Enhancing Costly Blockchain Electronic Health Record Systems with Serverless Integration

Abhijay Rana
Co-Author
Bellarmine College Preparatory
San Jose, CA

Kevin Lu
Co-Author
Bellarmine College Preparatory
San Jose, CA

Rudransh Singh
Co-Author
Bellarmine College Preparatory
San Jose, CA

***Abstract*—Electronic Healthcare Records (EHRs) are becoming an increasingly popular method for hospitals to store digitized patient records and medical data. However, as hospitals have accelerated in their adoption of EHRs nationwide, the concern of cyberattacks has simultaneously surged as well, leaving patient data vulnerable to data breaches. Blockchain technology offers a potential solution to enhance EHR cybersecurity due to its decentralized and immutable storage capabilities. However, despite the robust security and effectiveness of blockchains, it faces widespread adoption issues from hospitals. In this paper, we explore the significant costs and setup complexity that currently hinder the use of blockchain in EHRs. In addition, we investigate how the serverless application of blockchain, which reduces server load and energy usage by utilizing cold starts instead of keeping servers continuously running, offers an affordable alternative to hospitals. By integrating serverless architectures with blockchain, hospitals can utilize both secure and scalable EHR systems, combating the rise in cyberattacks. This paper aims to provide a comprehensive framework for the implementation of serverless blockchain technology in EHR systems. We explore the current vulnerabilities in EHR systems, evaluate current cost barriers to implementing blockchain-based EHRs, and propose a practical architecture for serverless blockchain integration.**

***Index Terms*—blockchain, Electronic Healthcare Records, serverless implementation, cybersecurity**

I. Introduction

Hospitals nationwide are accelerating their adoption of Electronic Health Record (EHR) systems. These EHRs are digitally stored collections of patient charts, medical information, and data, allowing for streamlined data sharing among hospitals and increased ease of access. In attempts to improve hospital efficiency and reduce the data mishandling common in analog systems, EHR implementation mandates are becoming more common, with the Health Information Technology for Economic and Clinical Health Act and 21st Century Cures Act both incentivizing the transition in the United States.

However, with this increase in electronically stored healthcare data comes an increased burden for cybersecurity, which many hospitals struggle to meet. Last year, 133 million Americans were impacted by data breaches or leaks, costing hospitals an average of 10.93 million dollars, a 53 percent increase from 2023 [1], [2]. These cyberattacks also lead to hospital inoperability due to frozen healthcare data, totaling over 77 billion dollars in downtime costs since 2016 [3]. These data breaches harm hospitals and individuals in multiple ways. Aside from the immediate financial losses, hospitals risk reputational damage, while patients risk having personal security data exposed publicly. These attacks have worsened since the onset of the COVID-19 pandemic, with some attackers even directly targeting virus research facilities [4]. Blockchain technology has emerged as a promising solution to enhance EHR cybersecurity, with its decentralized, immutable storage offering increased resistance to cyberattacks. However, the primary barriers to widespread blockchain integration in EHR systems remain high energy demands and setup complexity, currently deterring adoption [5].

To explore the performance implications of two approaches, we conducted an experiment using two different API implementations. One environment simulated a brokerage using blockchain technology while the other leveraged an in-memory key-value store. We then assessed tradeoffs between these systems in regard to computational efficiency and transactional speed, determining the validity of concerns that blockchain-based records systems are not cost- and compute-effective.

Serverless technologies have the potential to level the playing field for hospitals on energy usage, server load, and ease of setup. However, though existing literature explores the theoretical benefits of implementing serverless blockchain systems, there exists no comprehensive technical discussion on the integration of serverless blockchain with existing EHRs. We further attempt to fill this gap by providing a detailed framework for the implementation of serverless blockchain technology in EHR systems.

The paper is structured as follows: In Section II, we investigate current technical vulnerabilities in EHRs and the potential for blockchain to be used as a solution. Section III provides our methodology for our comparative investigation on blockchain and centralized system costs. In Section IV, we analyze our results and explore the benefits of implementing serverless technology on blockchain adoption. Finally, we explain how these serverless systems would work in practice.

II. Background

The centralized and insecure nature of current EHRs increases susceptibility to cyberattacks. Specifically, hospitals are falling victim to three main attacks: distributed denial of service (DDoS), ransomware, and phishing. DDoS attacks occur when attackers use large numbers of machines to compromise hospital systems by overwhelming hospital servers with requests. During the COVID pandemic, the number of DDoS attacks increased by 90% because server load was inherently higher from real patients [6]. Ransomware attacks occur when attackers either overwhelm

hospital systems and demand payment in exchange for freeing the servers or inject malware into hospital servers. After injecting malware, attackers either demand ransom for returning server access to the hospitals or returning access to patient data to continue treatment. These attacks are permitted by current EHRs due to their centralized and less secure nature, meaning that if the singular "node" is overwhelmed or injected with malware, all hospital functions halt because their singular point of data access is disabled [7]. Finally, phishing attacks occur when hospital employees unknowingly leak patient data through unauthorized channels. Both phishing and ransomware attacks occur when attackers can gain unauthorized access to hospital servers, but blockchain technology can be the solution to this, along with most other cybersecurity vulnerabilities in EHRs. Blockchain has been proposed by many as a solution to improve the security of EHRs against cyberware attacks and data breaches as it provides a decentralized and immutable alternative to storing patient data on hospital servers. [8].

Blockchain technology enhances data access control by implementing a transparent, automated, and cryptographically-based method to manage authorization roles. The decentralized nature of blockchain addresses the cyberattacks that current obsolete, centralized EHRs do not prevent. For example, decentralization improves DDoS mitigation by spreading detection and response duties across numerous nodes, removing single points of failure, and maintaining network integrity even if some nodes are compromised [21]. Similarly, the implementation of blockchain-based security frameworks such as BSFR-SH has proven to increase detection and defense against ransomware attacks by allowing constant data access even during a cyberattack, preventing attackers from holding hospital records hostage [22]. Further, the immutability and linked-list structure of blockchain enables a transparent version history that allows patients to check for data tampering. Specifically, permissions can be enforced through smart contracts deployed directly on the chain; i.e. patients can determine how long providers are allowed to access their health records and which files they are allowed access to in the first place. This is particularly important in regard to healthcare data, where patient records need to be securely managed to prevent unauthorized access and potential breaches [9]. For example, phishing attempts are less likely to result in unauthorized access to sensitive patient data since attackers would only gain access to the minimal data associated with the compromised user's role. Smart contracts can enforce access control policies automatically. Suppose suspicious activity is detected (e.g., multiple login attempts from different locations), smart contracts can dynamically adjust access rights or trigger alerts. In conjunction with artificial intelligence-enabled detection methods, the blockchain can use hybrid deep learning-based approaches combining autoencoder and multi-layer perceptron techniques based on unfettered access to internal data and traffic analytics to mitigate DDoS attacks [10]. However, this application is beyond the scope of this paper. Beyond its desirability for cybersecurity, blockchain provides an interoperable, standardized network that enables easy data exchange between multiple health providers. This reduces treatment costs and time due to redundant diagnostic tests so doctors can provide better care. The blockchain's immutability and linked-list structure enable a transparent version history that allows patients to check for data tampering.

However, implementing blockchain in EHR systems presents challenges that have prevented its widespread adoption. The high cost associated with blockchain implementation in EHR systems is a major barrier, as it requires substantial investment in computing power, infrastructure, and expertise [11]. Moreover, the difficulty of setup arises from the complexity of integrating blockchain technology with existing health information technology systems, leading to challenges in interoperability and scalability [12]. The lack of technical information and guidance on setting up blockchain-based EHR systems further complicates the implementation process, as it requires specialized knowledge and expertise in blockchain technology [13]. Additionally, the complexity of integrating blockchain with existing EHR systems and training healthcare staff on new technologies further adds to the overall cost of implementation [14]. Furthermore, the need for efficient consensus algorithms, security and privacy vulnerabilities, and user resistance adds to the challenges of implementing blockchain in EHR systems [11]. Integrating blockchain with cloud-based EHR systems also poses feasibility and scalability challenges, further contributing to the complexity of implementation [13]. Ensuring secure access control, data sharing, and privacy preservation in blockchain-based EHR systems requires sophisticated encryption, access control mechanisms, and interoperability with existing EHR systems [15].

III. Methodology

In this experiment, we aim to establish a quantitative comparison between request speed and relative costs of blockchain-based environments and centralized environments, to validate concerns regarding high costs for blockchain environments. The experiment has two scenarios, both implement a simple brokerage, for the purposes of extracting data about computational complexity - one implemented a blockchain ledger with private and public key authentication while the other used an in-memory object. The blockchain version implements three main classes: (i) Transaction – stores details like the sender's address, recipient's address, and content. It can sign transactions with a private key and validate them using the corresponding public key. (ii) Block – represents a block in the blockchain. Each block contains a timestamp, a list of transactions, the hash of the previous block, a nonce, and its own hash. The block can be mined by finding a hash that meets a certain difficulty level, and it validates the transactions it contains. (iii) Chain – manages the entire blockchain. It stores a list of blocks, handles the creation of new blocks, verifies the validity of the blockchain, and processes transactions. It includes methods for mining pending transactions, checking the balance of a specific address, and retrieving all transactions related to a specific address. The system uses SHA256 cryptographic hashing and elliptic curve cryptography for signing and verifying transactions. Both were written in JavaScript

for convenience, but since the results only depend on comparison, the speed of the language is irrelevant. The "regular" version implements a single class: Store. It stores users in a dictionary with individual balances and updates them per transaction. For each experiment, a public-facing REST-API was set up with three entry points: (i) POST "/create" (ii) GET "/balance" (iii) POST "/transaction." Then using Artillery, an open-source testing toolkit, we log results from a load-testing batch to record transaction latency. The CLI creates three phases that slowly ramp up in intensity and cycle through multiple, virtual users, completing a total of 1230 trials for each environment.

IV. Discussion and Serverless Solution

This section presents the results and key findings from our experiment. We load-tested two RESTful environments over thousands of server requests, comparing the blockchain setup with a traditional non-blockchain environment. We focused on metrics such as HTTPS request speed and the number of requests processed over time to compare the two environments under various load conditions.

In terms of HTTPS request speed, the non-blockchain RESTful environment demonstrated a faster average speed, as shown in Table 1. In the blockchain environment, response times ranged from a minimum of 4 milliseconds to a maximum of 72 milliseconds, with a mean response time of 7.4 milliseconds. The distribution of response times reveals that 75 percent of requests were completed within 7.9 milliseconds, 90 percent within 10.1 milliseconds, and 95 percent within 12.1 milliseconds. However, the 99th and 99.9th percentile saw sharp increases, with response times reaching 22 milliseconds and 37.7 milliseconds respectively. This suggests that the blockchain environment may be handling most requests generally efficiently, but there is a tail of significantly slower responses, likely due to anomalous delays with consensus and transaction validation.

TABLE I
Average HTTPS Response Times

Statistic	Blockchain (ms)	Centralized (ms)
Minimum (min)	4	0
Maximum (max)	72	24
Count	1230	1230
Mean	7.4	1.2
50th Percentile (p50)	7	1
Median	7	1
75th Percentile (p75)	7.9	1
90th Percentile (p90)	10.1	2
95th Percentile (p95)	12.1	2
99th Percentile (p99)	22	5
99.9th Percentile (p999)	37.7	21.1

In contrast, the non-blockchain conventional environment saw significantly faster and more consistent response times. The response time ranged from 0 milliseconds to a maximum of 24 milliseconds, significantly lower than the maximum time for the blockchain environment. The mean was just 1 millisecond, below one-seventh less. At the 75th percentile, times were still below 1 millisecond, and even at the 90th and 95th percentile, the average time was 2 milliseconds. Only at the 99th and 99.9th percentile did the time begin to increase, but even here the increase to 5 milliseconds and 21.1 milliseconds respectively in the centralized environment was significantly lower than the edge cases for the blockchain environment.

Figure 1 and Figure 2, which graph the number of HTTP requests processed over time in the blockchain and centralized environments respectively, explain this difference further. Figure 1 shows a delayed but sharp spike in request processing toward the end of the testing period. This suggests that the blockchain system accumulates requests due to the overhead time spend in consensus and validation processes, causing higher response times. Figure 2 shows that in the centralized environment, there is a steady and consistent increase in processed tweets over time. There is negligible loss in uniformity and efficiency in the centralized system, compared to the blockchain in Figure 1. These findings highlight the significant performance gap between the two environments, with the non-blockchain setup outperforming the blockchain environment in terms of both speed and consistency.

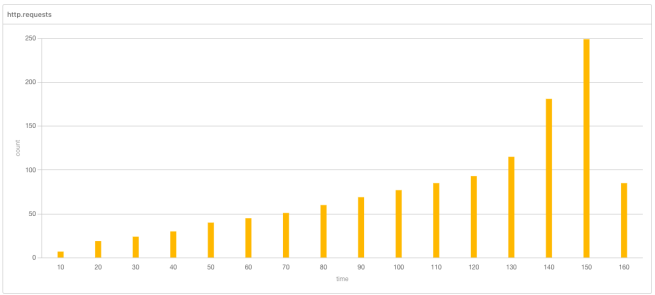

Fig. 1. Completed HTTP requests over time in a blockchain environment

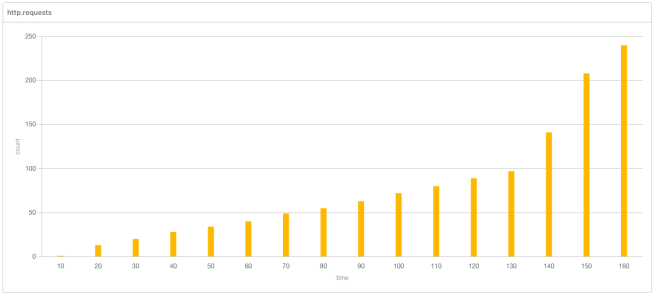

Fig. 2. Completed HTTP requests over time in a centralized environment

Moreover, the impacts of this gap extend beyond just response speed, especially for hospitals that are operating on scales of hundreds of thousands of requests on already limited and expensive compute capacity. When response times are slow, multiple processes are waiting for the CPU to complete its cycles, leading to additional time in between context switching and an increase in context switching as well. The server also becomes backlogged with queues which results in higher CPU usage, ultimately yielding a larger cost barrier to overcome to implement this technology. Our scenario involving blockchain ran on average 7 times as slow as the centralized data storage

experiment which shows that larger computational power would be involved and thus heftier costs would ensue.

To combat this barrier, we propose a serverless solution. The alternative of employing serverless computing instead of traditional centralized computing for electronic health record systems poses a massive upside due to the economic and performance advantages provided by multi-tenanted, inter-machine parallelism.

A. How does serverless overcome the obstacles of blockchain adoption?

Common concerns about cost, complexity, and performance of existing enterprise blockchain solutions erect huge barriers to entry, especially for an already resource-constrained industry like healthcare. Thus, the alternative of employing serverless computing instead of traditional centralized computing for electronic health record systems poses a massive upside due to the economic and performance advantages provided by multi-tenanted, inter-machine parallelism. In fact, serverless architectures for cloud computing have seen a massive boom in adoption with the entire market projected to grow from 3 billion dollars in 2017 to 22 billion dollars while being used by 50 percent of global companies in 2025 [16]. Broadly, serverless computers offer both scalability and affordability, reducing stress for developer operation teams. In this paradigm, instead of software being run on centralized monoliths that waste compute resources during periods of low usage, the serverless architecture automatically spins up lightweight virtual machines with only milliseconds of delay, referred to as cold start, and can spin these machines down after usage, making cloud bills cheaper by cutting down on idle time. Those cost savings are significant because blockchain networks are orders of magnitude more expensive than centralized database management systems. Novel applications of serverless onto blockchain are cheaper by 10 times or even 100 times for low throughput and cheaper by 3 times for high throughput defined by 100 tx/s or more when compared to non-serverless blockchain solutions like Quorum or Fabric operating on a server-based, single-box approach [19]. That means on average, FaaS, function as a service, was 90 percent cheaper than PaaS, platform as a service, through the elimination of idle server time [20]. In fact, making blockchain developer-friendly and auto-scaling is the lynchpin for wider adoption, a trend seen in the past with EMRs [18]. This level of compute optimization makes adopting blockchain solutions sensible for often resource-constrained hospitals. In addition to cost savings, reducing technical overhead is the most significant benefit of serverless computing. IT teams no longer have to routinely manage or maintain server architecture to manually provision, patch, scale, and monitor network usage. Currently, no solution employs serverless technology to deploy blockchains. The closest implementation is Amazon's Quantum Ledger Database, which is a centralized ledger solution but evidently not a blockchain. The problem here is the lack of a consensus algorithm which is vital for the data integrity of transactions between different entities, such as between hospitals, clinics, pharmacies, insurance companies, and other providers.

B. What are some cloud services that can be used?

Since blockchain solutions have multiple, compartmentalized components such as certificate authorities, membership service providers, a network of nodes, organizational units, and policies, a microservice-centered serverless approach perfectly fits this role. Serverless webhooks are designed to be triggered on an event, which works seamlessly for smart contract deployment.

1) Serverless Environments: Every single node needs to run serverless instances of the blockchain's gateway software and membership service provider while preserving the ledger's world state and transaction log within a serverless database, which dynamically adjusts capacity based on application demands, automatically scales input, output, and storage volume, and can instantly shut down, start-up, and scale to accommodate varying workloads, all without requiring users to manage individual instances. To manage these serverless environments, AWS Step Functions is a tool that orchestrates AWS Lambda functions and has HIPAA-eligibility status covered under the AWS Business Associate Addendum, a contract required under HIPAA rules that acknowledges appropriate safeguards for protected health information in place. In addition, regulatory compliance is easier than ever with the AWS HIPAA program, which provides secure, sanitized environments to process, maintain, and store protected health information.

2) Persistent Storage: Besides regulatory compliance, major cloud service providers provide multiple services of interest that serve technical needs. The following recommendations are mainly serviced by AWS, which offers the shortest cold start and cheapest billing in most cases. For databases, DynamoDB, FaunaDB, and RDS provide solid, cloud-managed solutions for persistent data storage.

3) Orchestration and Logging: To handle requests and compute allocation, services like API Gateway, Lambda, and Amazon MQ offer secure endpoints for the transfer of protected health information. Orchestration and upkeep for these microservices can be done with Terraform, which is an infrastructure-as-a-code tool, and CloudWatch to programmatically monitor operational logs to discover insight and troubleshoot issues [19].

The most practical way to implement a serverless blockchain is to create serverless implementations of peers, gateways, and orderers while strapping on existing solutions such as Hyperledger Fabric's modules for certificate authorities, policy processing, and membership service providers. This reduces development costs because it ensures only the most compute-intensive processes are rewritten. Figure 3 shows a schematic for the implementation of a Hyperledger Fabric-style blockchain. Briefly put, both peers and the orderer participate in a structured process to reach consensus. Designated endorsing peers simulate and approve transactions based on pre-established policies when a client sends an API Gateway transaction request. The orderer receives the endorsed transactions and employs Kafka as a messaging channel to dependably sort the transactions into blocks. Next, all peers receive these arranged blocks. Before committing the transactions to the blockchain, peers verify that they follow the rules of the network. Queries that require efficient read-only access to the blockchain data bypass the orderer and go straight to

the peers. All this is achieved through serverless functions and serverless persistent data storage.

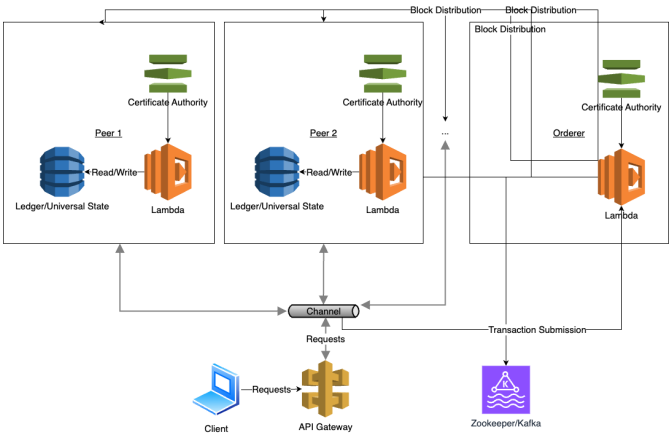

Fig. 3. Schematic for implementing a Hyperledger Fabric-style blockchain

While more secure, the serverless approach explained above has two potential problems. First, serverless functions incur cold start, or the initial delay due to cloud service providers initializing a new instance of the function to service an income request. As the AWS documentation explains, cold start occurs for 1 percent of innovations and can range from 100ms to over 1 second. Although this may seem fine at first, for our infrastructure that has tens if not hundreds of compartmentalized serverless functions, these delays can rack up. Currently, there are two solutions to mitigate cold start. The first idea is to provision a pre-warmed instance called "provisioned concurrency." The issue with this approach is increased cost which arguably turns serverless functions into always-on monoliths, which detracts from its cost-saving potential. The second idea is optimizing the function initialization workflow. Currently, they use a MicroVM manager known as Firecracker for AWS lambda. The issue with Firecracker is its documented inability to reclaim memory or storage after an idling VM no longer needs the resources, therefore making it a massive memory and disk hog. Using alternative managers like QEMU could provide significant performance gains [20]. But recently, a more novel approach for javascript environments was to utilize v8 isolates, which have their isolated contexts that can be run side by side on VMs, and are far more lightweight and therefore faster to spin up. Using this concept for high-performance languages like Golang, which powers most of Hypderledger's services, can significantly increase speed and cut down on cold starts. A second problem is vendor lock-in, which occurs when healthcare providers become too dependent on one specific serverless blockchain for their EHR, making it too expensive to switch to another system. This occurs when there is advanced proprietary technology developed without a focus on interoperability, along with unique smart contracts and compliance requirements. These lock-ins can lead to higher costs, reduced flexibility, and decreased negotiation power, ultimately making it difficult for healthcare providers to adopt more efficient solutions in the future. However, solutions like OpenFaaS and Knative can bridge the gap by providing a vendor-agnostic way to write serverless functions that then are deployed on separate CSPs. Another key point of discussion is the need for effective data migration strategies. Transitioning existing patient data from traditional EHR systems to a blockchain-based system requires careful planning to avoid data loss and ensure consistency. Hospitals must develop protocols for secure data transfer and validation to maintain the integrity of patient records during the migration process. This involves several stages, including data extraction from the old system, data cleansing to remove inconsistencies, data transformation to fit the blockchain schema, and thorough testing to verify that all data has been accurately transferred, and encryption methods should be applied to safeguard sensitive information against breaches.

A problem may also arise from transferring of data to the serverless environment. Data extraction involves pulling all relevant patient records from the existing EHR system. This step must account for various data formats and sources to ensure a comprehensive migration. Following extraction, data cleansing is critical to identify and rectify errors, duplicates, and incomplete records. This ensures the accuracy and reliability of the data being migrated. Data transformation aligns the extracted data with the new blockchain schema. This may require mapping old data fields to new ones, ensuring compatibility with the blockchain's structure and standards. Automating this process with ETL tools can enhance efficiency and accuracy. Thorough testing is essential to validate the migration process. This includes running test migrations with sample data to identify potential issues before the full-scale migration. Verification steps should include checking data integrity, accuracy, and completeness to ensure no data is lost or altered during the process. Post-migration validation involves comparing the data in the new blockchain-based system with the original data to ensure consistency. Hospitals should implement audit trails to track the migration process and provide transparency. These trails can help identify and resolve discrepancies quickly. Additionally, encryption methods should be employed throughout the migration to protect sensitive patient information from unauthorized access. This includes using encryption protocols during data transfer and at rest.

V. Conclusion and Future Work

In this paper, we discussed the benefits of implementing blockchain technology into existing electronic healthcare record systems. Existing systems have proven to be inadequate for hospitals to store their patient data effectively and securely. They lack the proper technology to store data and choose to do so in centralized systems, which makes patient data increasingly vulnerable to cyberattacks such as DDoS, ransomware, and phishing attacks. These attacks have shown to be costly, violating patients' private data and costing hospitals millions, if not billions, of dollars. Blockchain has been a recommended solution to this evident problem, but has been an unpopular solution because of concerns around cost and performance, and worries that it would force hospitals to allocate a large amount of funding to improving computing power and infrastructure to support the blockchain. In this paper, our experiment found that blockchain-based environments run at speeds up to 7 times slower than centralized environments, validating these concerns. However, serverless blockchains may be

an effective solution as serverless computing breaks down the high cost barrier that is associated with blockchain technology, providing a potentially secure and affordable solution to hospitals. We propose a serverless blockchain-based solution to store as well as service a decentralized ledger that can leverage existing, easy-to-use cloud services. The serverless alternative would also require less technical knowledge for the IT teams that implement and maintain the software, providing a straightforward and affordable solution to hospitals.

Future research must expand on the full-scale and practical implementations of these decentralized EHRs. Investigations must be made into the compliance of these decentralized ledgers with legal frameworks and ethical guidelines. Further, it is critical to develop systems for the contained and secure migration of existing hospital data onto these new ledgers. Finally, along with research into alternative serverless technologies for more efficiency, researchers can explore augmenting this serverless data storage and its potentially high costs through the incorporation of artificial intelligence and machine learning algorithms to optimize cloud runtimes, potentially finding ways to reduce function costs with increased training data over time. The integration of artificial intelligence and machine learning into serverless blockchain systems offers significant potential for optimization. AI and ML can analyze historical usage patterns to predict future demands and dynamically adjust resource allocation, thereby reducing costs and improving efficiency. For instance, predictive models can identify peak usage times and prewarm serverless functions to mitigate cold start issues. AI-driven optimization can also enhance load balancing and fault tolerance within the blockchain network, ensuring that the system remains resilient and efficient under varying workloads. Developing systems for the secure migration of existing hospital data to blockchain-based systems is critical, and an investigation into the use of ETL tools should be conducted.

REFERENCES

[1] U.S. Department of Health and Human Services, "U.S. Department of Health and Human Services - Office for Civil Rights," Hhs.gov, 2024. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. [Accessed: 1-Jul-2024].

[2] IBM, "Cost of a Data Breach Report 2023," 2023. [Online]. Available: https://www.ibm.com/downloads/cas/E3G5JMBP.[Accessed: 3-Jul-2024].

[3] P. Bischoff, "Ransomware Attacks on US Healthcare Organizations Cost 20.8bn in 2020," Comparitech, Feb. 11, 2020. [Online]. Available: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/. [Accessed: 5-Jul-2024].

[4] M. Muthuppalaniappan and K. Stevenson, "Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health," International Journal for Quality in Health Care, vol. 33, no. 1, Sep. 2020. [Online]. Available: https://doi.org/10.1093/intqhc/mzaa117. [Accessed: 6-Jul-2024].

[5] Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain Technology for Electronic Health Records," International Journal of Environmental Research and Public Health, vol. 19, no. 23, p. 15577, Nov. 2022. [Online]. Available: https://doi.org/10.3390/ijerph192315577. [Accessed: 29-Jun-2024].

[6] Z. Zhou, A. Gaurav, B. B. Gupta, H. Hamdi, and N. Nedjah, "A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic," Neural Computing and Applications, Sep. 2021. [Online]. Available: https://doi.org/10.1007/s00521-021-06389-6. [Accessed: 3-Jul-2024].

[7] N. Thamer and R. Alubady, "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," 2021 1st Babylon International Conference on Information Technology and Science (BICITS), Apr. 2021. [Online]. Available: https://doi.org/10.1109/bicits51482.2021.9509877. [Accessed: 5-Jul-2024].

[8] A. H. Mayer, C. A. da Costa, and R. da R. Righi, "Electronic health records in a Blockchain: A systematic review," Health Informatics Journal, vol. 26, no. 2, p. 146045821986635, Sep. 2019. [Online]. Available: https://doi.org/10.1177/1460458219866350. [Accessed: 3-Jun-2024].

[9] A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," Transactions on Emerging Telecommunications Technologies, Aug. 2021. [Online]. Available: https://doi.org/10.1002/ett.4333. [Accessed: 13-Jun-2024].

[10] T. Liu, F. Sabrina, J. Jang-Jaccard, W. Xu, and Y. Wei, "Artificial Intelligence-Enabled DDoS Detection for Blockchain-Based Smart Transport Systems," Sensors, vol. 22, no. 1, p. 32, Dec. 2021. [Online]. Available: https://doi.org/10.3390/s22010032. [Accessed: 15-Jun-2024].

[11] P. Durneva, K. Cousins, and M. Chen, "Blockchain Technology in Patient Care: Current State of Research, Challenges and Future Research Directions (Preprint)," Journal of Medical Internet Research, vol. 22, no. 7, Mar. 2020. [Online]. Available: https://doi.org/10.2196/18619. [Accessed: 31-May-2024].

[12] A. D. Samala and S. Rawas, "Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability. — International Journal of Online and Biomedical Engineering — EBSCOhost," openurl.ebsco.com, Feb. 01, 2024. [Online]. Available: https://doi.org/10.3991/ijoe.v20i02.45693. [Accessed: 9-Jun-2024].

[13] J. H. Beinke, C. Fitte, and F. Teuteberg, "Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study," Journal of Medical Internet Research, vol. 21, no. 10, p. e13585, Aug. 2019. [Online]. Available: https://doi.org/10.2196/13585. [Accessed: 8-Jun-2024].

[14] V. Louis and P. Maheshwari, "Blockchain Technology in Healthcare, Current and Future Trends – A Systematic Review," Mar. 2023. [Online]. Available: https://doi.org/10.21203/rs.3.rs-2613305/v1. [Accessed: 19-Jun-2024].

[15] Rihab Benaich, Saida El Mendili, and Youssef Gahi, "Moving Towards Blockchain-Based Methods for Revitalizing Healthcare Domain," Lecture notes in networks and systems, pp. 16–29, Jan. 2023. [Online]. Available: https://doi.org/10.1007/978-3-031-42317-8_2. [Accessed: 14-Jun-2024].

[16] J. Wen, Z. Chen, X. Jin, and X. Liu, "Rise of the Planet of Serverless Computing: A Systematic Review," ACM Transactions on Software Engineering and Methodology, Jan. 2023. [Online]. Available: https://doi.org/10.1145/3579643. [Accessed: 3-Jul-2024].

[17] Johannes Sedlmeir, T. Wagner, E. Djerekarov, R. Green, Johannes Klepsch, and S. Rao, "A Serverless Distributed Ledger for Enterprises," arXiv (Cornell University), Jan. 2021. [Online]. Available: https://doi.org/10.48550/arxiv.2110.09221. [Accessed: 4-Jul-2024].

[18] A. Kaplunovich, Karuna Pande Joshi, and Y. Yesha, "Scalability Analysis of Blockchain on a Serverless Cloud," Maryland Shared Open Access Repository (USMAI Consortium), Dec. 2019. [Online]. Available: https://doi.org/10.1109/bigdata47090.2019.9005529. [Accessed: 5-Jul-2024].

[19] A. Kumari and B. Sahoo, "Serverless Architecture for Healthcare Management Systems," Advances in healthcare information systems and administration book series, pp. 203–227, Jun. 2022. [Online]. Available: https://doi.org/10.4018/978-1-6684-4580-8.ch011. [Accessed: 12-Jun-2024].

[20] H. Dutka, "Why We Replaced Firecracker with QEMU," Hocus Blog, Jul. 10, 2023. [Online]. Available: https://hocus.dev/blog/qemu-vs-firecracker. [Accessed: 21-Jun-2024].

[21] R. Chaganti, B. Bhushan, and V. Ravi, "A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions," Computer Communications, vol. 197, pp. 96–112, Jan. 2023. [Online]. Available: https://doi.org/10.1016/j.comcom.2022.10.026. [Accessed: 8-Jul-2024]

[22] M. Wazid, A. K. Das, and S. Shetty, "BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare," IEEE Transactions on Consumer Electronics, pp. 1–1, 2022. [Online]. Available: https://doi.org/10.1109/tce.2022.3208795. [Accessed: 5-Jul-2024]