Innovative Framework for Secure Healthcare Data Management: Utilizing Ethereum Blockchain

Iqra Sadia Rao
Department of Computer System & Technology,
Universiti Malaya, Kuala Lumpur, Malaysia
s2033970@siswa.um.edu.my/iqrasrao@gmail.com

Miss Laiha Mat Kiah
Department of Computer System & Technology,
Universiti Malaya, Kuala Lumpur, Malaysia
misslaiha@um.edu.my

***Abstract*— In this paper, we propose an enhanced framework based on Ethereum blockchain technology for the healthcare sector. Currently, healthcare systems are often centralized, with a single entity controlling and managing patient data. This can make it difficult for patients to access and share their medical information, while also creating potential security risks. Furthermore, existing frameworks may not be able to manage large amounts of data due to Ethereum's scalability limitations. An Ethereum-based framework utilizing blockchain technology could help address these issues by providing a decentralized and secure system, giving patients greater control over their data and reducing the risk of unauthorized access. Additionally, Ethereum-based smart contracts could automate various healthcare processes, such as claims processing and appointment scheduling, improving efficiency and reducing administrative costs. This paper contributes to the development of such a framework by utilizing Apache Kafka techniques to build a private Ethereum blockchain that improves scalability and generates immutable and secure records via smart contract-generated hashes as it is immutable, secure and scalable.**

Keywords—Decentralized AI; Blockchain; Ethereum; Healthcare

I. INTRODUCTION

By enhancing the security and interoperability of electronic medical records (EMRs) [1] and opening up new use cases like clinical trial data sharing and precision medicine, blockchain technology has the potential to completely transform the healthcare sector.

The ability to create a safe, decentralized record-keeping system is one of the key advantages of adopting blockchain in healthcare. EMRs can be stored on a blockchain, enabling healthcare providers to access and update them in real time while maintaining a tamper-proof record of all changes. This can help to reduce errors and improve the accuracy of medical records [2].

Another potential use case for blockchain in healthcare is the sharing of clinical trial data. By using a decentralized platform, researchers can securely share data with one another and with regulatory agencies, helping to accelerate the development of new treatments and therapies.

Precision medicine is another area where blockchain could have a significant impact. By using blockchain-based platforms, healthcare providers can securely share and access genomic data, enabling them to tailor treatments to the specific needs of individual patients.

Overall, the use of blockchain in healthcare [3][4] has the potential to improve the security, efficiency, and interoperability of the industry, leading to better outcomes for patients.

Transparency and communication between patients and healthcare providers have improved as a result of the usage of blockchain technology in the healthcare sector. Because of duplications, the use of various names and identities, and their availability across many networks, healthcare records are becoming larger and more complicated, but they have not yet been optimised for these characteristics. Additionally, it is now crucial to maintain data security and stop illicit activity. Patient data can be utilised or sold if unauthorised people are permitted access, and everyone with access will be able to see the personal information of the patients. Data privacy for patients is essential for effective healthcare administration[1].

We are proposing that every time doctors meet a patient, information on underlying illnesses, food or drug sensitivities, and prescribed drugs must be gathered. In order to effectively diagnose and treat patients, these data allow for the reduction of needless laboratory or imaging procedures. Physicians can access medical information about patients who often attend an emergency department (ED) [5] without the need for an extra report.

In Malaysia, medical records are still commonly transmitted through paper or telephone when patients elect to shift from one hospital to another. This is often referred to as the "discharge summary" process, where the patient's medical records are printed out and given to the patient to be carried to the next hospital, or are sent through fax or email. However, the adoption of digital medical records in Malaysia still faces challenges, such as limited funding and technical infrastructure, as well as concerns around data privacy and security. It is important for healthcare providers and policymakers to continue to work towards a more seamless and secure system for sharing medical records, while also addressing these challenges and ensuring the privacy and security of patient data. In contrast, it can be challenging to learn a patient's whole medical history when they unexpectedly visit a neighboring hospital, particularly in an emergency, as patients sometimes forget specifics about their former illnesses, dosages, or drug usage. Personal health records (PHRs) connected to hospitals can offer reliable data, but if the hospital does not create and distribute PHRs, the information is not accessible electronically [6].

The paper is organized into several sections, each with a specific focus. In Section 2, the authors address objections that may arise regarding the proposed health record management platform. Section 3 provides background information, including a discussion of Blockchain in Healthcare and a review of prior system architectures. This section helps to contextualize the proposed platform and its potential benefits. Section 4 is dedicated to the proposed platform itself, which is blockchain-based and utilizes Kafka, smart contract hash architecture. This section provides a

 ISBN: 978-1-68558-080-3

detailed overview of the platform's architecture and features. Section 5 covers the performance metrics, providing a quantitative analysis of the platform's capabilities. In Section 6, the authors offer a discussion of the platform, including its strengths and weaknesses, and consider how it could be improved in the future. Section 7 presents the conclusions that can be drawn from the proposed platform and its potential impact on the healthcare industry. Finally, the authors include Acknowledgments and References sections. The organization of the paper helps to provide a clear and concise understanding of the proposed health record management platform and its potential benefits for the healthcare industry.

II. OBJECTIVES

In the envisaged architecture, the blockchain regulates the authorization of data transfers between patients, healthcare providers, and other users. The blockchain uses Apache Kafka to scale the incoming data and manage it in immutable logs. The blockchain does not physically replace the electronic health record system since the majority of hospital information systems store comprehensive Personal Health Records (PHRs) in a secure database on site or in a backup location outside the hospital. Only the data's security, confidentiality, integrity, and availability [3] are ensured by the blockchain's design. Stakeholders have access to read and write electronic health record data that can be securely sent to and from other systems via the blockchain.

The main contributions of this paper are:

- To present the proposed framework for the health information records on Ethereum blockchain.
- To present comprehensive literature for readers relating Blockchain in Healthcare and on security and privacy of the Electronic Health Record (EHR) and Personal Health Records (PHR).
- To provide an understanding of the state-of-the-art techniques implemented in the healthcare and blockchain
- To get cryptographic security visa Hash code in smart contracts which are only accessible to the designated personnel.
- This architecture is formed via a private P2P network, where health records are organized into data blocks comprising a linked list and a distributed ledger of health data.
- This architecture introduced the blockchain scalability issue with the data management can be an issue. The proposed framework not only address the security as well as scalability of data while using blockchain.

III. BACKGROUND

Blockchain technology is based on cryptography, which is used to secure transactions and ensure the privacy of users. Two key cryptographic concepts used in blockchain are hashing and smart contracts [4][16][17].

Hashing is the process of taking an input (or "message") and returning a fixed-size string of characters, which is called the "hash." The same input will always produce the same hash, but even a small change to the input will produce a very different hash. This makes it useful for verifying the integrity of data, as any changes to the input will result in a different hash [8].

Smart contracts are self-executing contracts with the terms of the agreement written directly into code. They allow for the automation of certain processes, such as the transfer of assets. They are stored and replicated on the blockchain network, and can be programmed to trigger actions based on specific events or conditions.

It is important to note that as the technology and understanding of blockchain is evolving rapidly, new research and literature is being produced frequently. Google is showing the recent trends in the Health Information Exchange.

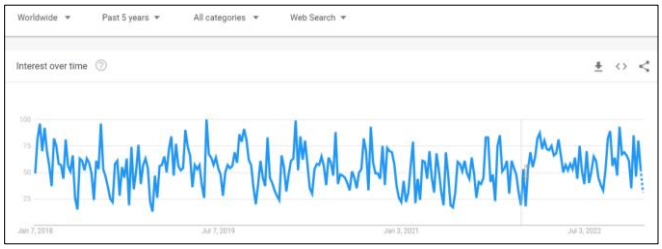

Figure1. Global Health Information Exchange (HIE) google trend analysis (Past 5 years 2018-2022)

In order to facilitate exchange agreements between hospitals, clinical areas, regulators, insurers, and even patients, HIE network organizations have developed. They guarantee to offer genuine integrated health systems with support for Electronic Health Records (EHR). The evidence that is now available continues to point to these systems' incapacity to satisfactorily serve stakeholder demands. This present architecture has been under fire for being opaque and having a centralized authority for failure, attack, and ownership. Through intentional or unintentional behaviors of these intermediaries, a lack of confidence regarding the security and privacy of entrusted patient information is growing [4].

Figure 2. Global Health Information Exchange (HIE) google Countries wise trend analysis.

A. Blockchain In healthcare

1) Study Rationale

The trust gap prevalent in conventional HIE continues to be revealed as a result of competing interests, the inability of traditional HIE and PHR-based exchanges to deliver on the promise of a shared, integrated EHR, and a number of other factors. This distrust has grown as a result of privacy regulations and data breach incidents. Stakeholders are reluctant to cooperate or collaborate at the levels necessary for shared value as a result. The effect is lower health outcomes and rising healthcare expenses. Figure 1 shows the Google patterns over the past 20 years, which may help to

 ISBN: 978-1-68558-080-3

understand why HIE has attracted attention consistently over that time [4][5].

If this tendency is a clear indicator of contemporary global interests in Figure 2 it follows that these difficulties persist despite ten years of technical progress. We speculate that one major reason for the lack of advancement may be the trust gap. Blockchain is currently being used by researchers to assist solve some of these trust-related problems. The rising surge of interest in blockchain in healthcare has been stoked by this and a number of other factors.. The study in [4] was commissioned to learn more about this field of study and how it has developed.

2) Prior System Architectures

The following two prior Ethereum based architectures have been analyzing because the recent blockchain usage is primarily based on Ethereum due to its smart contract-based technology. The properties of the mentioned architectures are far better than the previous blockchain based architecture in previous years. These two are the latest to smart frameworks which are managing the data for health records. Data sharing that is both secure and scalable is necessary for group clinical decision-making. However, conventional clinical data initiatives are frequently segregated, which obstructs effective information interchange and hinders treatment decisions for patients [5].

The following restrictions apply to the Ficain DApp because it was created using various presumptions:

- Has no mention of semantic interoperability. The semantic interoperability problems that the FHIR standards have not yet completely accounted for cannot be solved by FHIRChain. Therefore, manual examination and mapping of preset ontologies by professionals in the fields of medicine and health data are needed to offer semantics to clinical data, and this will continue to be the major topic of our future research in this area.
- With older systems that do not support FHIR, compatibility issues might arise. Many historical systems may employ other communications norms, such as the more widely used HL7 v2 norms.
- It cannot prevent medical malpractice. Clinicians who are interested in working together to provide clinical decision assistance for patients in remote locations are the target users of FHIRChain. Our present design assumes that users won't abuse, mishandle, or unethically disseminate the data they communicate over our DApp.

- deployment fees for DApps. Contrary to popular public blockchains like Ethereum, our DApp is created utilising a private testnet with no transaction fees (e.g., transaction fees). Therefore, if our DApp was made available on a public blockchain, it would not be free. However, the ease of use offered by a public blockchain may make it more affordable to use than it would be to buy, operate, and maintain a proprietary clinical data exchange infrastructure [5].

The architecture, known as Ancile [6], combines smart contracts on an Ethereum-based blockchain for improved access control and data obfuscation in addition to advanced cryptographic techniques for added safety. In order to understand how the framework could address chronic privacy and security challenges in the healthcare industry, this article will look at how Ancile interacts with the diverse expectations of patients, providers, and other parties. Multiple parties may safely interact with the blockchain and its data thanks to Ancile. Ancile prioritizes secure contact, therefore the architecture we provide contains a number of additions intended to boost privacy and interoperability. The Ancile blockchain, in contrast to other blockchain EHR systems that have been developed, first maintains hashes of the data references while transferring the actual query link information in a private transaction via HTTPS.

The patient's ownership rights are the main emphasis of design. As a result, our design adheres to the notion that the patient owns the data and that it is not a commodity to be traded. As a result, Ancile does not include any mining incentives beyond the requirement to utilize the system.

We believe that governments and service providers already have an incentive to protect patient medical information. On the blockchain, we also take into consideration the various roles played by patients, providers, and third parties by using smart contract capabilities for access control. This enables the stratification of jobs to better serve the various demands of users [12].

It is important to note that many of the technologies used in the proposed Ethereum-based healthcare framework, such as permissioned blockchains and smart contracts, are still in the early stages of development. Therefore, the success of the framework is highly dependent on the success of these technologies. It should also be noted that the proposed solution, Ancile, should not be seen as a complete solution to the larger issue of Electronic Health Record (EHR) security. While it provides a method for re-encrypting a symmetric key using proxies selected by the patient in a pseudo-random manner, compliance with legal requirements for medical data and patient privacy protection requires that the proxy group and RC must have been formed beforehand using blockchain technology. Now that we know that blockchain technology is suffering from scalability issue Anicle [6], wouldn’t recommend solution.

The PHR blockchain architecture created in this study provides an effective solution for the management and usage of PHRs. The platform was originally presented in Southeast Asian countries through the Asia eHealth Information Network, [7] and it is currently the first PHR management platform for cross-regional medical data exchange (AeHIN).

In order to transmit, store, and share PHR data securely between patients and medical healthcare providers, a blockchain-based PHR exchange architecture and management platform was developed. Among its features are the ability to see PHRs for personal health management, exchange PHRs with a physician, and perform security checks on blockchain data. The PHR administration component's user interface has also been developed.

 ISBN: 978-1-68558-080-3

IV. PROPOSED HEALTH RECORD MANAGEMENT PLATFORM BLOCKCHAIN BASED KAFKA SMART CONTRACT HASH ARCHITECTURE

The study saved smart contract hash values in a blockchain to safeguard the PHR data and verify the accuracy of the PHR contents since blocks in a blockchain cannot be tampered with or maliciously altered. The blockchain architecture employed was Ethereum's private chain, and the Ethereum protocol's Geth (Go Ethereum) application was used to move transactions from the proposed platform to the blockchain exchange framework, produce new blocks, and establish a connection to the blockchain. as seen in Figure 4.

The data are encrypted while being transmitted over the network to prevent private information from being compromised. To protect the user's privacy, the platform encrypts the health record before uploading it to the safe database. A malicious attacker will only succeed in getting a set of random numbers if they try to access the block content. The encryption process combines asymmetric encryption with hash encryption. The block content is secured using a hash encryption method that transforms data into a collection of hexadecimal characters using SHA-256[9][13].

For scalability of data on the blockchain Apache Kafka has been introduced. The data blocks in the super peer's network are distributed using the Apache Kafka platform. By expanding its producer and consumer classes, which represent client nodes delivering and receiving data locks, respectively, Kafka abstracts application concerns about data replication [10][14][15].

To understand the dynamics of the apache Kafka and components the Figure 3 is displaying.

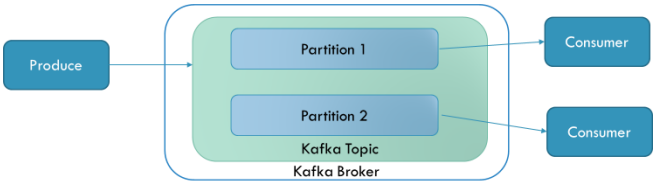

Figure 3. Apache Kafka Structure

Below Figure 4 shows the architecture of the Apache Kafka build Ethereum blockchain. The most well-liked distributed publish-subscribe messaging system is Kafka. Topics, brokers, producers, and consumers make up it. Topics are how Kafka groups a stream of messages. The producer sends out streaming messages, which are then retrieved by the consumer. One or more servers, referred to as brokers, make up a Kafka, which collects and stores data reliably before publishing relevant topics. Kafka cluster node status is monitored using Apache Zookeeper. A broker receives messages from producers. The customer obtains this information without any loss, and the broker retains it. (Performance Evaluation of Intrusion Detection Streaming Transactions Using Apache Kafka and Spark Streaming).

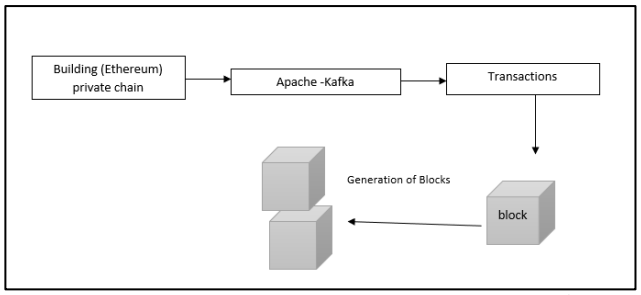

Figure 4. Proposed Private Blockchain built with Apache Kafka

Fast in-memory processing is offered by Apache Kafka. It is a flexible tool for a wide variety of large data processing applications since it is appropriate for both batch and streaming data.

These activities consist of interactive big data searches, graph processing, and machine learning [11]. Apache Kafka will increase effectiveness: The speed of block formation is increased, and waiting times for data interchange are decreased. extremely scalable and compatible: Additionally, intelligent collaborative construction may be finished.

While Apache Kafka is a powerful tool for real-time data processing, it is important to carefully consider its potential disadvantages, particularly in terms of system complexity, security, and message reliability, when evaluating its use for specific applications. Potential disadvantage is the complexity of configuring and managing a Kafka cluster. Setting up a Kafka cluster requires a deep understanding of the underlying system architecture, and can be challenging for organizations with limited technical expertise. In addition, Kafka lacks robust monitoring and management tools, which can make it difficult to diagnose and resolve issues when they arise.

Kafka's reliance on a publish-subscribe messaging model can sometimes result in message loss or duplication. While Kafka provides mechanisms for handling these issues, they can add additional complexity to the system architecture and require careful configuration to ensure reliable data processing.

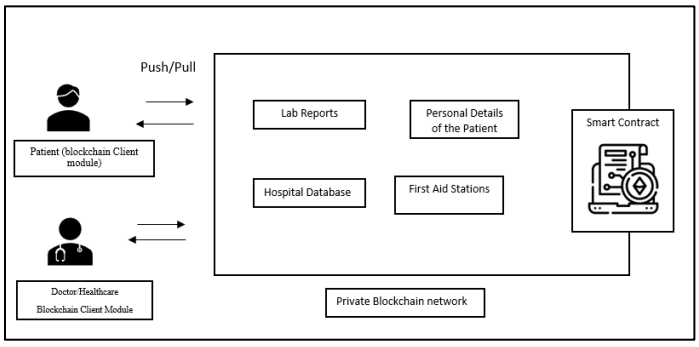

Figure 5. Proposed personal health record blockchain based Framework

V. PERFORMANCE METRICS

Blockchain security can be measured by various performance metrics. Some commonly used metrics to evaluate blockchain security include:

Decentralization: This metric measures the distribution of control within a blockchain network. A more decentralized network [2][3] is considered more secure as it is less susceptible to a single point of failure.

Consensus mechanism: This metric measures the method used to reach agreement on the state of the blockchain.

 ISBN: 978-1-68558-080-3

Different consensus mechanisms have different security properties, and some are considered more secure than others.

Hash rate: This metric measures the computational power of a blockchain network, and is an indicator of the security of the network against a 51% attack.

Network size: This metric measures the number of nodes in a blockchain network, and is an indicator of the security of the network against a Sybil attack [3].Network size will be easier to maintain.

Smart contract security: This metric measures the security of the smart contracts that run on the blockchain. Smart contracts can have vulnerabilities that can be exploited by attackers, so it is important to ensure that they are secure.

Auditing and testing: This metric measure the extent to which the codebase of the blockchain is audited and tested for security vulnerabilities [4]. It is important to note that security is a complex and multifaceted issue, and no single metric can fully capture it. Therefore, it is important to consider multiple metrics to get a comprehensive understanding [8] of the security of a blockchain.

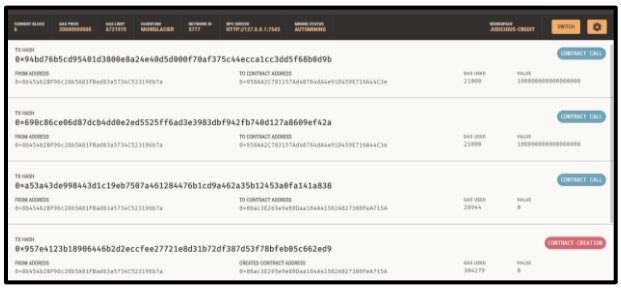

Figure 6. Blockchain generated Smart Contracts and contract calls on Ganache

Blockchain technology as in Figure 6, some transactions were done to implement private blockchain and it is often considered to be a secure and private way to conduct transactions, but there are certain factors that can affect the privacy of a blockchain network. Some performance metrics that can be used to evaluate the privacy of a blockchain include:

Anonymity: This metric measures the degree to which users are able to hide their identities on the blockchain. Anonymity can be achieved through techniques such as zero-knowledge proofs, ring signatures, and coin mixing.

Confidentiality: This metric measures the degree to which the details of transactions are kept private. Confidentiality can be achieved through techniques such as confidential transactions and zero-knowledge proofs.

Traceability: This metric measures the degree to which the transactions on the blockchain can be traced to specific individuals. Some blockchain networks, such as Bitcoin, have a high degree of traceability, while others, such as Monero, have been designed to provide a high degree of privacy.

Scalability: This metric with use of Apache Kafka will increase 6 times to manage the implementation with proposed framework.

Network analysis: This metric measures the degree to which the blockchain network can be analyzed to reveal information about the users and their transactions.

Data protection and encryption: This will potentially increase 80 times increasing the data protection via Apache Kafka. This metric measures the level of data protection and encryption implemented in the blockchain network to ensure the privacy of the data.

It is important to note that even though blockchain technology has some features that ensure privacy and security, it is not completely private. There are also other factors that can affect the privacy of a blockchain, such as the regulatory environment and the use of third-party services.

VI. DISCUSSION

This framework A blockchain-based personal health record (PHR)/EHR system has the potential to transform the PHR/EHR industry by providing a secure, decentralized, and tamper-proof way to store and share health information.

One of the main benefits of using a blockchain for PHR is the increased security it provides. Blockchain technology is inherently secure, as it uses advanced cryptography to ensure that once data is entered into the blockchain, it cannot be altered or deleted. This would help to prevent unauthorized access to sensitive health information and protect patients' privacy. Additionally, a blockchain-based PHR system would allow patients to have full control over their health data, enabling them to share their records with medical professionals and other authorized parties as needed. This would reduce the need for paper records and improve the speed and efficiency of care. Another potential benefit of using a blockchain for PHR is that it would enable the creation of a decentralized network of health data, allowing for better data sharing and collaboration among healthcare providers. This would enable healthcare providers to access a patient's complete health history, which could help to improve patient outcomes and reduce healthcare costs.

However, it is important to note that this technology is still in its early stages and there are still several challenges that need to be addressed such as data privacy, data security, interoperability, data sharing regulation and standardization.

We have created smart contracts and also worked on the Ethereum blockchain build with Apache Kafka where the scalability issue can be solved for the Ethereum blockchain in-case of wide adoption of the blockchain technology.

Work is in progress to create a complete interface for implementation of the proposed methodology majorly work remaining on the UI/UX off the health application and connecting the Ethereum blockchain build with Kafka and then the smart contracts with personal health records are saved in the

VII. CONCLUSION

Blockchain-based architecture is a distributed database system that uses a chain of blocks to store data in a decentralized manner. This architecture is highly secure, transparent, and immutable, making it useful for a wide range of applications. However, one of the main challenges with blockchain-based systems, including Ethereum, is scalability. This is due to the consensus mechanism, which requires all nodes in the network to process every transaction. To address this challenge, our proposed

 ISBN: 978-1-68558-080-3

framework combines Ethereum with Apache Kafka, a highly scalable and high-performance messaging platform.

The key features of our proposed architecture include decentralization, scalability, immutability, security, and transparency to increase potentially 6 times than the current available solutions. Decentralization ensures that the database is distributed across a network of computers, making it difficult for any one party to manipulate the data. Immutability ensures that once data has been added to the blockchain, it cannot be altered or deleted, ensuring the integrity of the records. Security is ensured through the use of cryptographic techniques, which prevent unauthorized access to the data. Transparency is provided by recording all transactions and changes to the database, which can be viewed by all parties.

Our proposed framework uses Apache Kafka as the underlying messaging platform for the Ethereum-based blockchain system, which offloads some of the workload from the Ethereum nodes and distributes it across a Kafka cluster. This improves the scalability of the system, allowing it to handle large volumes of data in real-time.

In summary, the use of a blockchain-based architecture can help to create secure, transparent, and decentralized record-keeping systems. Our proposed framework addresses the scalability challenge of Ethereum by using Apache Kafka, making it useful for a wide range of applications

VIII. FUTURE DIRECTIONS

Our proposed blockchain-based Personal Health Records (PHR) framework has several important points that make it a suitable candidate for full implementation:

Firstly, PHRs are critical for the foundation of precision medicine, which is the future of healthcare. Our PHR framework has the potential to be implemented on a large scale due to its scalability feature, which enables PHRs to be exchanged between nations and allows for potential precision medicine uses in the future. Secondly, financial data management systems have already successfully employed blockchain technology to secure data security and privacy. With improved system specifications and a greater private blockchain, work can be done to scale the framework and improve the user interface and user experience. Thirdly, the current global operations require the development of a cross-country medical care infrastructure, and our proposed blockchain-based PHR framework can play a significant role in this infrastructure. Lastly, by building the blockchain on a sidechain with better system specifications, we can yield better results, and smart contract transactions can be managed more effectively.

Overall, our proposed blockchain-based PHR framework has the potential to revolutionize the healthcare industry by providing a secure, transparent, and decentralized record-keeping system for patients' medical records. It is now time to move forward with full implementation of the proposed methodology.

ACKNOWLEDGEMENT

The authors would like to thank the Ministry of Higher Education Malaysia work is supported financially by the Ministry of Higher Education Malaysia via Fundamental Research Grant Scheme (FRGS/1/2019/ICT05/UM/01/1).

REFERENCES

[1] Hassan Mansur Hussien,*, Sharifah Md Yasin a,b,*, Nur Izura Udzir Mohd Izuan Hafez Ninggal a, Sadeq Salman Blockchain technology in the healthcare industry: Trends and opportunities,2021

[2] Yuri Choi 1,y, June-sung Kim 2,y, In Ho Kwon ,*, Taerim Kim 3 , Su Min Kim 4, Wonchul Cha 3,4,5, Jinwoo Jeong 1 and Jae-Ho Lee Development of a Mobile Personal Health Record:Application Designed for Emergency Care in Korea; Integrated Information from Multicenter Electronic Medical Records,2020

[3] Hsiu-An Lee, Hsin-Hua.Kung, BS; Jai Ganesh Udayasankaran, MSc, MBA; Boonchai Kijsanayotin3,4,7, MSc, MD, PhD; Alvin B Marcelos MD; Louis R Chao1, PhD; Chien-Yeh HsuAn Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study,2020

[4] Emeka Chukwu And Lalit Garg,A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations, Feburary 2020.

[5] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018, doi: 10.1016/j.csbj.2018.07.004.

[6] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustain. Cities Soc., vol. 39, no. December 2017, pp. 283–297, 2018, doi: 10.1016/j.scs.2018.02.014.

[7] Lee, A., Kung, H., Udayasankaran, J. G., Kijsanayotin, B., Marcelo, A. B., Chao, L. R., & Hsu, Y. (2020). An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study. Journal of Medical Internet Research, 22(6). https://doi.org/10.2196/16748

[8] Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in healthcare: A systematic review,” Healthc., vol. 7, no. 2, 2019, doi: 10.3390/healthcare7020056.

[9] Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, “A systematic review of the use of blockchain in healthcare,” Symmetry (Basel)., vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.

[10] A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, “Scalability Challenges in Healthcare Blockchain System-A Systematic Review,” IEEE Access, vol. 8, pp. 23663–23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

[11] Swathi and M. Venkatesan, “Scalability improvement and analysis of permissioned-blockchain,” ICT Express, vol. 7, no. 3, pp. 283–289, 2021, doi: 10.1016/j.icte.2021.08.015.

[12] K. Abbas, M. Afaq, T. A. Khan, and W. C. Song, “A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry,” Electron., vol. 9, no. 5, pp. 1–31, 2020, doi: 10.3390/electronics9050852.

[13] C. Martín, P. Langendoerfer, P. S. Zarrin, M. Díaz, and B. Rubio, “Kafka-ML: Connecting the data stream with ML/AI frameworks,” Futur. Gener. Comput. Syst., vol. 126, pp. 15–33, 2022, doi: 10.1016/j.future.2021.07.037

[14] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, “Analyzing the performance of a blockchain-based personal health record implementation,” J. Biomed. Inform., vol. 92, no. March, p. 103140, 2019, doi: 10.1016/j.jbi.2019.103140.

[15] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” Journal of Biomedical Informatics, vol. 71. pp. 70–81, 2017, doi: 10.1016/j.jbi.2017.05.012.

 ISBN: 978-1-68558-080-3

[16] Saxena, R., Arora, D., Nagar, V., & Mahapatra, S. (2023). Blockchain in Healthcare: A Review. Recent Advances in Blockchain Technology: Real-World Applications, 165-185.

[17] Tabassum, T., Akter, F., & Uddin, M. N. (2023). An Ethereum Blockchain-Based Healthcare System Using Smart Contract. In Applied Informatics for Industry 4.0 (pp. 34-45)

 ISBN: 978-1-68558-080-3