0.8
100	2.2	1.3
150	2.9	1.7
200	3.4	2.3
250	3.9	2.6
300	4.4	3.1

V. CONCLUSION AND FUTURE WORK

Many healthcare organizations today fail to protect patient information from unauthorized access, making it challenging to scale patient privacy requirements. It is crucial to solve security and scalability challenges in medical data processing in light of the advent of Healthcare 4.0. The field has witnessed the popularity of big data, cloud computing, Internet of Things (IoT), and Blockchain technologies. Although systems based on centralized cryptography have been developed to protect medical records, they typically offer a partial solution. This paper suggests a framework that merges Blockchain technology with cloud services to overcome the challenges arising from the increasing volume of health information. We demonstrate how the suggested framework can adapt while maintaining its efficiency and effectiveness.

We also highlight the adaptability of the proposed system by leveraging the advantages of both technologies; this hybrid solution overcomes some of the limitations associated with traditional EHR systems. The framework is designed to offer an effective and efficient solution for healthcare information management, capitalizing on the security and transparency of

Blockchain and the scalability of cloud computing. The paper also explains how the framework addresses scalability and security challenges in Healthcare 4.0—providing a reliable and scalable platform for storing, maintaining, and transferring EHRs. With a flexible and efficient system capable of meeting the evolving needs of the healthcare industry, it ensures the safety of patient information from unauthorized access.

A. Future Work

The future roadmap should prioritize enhancing Healthcare 4.0 architecture, adopting a smart city approach, i.e., SmartCity 4.0. A key aspect involves integrating a quantum-aware Blockchain that addresses challenges related to efficient keyword searches in smart healthcare scenarios [55]. This involves utilizing advanced post-quantum cryptography algorithms for decryption, search requests, and commitments. The efficient storage, retrieval, and analysis of vast amounts of patient data generated by healthcare systems become challenging. Incorporating Blockchain technology has proven instrumental in overcoming some of the healthcare system's scalability, security, and interoperability challenges.

Another approach that can be considered as future work is Sharding. It involves breaking down the Blockchain into smaller units known as shards, enabling it to handle transactions concurrently. Implementing Sharding can enhance healthcare information systems' scalability and transaction processing capacity. Additionally, side chains can offload specific operations from the primary Blockchain, i.e., data storage or complex computations, to enhance scalability further. This approach supports streamlining processes and managing the load on the main Blockchain, contributing to improved scalability in healthcare or smart city structures.

Funding Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University (KFU), Al-Ahsa, Kingdom of Saudi Arabia [Grant No. A281].

References

[1] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, “Fog computing for Healthcare 4.0 environment: Opportunities and challenges,” *Computers & Electrical Engineering*, vol. 72, pp. 1–13, Nov. 2018, doi: https://doi.org/10.1016/j.compeleceng.2018.08.015.

[2] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “A Survey on Security and Privacy Issues in Modern Healthcare Systems,” *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1–44, Jul. 2021, doi: https://doi.org/10.1145/3453176.

[3] R. Talati and P. Chaudhari, "The Road-ahead for E-healthcare 4.0: A Review of Security Challenges," *2022 1st International Conference on Informatics (ICI)*, Noida, India, 2022, pp. 208-213, doi: 10.1109/ICI53355.2022.9786917.

[4] M. Mushtaq, M. A. Shah and A. Ghafoor, "the internet of medical things (iomt): security threats and issues affecting digital economy," *Competitive Advantage in the Digital Economy (CADE 2021)*, Online Conference, 2021, pp. 137-142, doi: 10.1049/icp.2021.2420.

[5] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, “Securing electronics healthcare records in Healthcare 4.0 : A biometric-based approach,” *Computers & Electrical Engineering*, vol. 76, pp. 398–410, Jun. 2019, doi: https://doi.org/10.1016/j.compeleceng.2019.04.017.

[6] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R. M. Parizi, and K.-K. R. Choo, “Fog data analytics: A taxonomy and process model,” *Journal of Network and Computer Applications*, vol. 128, pp. 90–104, Feb. 2019, doi: https://doi.org/10.1016/j.jnca.2018.12.013.

[7] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, “Blockchain technology in the healthcare industry: Trends and opportunities,” *Journal of Industrial Information Integration*, vol. 22, p. 100217, Jun. 2021, doi: https://doi.org/10.1016/j.jii.2021.100217.

[8] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7059-7067, Oct. 2022, doi: 10.1109/TII.2021.3084753.

[9] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, “Resource allocation and trust computing for Blockchain-enabled edge computing system,” *Computers & Security*, vol. 105, p. 102249, Jun. 2021, doi: https://doi.org/10.1016/j.cose.2021.102249.

[10] W. Wang *et al*., "Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks," in *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883-8891, 1 June1, 2022, doi: 10.1109/JIOT.2021.3117762.

[11] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, Jun. 2019, doi: https://doi.org/10.1016/j.jnca.2019.02.027.

[12] M. Shashi, “Leveraging Blockchain-Based Electronic Health Record Systems in healthcare 4.0,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 12, no. 1, pp. 1–5, Dec. 2022, doi: 10.35940/ijitee.a9359.1212122.

[13] S. Surati, S. Patel, and K. Surati, “Background and Research Challenges for FC for Healthcare 4.0,” *Signals and communication technology*, pp. 37–53, Aug. 2020, doi: https://doi.org/10.1007/978-3-030-46197-3_2.

[14] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in *IEEE Access*, vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[15] A. Ishaq, B. Qadeer, M. A. Shah and N. Bari, "A Comparative study on Securing Electronic Health Records (EHR) in Cloud Computing," 2021 26th International Conference on Automation and Computing (ICAC), Portsmouth, United Kingdom, 2021, pp. 1-7, doi: 10.23919/ICAC50006.2021.9594178.

[16] H. B. Mahajan, “Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap,” *Wireless Personal Communications*, Sep. 2022, doi: https://doi.org/10.1007/s11277-022-09535-y.

[17] R. Ganiga, R. M. Pai, M. P. M. M., and R. K. Sinha, “Security framework for cloud based electronic health record (EHR) system,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, p. 455, Feb. 2020, doi: https://doi.org/10.11591/ijece.v10i1.pp455-466.

[18] A. Sabur, A. Chowdhary, D. Huang, and A. Alshamrani, “Toward scalable graph-based security analysis for cloud networks,” *Computer Networks*, vol. 206, p. 108795, Apr. 2022, doi: https://doi.org/10.1016/j.comnet.2022.108795.

[19] A. Fernandes, V. Rocha, A. F. d. Conceição and F. Horita, "Scalable Architecture for sharing EHR using the Hyperledger Blockchain," *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, Salvador, Brazil, 2020, pp. 130-138, doi: 10.1109/ICSA-C50368.2020.00032.

[20] I. Ahmad, S. Abdullah, and A. Ahmed, “IoT-fog-based healthcare 4.0 system using Blockchain technology,” *The Journal of Supercomputing*, Sep. 2022, doi: https://doi.org/10.1007/s11227-022-04788-7.

[21] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” *Journal of Information Security and Applications*, vol. 50, no. 1, p. 102407, Feb. 2020, doi: https://doi.org/10.1016/j.jisa.2019.102407.

[22] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," in *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881-888, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008906.

[23] Y. Wu, H. -N. Dai and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in

Industry 4.0," in *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300-2317, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3025916.

[24] M. M. Alhejazi and R. M. A. Mohammad, “Enhancing the Blockchain voting process in IoT using a novel Blockchain Weighted Majority Consensus Algorithm (WMCA),” *Information Security Journal: A Global Perspective*, pp. 1–19, Jan. 2021, doi: https://doi.org/10.1080/19393555.2020.1869356.

[25] A. Omran Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, “Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things,” *Computers, Materials & Continua*, vol. 68, no. 1, pp. 359–376, 2021, doi: https://doi.org/10.32604/cmc.2021.014753.

[26] A. Carvalho, J. W. Merhout, Y. Kadiyala, and J. Bentley II, “When good blocks go bad: Managing unwanted Blockchain data,” *International Journal of Information Management*, vol. 57, p. 102263, Apr. 2021, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102263.

[27] Y.-M. Guo *et al.*, “A bibliometric analysis and visualization of Blockchain,” *Future Generation Computer Systems*, vol. 116, pp. 316–332, Mar. 2021, doi: https://doi.org/10.1016/j.future.2020.10.023.

[28] P. V. Kakarlapudi and Q. H. Mahmoud, “A Systematic Review of Blockchain for Consent Management,” *Healthcare*, vol. 9, no. 2, p. 137, Feb. 2021, doi: https://doi.org/10.3390/healthcare9020137.

[29] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, “The benefits and threats of Blockchain technology in healthcare: A scoping review,” *International Journal of Medical Informatics*, vol. 142, no. 1, Oct. 2020, doi: https://doi.org/10.1016/j.ijmedinf .2020.104246.

[30] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” *Future Generation Computer Systems*, vol. 95, pp. 420–429, Jun. 2019, doi: https://doi.org/10.1016/j.future.2019.01.018.

[31] T. T. Thwin and S. Vasupongayya, “Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems,” *Security and Communication Networks*, vol. 2019, pp. 1–15, Jun. 2019, doi: https://doi.org/10.1155/2019/8315614.

[32] T. T. Thwin and S. Vasupongayya, “Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems,” *Security and Communication Networks*, vol. 2019, pp. 1–15, Jun. 2019, doi: https://doi.org/10.1155/2019/8315614.

[33] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using Blockchain technology,” *Multimedia Tools and Applications*, Jun. 2019, doi: https://doi.org/10.1007/s11042-019-07835-3.

[34] B. Shen, J. Guo, and Y. Yang, “MedChain: Efficient Healthcare Data Sharing via Blockchain,” *Applied Sciences*, vol. 9, no. 6, p. 1207, Mar. 2019, doi: https://doi.org/10.3390/app9061207.

[35] G. Yang, C. Li, and K. E. Marstein, “A Blockchain-based architecture for securing electronic health record systems,” *Concurrency and Computation: Practice and Experience*, Aug. 2019, doi: https://doi.org/10.1002/cpe.5479.

[36] X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," in *IEEE Access*, vol. 7, pp. 118943-118953, 2019, doi: 10.1109/ACCESS.2019.2937685.

[37] B. Alhayani and A. A. Abdallah, “Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN,” *Engineering Computations*, vol. ahead-of-print, no. ahead-of-print, Sep. 2020, doi: https://doi.org/10.1108/ec-02-2020-0107.

[38] B. Al-Hayani and H. Ilhan, “Efficient cooperative image transmission in one-way multi-hop sensor network,” The International Journal of Electrical Engineering & Education, vol. 57, no. 4, pp. 321–339, Dec. 2018, doi: https://doi.org/10.1177/0020720918816009.

[39] A. S. Kwekha-Rashid, H. N. Abduljabbar, and B. Alhayani, “Coronavirus disease (COVID-19) cases analysis using machine-learning applications,” *Applied Nanoscience*, May 2021, doi: https://doi.org/10.1007/s13204-021-01868-7.

[40] A. Carvalho, J. W. Merhout, Y. Kadiyala, and J. Bentley II, “When good blocks go bad: Managing unwanted Blockchain data,” *International Journal of Information Management*, vol. 57, p. 102263, Apr. 2021, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102263.

[41] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li and Z. Ming, "Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach," in *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2226-2237, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3035437.

[42] J. Sunny, N. Undralla, and V. Madhusudanan Pillai, “Supply chain transparency through Blockchain-based traceability: An overview with demonstration,” *Computers & Industrial Engineering*, vol. 150, no. 150, p. 106895, Dec. 2020.

[43] P. V. Kakarlapudi and Q. H. Mahmoud, “A Systematic Review of Blockchain for Consent Management,” *Healthcare*, vol. 9, no. 2, p. 137, Feb. 2021, doi: https://doi.org/10.3390/healthcare9020137.

[44] W. Yahya *et al.*, “Study the influence of using guide vanes blades on the performance of cross-flow wind turbine,” *Applied Nanoscience*, Jun. 2021, doi: https://doi.org/10.1007/s13204-021-01918-0.

[45] M. Usman and U. Qamar, “Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology,” *Procedia Computer Science*, vol. 174, pp. 321–327, 2020, doi: https://doi.org/10.1016/j.procs.2020.06.093.

[46] I. Abunadi and R. L. Kumar, “BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients,” *Sensors*, vol. 21, no. 8, p. 2865, Apr. 2021, doi: https://doi.org/10.3390/s21082865.

[47] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, “Cloud-assisted secure eHealth systems for tamper-proofing EHR via Blockchain,” *Information Sciences*, vol. 485, pp. 427–440, Jun. 2019, doi: https://doi.org/10.1016/j.ins.2019.02.038.

[48] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C.-M. Chen, “A secure Blockchain-based e-health records storage and sharing scheme,” *Journal of Information Security and Applications*, vol. 55, p. 102590, Dec. 2020, doi: https://doi.org/10.1016/j.jisa.2020.102590.

[49] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-Based Medical Records Secure Storage and Medical Service Framework,” *Journal of Medical Systems*, vol. 43, no. 1, Nov. 2018, doi: https://doi.org/10.1007/s10916-018-1121-4.

[50] Y. Wang, A. Zhang, P. Zhang and H. Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain," in *IEEE Access*, vol. 7, pp. 136704-136719, 2019, doi: 10.1109/ACCESS.2019.2943153.

[51] P. Pandey and R. Litoriya, “Securing and authenticating healthcare records through Blockchain technology,” *Cryptologia*, vol. 44, no. 4, pp. 1–16, Jan. 2020, doi: https://doi.org/10.1080/01611194.2019.1706060.

[52] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure Blockchain-based healthcare data management system,” *Computer Networks*, vol. 200, p. 108500, Dec. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108500.

[53] L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in *IEEE Access*, vol. 7, pp. 149935-149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[54] G. L. Tortorella, F. S. Fogliatto, A. Mac Cawley Vergara, R. Vassolo, and R. Sawhney, “Healthcare 4.0: trends, challenges and research directions,” *Production Planning & Control*, vol. 31, no. 15, pp. 1–16, Dec. 2019, doi: https://doi.org/10.1080/09537287.2019.1702226.

[55] “Intelligent Sensing Technology, Smart Healthcare Services, and Internet of Medical Things-based Diagnosis,” *American Journal of Medical Research*, vol. 6, no. 1, pp. 13–18, 2019, Accessed: May 18, 2024. [Online]. Available: https://www.ceeol.com/search/article-detail?id=762693.

[56] O. Mustafa, “Overview of Amazon Web Services,” pp. 1–35, Jan. 2023, doi: https://doi.org/10.1007/978-1-4842-9303-4_.

[57] H. Aghahosseini and M. Sakhaei-nia, “Interoperability and Standards in Blockchain-based EHR,” *Advances in the Standards & Applied Sciences*, vol. 2, no. 1, pp. 4–12, Jan. 2024, doi: https://doi.org/10.22034/asas.2023.420797.1043.