Human-centric Computing and Information Sciences

November 2022 | Volume 12

www.hcisjournal.com

KIPS Korea Information Processing Society

KIPS CSWRG Korea Information Processing Society Computer Software Research Group

HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2022) 12:55
DOI: https://doi.org/10.22967/HCIS.2022.12.055
Received: January 24, 2022; Accepted: March 21, 2022; Published: November 30, 2022

choicocake

Healthcare Ledger Management: A Blockchain and Machine Learning-Enabled Novel and Secure Architecture for Medical Industry

Abdullah Ayub Khan[1,2], Asif Ali Laghari[1], Muhammad Shafiq[3,*], Omar Cheikhrouhou[4], Wajdi Alhakami[5], Habib Hamam[6], and Zaffar Ahmed Shaikh[2]

Abstract

Distributed transactions in e-Healthcare and the evaluation of medical data have become an active research area of information technology that delivers medical records management and optimization without manually visualizing the computational loss. The increased use of e-Healthcare applications for availing medical services requires efficient computation during the processing of medical transactions and preservation through intelligent measurement analysis. Medical industries often involve and aim for the smooth application of medical transmission of demanding services. Thus, there are significant requirements for calculating loss during optimization and management in the distributed private network. In this paper, we contribute to two different objectives. First, we propose a machine learning-based stochastic gradient descent method for managing medical records and optimizing day-to-day transactions of e-Healthcare applications. This approach evaluates the loss of medical features during computation and enables optimized details of data transmission. Secondly, a blockchain-distributed E-Healthcare novel and a secure serverless architecture are proposed for the medical industry to protect transactions and preserve immutable storage. The simulation result shows the proposed system computations, such as loss = 0.7 (7%), learning-rate = goldilocks, ledger optimization =0.23 (23%), transmission power = -18 dBm, jitter = 32 ms, delay =90 ms, throughput = 170 bytes, duty-cycle and delivery = 0.10(10%), and calculate dynamic response.

Keywords

Smart Contracts, Blockchain, Machine Learning (ML), Stochastic Gradient Descent (SGD), E-Healthcare, Information Management and Optimization

1. Introduction

E-Healthcare applicational medical records management is the process of scheduling, sorting, examining, analyzing, and preserving patients' sensitive information [1]. It can help to track patients' causes of diseases, establish efficient monitoring to improve treatment processes and establish effective manufacturing of

***Corresponding Author:** Muhammad Shafiq (mshafiq@ieee.org)
[1]Department of Computer Science, Sindh Madressatul Islam University, Karachi, Sindh, Pakistan
[2]Faculty of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, Sindh, Pakistan
[3]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China
[4]CSE Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax, Tunisia
[5]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
[6]Faculty of Engineering, Moncton University, Moncton, Canada

medicines with accurate record prevention. The current strategy of information transactions, management, and delivery includes medical services requests and availing, services scheduling with cost-efficiency and documenting, recording patients' emergency complaints, manual diagnosis, counseling, and corresponding treatment evaluated in health information for the medical industry [2, 3]. Nowadays, the advancement in information technology makes the transmission of digital data electronically through e-Healthcare applications; and so, the big data of medical transactions evolves and needs dynamic, cost-efficient investigation and management problems come into existence [4]. To manage efficient e-Healthcare transactions, the generation of electronic medical data needs efficient run-time processing, classification, and prediction of the futuristic rate of data emergence. Often, these investigational records are required to be shared among different healthcare sectors. It also includes the pharmaceutical and medical device industries, health insurance providers, researchers, pharmacists, and other stakeholders [5, 6]. These challenging aspects pose serious problems in handling day-to-day generated patients' sensitive data.

The existing processes for capturing health-related data during processing are insecure. The lifecycle of medical data scheduling, processing, organizing, and managing requires consideration. Secondly, to investigate individual aspects of processed information before transmission over the network in terms of integrity, confidentiality, transparency, and provenance [7, 8]. And so, preserve each piece of investigated information in the server-based centralized storage or cloud environment. These investigated records are helpful in the diagnostic, treatment classification, medicine recommendation, and futuristic prediction of data generation and the required level of medical production.

However, the patients of e-Healthcare may receive transfer consulting from one hospital to another hospital during the treatment process [9]. Patients have the right to define access control by stating what type of data will be shared and how long with whom [9, 10]. There is still an uncertain manner derived for stakeholders participating between two different channels, in which authentic users can get control access (read-only) to sensitive health records [11, 12]. Substantially, the process of exchanging the patients' records between different channels creates a complex environment, such as platform interoperable related issues. With the new trend towards personalized healthcare for efficient treatment, diagnosis, and medicine production, existing e-Healthcare systems that utilize server-based centralized procedures are restricted when it comes to providing a cohesive view and protected shared access control to the medical history of the patient, diagnosis, and health-related transactions with participating stakeholders (authentic). In fact, the e-Healthcare data of the centralized-server approach is vulnerable in terms of alteration, redundancy, and tampering or forgery that can lead to data integrity, transparency, and provenance problems. In addition, all the people who are involved, including the patients, need to trust the central-service experts and be aware of their current security and protection procedures [13, 14].

The preserved e-Healthcare patient diagnostic and health-related records need to be utilized for futuristic predictive analysis, management, and optimization [15]. Individual recorded medical entities are investigated in accordance with the rate of quality measurement of patients' diseases and getting efficient treatments on time, the transmission of medical service deliveries, consultant prescription-related information, etc. For this purpose, machine learning (ML) is used to formulate predictive models. It starts with the features and labels of recorded health data to design a prediction function, as shown in Fig. 1. By training the complete model, there is a need to tune parameters at each stage of data selection and examination. The overall process of predictive futuristic health-related information evaluates the loss of data points in optimization and management, as shown in Fig. 1.

Blockchain e-Healthcare can strengthen security, provide serverless hash-based (SHA-256) encryption performance, and store health records and service delivery transactions on an immutable distributed storage. However, the event of medical node transactions can be stored in a gazette-like chain structure that is connected through different channels in a serverless private network. These business rules are managed and controlled via digital contracts (smart) to achieve distributed automated health service deliveries and emergency responses through the applications in the serverless environment. Many medical industries envisioned the purpose of achieving digital ledger integrity, traceability, provenance, and immutability to enable distributed medical preservation in immutable storage and analysis. The reason

for the movement towards a decentralized environment is to protect medical ledgers against a variety of cyber-attacks usually intended for server-based centralized systems [17, 18]. This blockchain decentralized procedure of protected serverless network enables us to enhance the distributed medical nodes' defense ability with hash-based re-encryption along with the blockchain Hyperledger intrusion detection mechanism and preservation. The design of customized blockchain consensus policies ensures the secure transmission and delivery of health services, as well as immutability, distributed trust, integrity, and transparency in the transactions of each node in the chain.

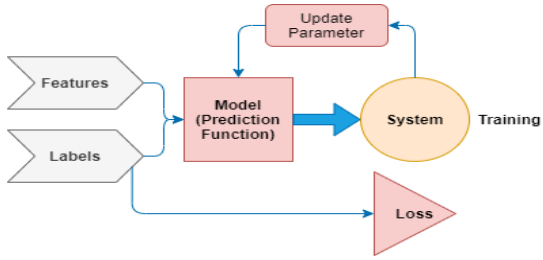

Fig. 1. The current procedure of machine learning for calculating loss function.

This paper deals with the design of the proposed novel and secure blockchain ML-enabled architecture for medical industries to manage distributed health transmissions and ledger management with optimization. The proposed collaborative architecture provides health-related day-to-day ledger transaction management and optimization along with the information provenance, traceability, and assurance for performing different consensus operations. It also creates trust between the participating stakeholders (different hospitals) and enables events of execution while data is generated from patients' end, collecting each record, storing, analyzing, and interpreting the electronic services through the e-Healthcare distributed applications. The private serverless network is designed to protect the privacy of all transactions made by e-Healthcare applications and store individual records in the distributed immutable nodes of data in encrypted storage.

The major contributions of this paper are as follows:

- This paper describes the detailed design of the current process of e-Healthcare related medical transactions classification, scheduling, analysis, organization, management, optimization, and preservation with service delivery protocol-related problems and challenges as well as privacy and protection issues.
- We designed and implemented the proposed architecture to examine and analyze preserved day-to-day patients' medical transactions with the rate of data optimization and predict futuristic logs. The proposed collaborative architecture is efficient and effective when it comes to diagnosis, treatment criteria, data management, and optimization because it uses ML-enabled stochastic gradient descent (SGD).
- It shows how to build a new and secure e-Healthcare application and management ledger with blockchain smart contracts and a secure serverless permissioned private network for the medical industry. Finally, the blockchain smart contracts (chaincodes) are designed, implemented, and deployed to automate day-to-day dynamic medical applicational data serverless transmission, preservation, update ledger, and exchange of analyzed futuristic logs (optimization details) among the participating stakeholders in the private network.

The remainder of this paper is structured as follows. In Section 2, we evaluate and analyze several related kinds of literature on blockchain, smart contracts, Hyperledger, distributed network protocols, and ML-enabled electronic healthcare ledger loss prediction and optimization for the medical industry. The blockchain ML-based SGD-enabled secure distributed serverless e-Medical applicational information transaction, management, and optimization architecture is proposed in Section 3. In Section 4, the simulations are performed using a benchmark dataset and demonstrate a few open research issues with futuristic assumptions. Finally, we conclude this research paper in Section 5.

Table 1. Blockchain machine learning-enabled e-Healthcare related literature

Research methods	Research description	Issues/Challenges/Limitations	Similarity/Weakness
Hyperledger Fabric-machine learning (N-gram)-enabled drug-related information management and recommendation system for medical industries [19]	The authors of this paper proposed two different modules for secure medicine-related data management and provided a recommendation platform for consumers. The Hyperledger fabric is used to deploy a modular architecture for secure data transmission and preservation in the protected private network, whereas the machine learning-enabled N-gram LightGBM model is designed to provide efficient drug-related information to the participating stakeholders.	-A private permissioned network is designed -Predefined consensus policies of the Hyperledger fabric are used -Recommendation systems suggest only top-rated or highly utilized medicines	-Blockchain Hyperledger fabric -N-gram LightGBM model -REST API
The role of distributed e-Healthcare applications for secure health ledgers and maintaining the privacy of medical records using blockchain Hyperledger technology [21]	This paper indicated the privacy and security issues in the client-server and concerns about e-Healthcare data management, records, and preservation. This paper also highlighted a few potential challenges (such as regulatory compliance, etc.), and demonstrated the impact of distributed ledgers in the medical environment.	-Digital signature-based asymmetric cryptography -Proof of work, proof-of-stake, and delegated proof-of-stake are used -Predefined consensus policies are utilized	-Blockchain consortium network -Ethereum -Public channel for electronic medical ledger transaction
Blockchain-enabled e-Healthcare protected records preserved in secure distributed storage using KNN training protocols [20]	Jabarulla and Lee [20] proposed a secure technique of KNN for a privacy preservation solution. The KNN training over IoT data employs blockchain distributed ledger technology with a partially homomorphic cryptosystem in order to protect participating stakeholders.	-Secure biasing operations -A secure comparison protocol is derived -Secure polynomial operation is applied before data preservation	-Rigorous analysis -Homomorphic cryptosystem -Encrypted data sharing via blockchain -Blockchain node scalability evaluation
Fitness health-related data management and optimization using the Internet of Things (IoT) enabled blockchain distributed platform [22]	Frikha et al. [18] proposed a process of capturing medical data, examining, preserving, analyzing, presenting, managing, and storing it through fitness intelligent devices, which were deployed in connection with the proposed IoT.	-Scope of data and privacy-related challenges -Patient-centric application -For design consensus protocols, the Raspberry Pi 3 is used.	-Blockchain Ethereum -Public permissionless network -Secure channel for transactions is deployed
Blockchain public permissionless network is designed for secure authentication between participating stakeholders of the e-Healthcare ledger environment [22]	The authors of this paper proposed a secure blockchain-based distributed architecture tailored specifically to cater to the needs of electronic healthcare applications.	-Platform interoperability issues -Computationally expensive -Pure decentralized in nature blockchain	-Reliable cryptography with blockchain -Public network -Predefine consensus protocol -Hash-encryption SHA-256
Blockchain-enabled digital healthcare preserve system for fourth industry healthcare revolution applications [23]	Tanwar et al. [21] proposed an access control policy algorithm to enhance medical data accessibility between stakeholders. Further, assisting in the experimentation of distributed environments to create the Hyperledger fabric-enabled e-Healthcare records sharing system, which is deployed by the use of smart contracts.	-Cross-chaining limitations -Round trip time evaluation. -Streamline data formulation.	-Hyperledger Fabric -Private channel -Proof-of-authentication -Proof-of-work -Distributed ledger preservation

2. Related Work

The e-Healthcare-enabled applicational records are employed by the medical industry using a server-based centralized infrastructure, in which different hospitals retain primary knowledge of patients' clinical details [19, 20]. The patients' clinical or health records received from different sources who get treatment from distinct consultants for different diseases are scattered or redundant in the different central servers (active or passive). To address the clinical records filtration, organization, management, and optimization-related challenges, various client-server-enabled centralized e-Healthcare applications of the distinct organization are proposed. However, in this scenario, security and protection are the main areas of concern in the central-server and cloud-enabled environment. Recently, several client-servers-enabled server-based e-Healthcare researchers presented solutions that address the security and privacy concerns. A few experts came up with different ideas, like storing clinical data in the cloud and recording encryption (hash-based) details in a group network.

In this context, we examine and analyze several E-Healthcare systems' data management procedures, evaluate loss functions while optimizing records and management, and tackle secure transmission protocols using blockchain ML models and related literature [20–23] (as shown in Table 1), which are discussed as follows.

3. Blockchain and Machine Learning-Enabled Proposed Architecture for Medical Industry

Fig. 2 presents the proposed e-Healthcare simple architecture for medical industries, which provides minimal functionality to program events of health-related node transactions. This architecture is designed according to the blockchain permissioned network due to the benefits it has over the public infrastructure. The proposed blockchain-enabled e-Healthcare architecture consists of stakeholders, including end-users (patients), authorized members by the patient, consultant, emergency staff, hospital, health authority, and blockchain engineer. These stakeholders' assets (read-only and write) request for medical services, medical test data, and other health-related transactions, for example, adding new records, updating records, and medical queries in the immutable storage. This designed platform involves different hospitals throughout the region and stakeholders connected to the single secure, permissioned private network. As illustrated in Fig. 2, the health authorities and other medical industries are participating in this ledger to facilitate quick access to and analysis of the futuristic assumptions. In each health-related transaction, there are two different portions highlighted: one is read-only and the other acts as a full node control (administrative environment). The proposed blockchain distributed architecture was designed, implemented, and deployed, and it supports four different types of transactions (as mentioned in contracts 1 and 2), such as AddMedicalLedger(), UpdateMedicalLedger(), SecureTransaction(), and NodeConPreservation().

To perform e-Healthcare transactions, the permission/approval of the blockchain engineer is required, as shown in Fig. 2 and Contract 1. Before every transaction in this ledger, stakeholders get authentication from the blockchain engineer, and then they send the new node transactions to the blockchain network. After the transaction execution, the blockchain engineer generates the node for the transaction and broadcasts it to other participating stakeholders (hospitals/medical industries).

The blockchain consensus protocols are used to add new node transactions to the immutable ledger and to update it. For this purpose, we tuned practical byzantine fault tolerance (PBFT) in accordance with the e-Healthcare selection of protocol over the most commonly used proof-of-encrypted transaction because patients get less delay and faster response with reduced throughput. This procedure supports secure communication transmission and ledger maintenance. These day-to-day e-Healthcare transactions are stored in the protected ledger, which is immutable in nature and is used for the analysis of futuristic predictions related to big medical data management and optimization. For this reason, we used ML-based SGD to optimize the big data of the individual patient to release day-to-day storage before preserving it in the immutable system. InterPlanetary File Storage (IPFS) is used as a digital data storage infrastructure that provides a distributed storage environment (active/passive). However, to access this storage, we

separate communication channels into off-chain and on-chain. As shown in Fig. 2, an off-chain communication channel is an outer channel to access the blockchain encrypted environment, while an on-chain is the inner one.

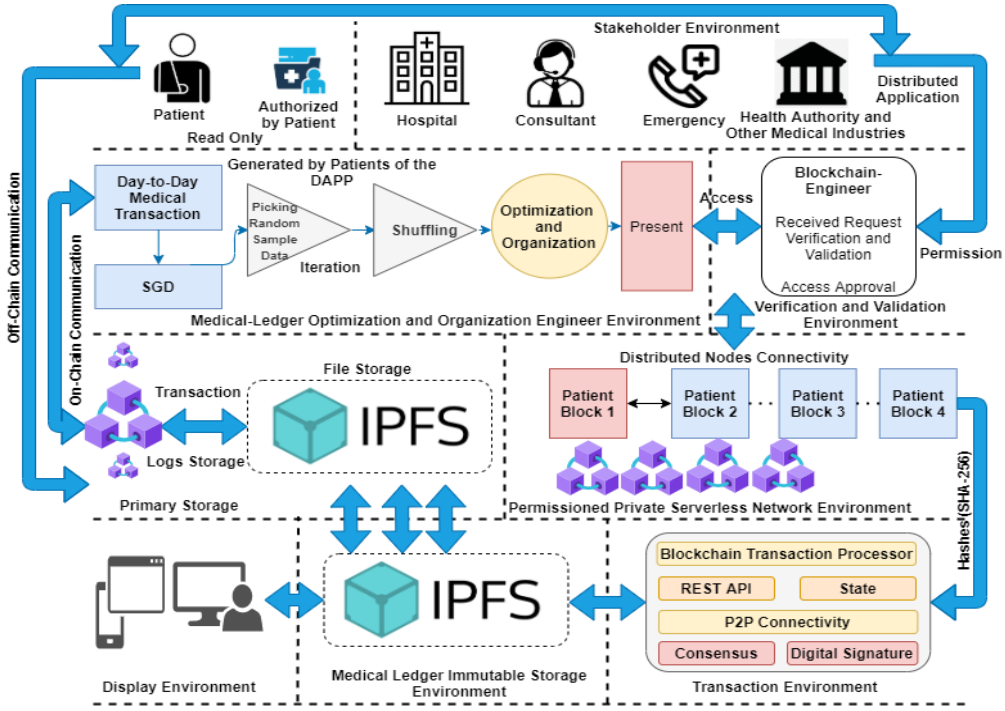

Fig. 2. The novel and secure proposed architecture for e-Healthcare applications.

3.1 Notation and Problem Formulation

SGD is one of the most powerful optimization techniques in ML. Despite this, a gradient descent (ML technique) is performed as another type of optimization and data management purpose, which acts as a slop of a function. This optimization measures the degree of patient health-related service change (in day-to-day transactions) of a variable in response to the changes of another variable (previously preserved). This provides a convex function whose output is the partial derivative of a set of the range of parameters in accordance with the inputs. The evaluation matrix demonstrates that the greater the gradient, the steeper the slope. The procedure starts when gradient descent runs iteratively to execute the finding values towards the optimal values of the parameters. Similarly, for minimal criteria, the optimal solution method finds the minimum possible values of the given loss function.

A system that is linked with a random probability is formulated and is known as stochastic. In the huge amount of medical data generated through distributed e-Healthcare applications on day-to-day transactions, a few samples are selected randomly instead of a whole data set for each iteration, optimizing the data in a better manner for the organization, as shown in Fig. 3.

In SGD, we find the gradient of the loss function of an individual patient's services at every loop instead of the sum of the gradient loss functions of all the patient's utilized services. After that, only one sample from the preserved patient records is chosen at random for every iteration. For the path selection for reaching the minima, the algorithm chooses randomly, which is usually noisier than the simple gradient descent. The selection of the path does not impact us as long as we reach the minima and within a short interval of time.

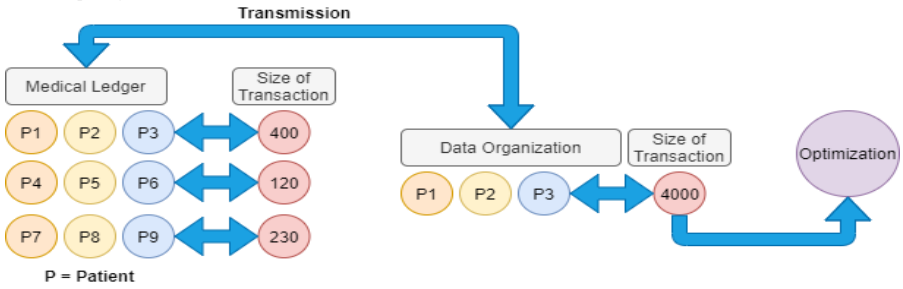

Fig. 3. Preserved medical ledger.

The problem of medical ledger minimization requires an object function design that has the form of a sum mechanism, such as:

$$Q(m) = {}^{1}/_{a} \sum_{j=1}^{a} Q_j\,(a) \tag{1}$$

where m is the parameter that is used to tune $Q(m)$ for estimate minimization, every individual summed function is associated with the *j*-th observation.

The true gradient of $Q(m)$ is approximated by a gradient at an individual point of record (individual patient in each iteration), as the expression is:

$$m = m - \eta \nabla Qj(m) \tag{2}$$

Through the training set, the SGD performed the $m = m - \eta \nabla Qj(m)$ update for every individual (patient) training. There are lots of passes that can be made over the training all the preserved (day-to-day) until the SGD converges.

When the algorithm reaches the point of interval (individual approximately 86%), the data can be shuffled for each iteration to secure duty cycles.

In this process, we used the goldilocks learning rate mechanism so the SGD for the medical ledger could converge more efficiently. In pseudocode, the SGD for medical ledger optimization and organization is presented as follows (Fig. 4).

$for\ loop\ in\ range\ (a)$; which is $0_k = 0_k$ – alpha (z'– z) b_k
$def\ \ Stochastic\ Gradient\ Descent\ (f, theta, alpha, num_{iters})$:
Arguments,
f = optimization function
theta = starting point
num_{iters} = number of iterations in the complete procedure
where, initital_iteration = 0; second_iteration = thetas
for loop in xrange(initial_iteration)
new == f(second); second = second – (alpha * new)

Fig. 4. Pseudo-representation of the SGD mathematics.

The code of SGD makes use of vectorization libraries except to compute individual records (in a single iteration) separately. As a result, we get smoother convergence. This convergence of SGD has been analyzed using convex minimization with an approximation of stochastic where the learning rate is equal to η.

After this procedure, we compute 560 iterations, which is the total number of iterations; the average of the individual is equal to 1.6. And so, the rate of ledger optimization is equal to 86.9%, which is more efficient and better than the other state-of-the-art methods.

3.2 Smart Contracts for E-Healthcare Applicational Transactions and Distributed Node Connectivity

For secure medical transactions and preservation, we designed and created a blockchain smart contract to enable a real-time distributed health system that monitors, manages, and optimizes medical ledgers. The AddMedicalLedger() is designed, created, deployed, and initiated by the blockchain engineer and participating stakeholders, as shown in Fig. 5. The function of this contract is to authorize new devices before verification and validation of individual requests are received by the blockchain engineer. After validation, the patient is allowed to utilize medical services such as consultant guidance, medical alerts, etc. The contract adds a new node in the ledger after checking the node's existence. The alert of an added node is sent to every participant who acts as interconnected and needs to know the details of transactions (UpdateMedicalLedger()), such as patient-doctor, consular-patient, etc. The blockchain-engineer is the only response that handles all the transactions that occur in the e-Healthcare distributed environment and manages preservation, along with security and privacy, using a cryptographic hash-encryption mechanism. This contract also records additional details of the new node addition and transactions, such as device ID registration (dIDReg()), stakeholder registration (stkReg()), list of services (listSer()), delivery of services (deliverySer()), preserve logs (preLogs()), ledger management (ledgerMang()), ledger optimization (ledgerOpt()), store details of ledger optimization with loss (storeDLOL()), blockchain timestamp [execution], and other related activities.

Whereas, as shown in Fig. 5, the SecureTransaction() contract is designed, created, deployed, and initiated between the blockchain engineer and stakeholders for managing secure events of node transactions in the distributed permissioned network environment. Day-to-day medical transactions are preserved after the examination and analysis of privacy and protection in the distributed ledger environment. NodeConPreservation() was written to automate overall node preservation in immutable storage. The blockchain engineer is responsible for handling all the node connectivity and secure preservation solutions. This contract also records additional information related to the medical ledger, such as node size (nodeSize()), batch number (batchNumber()), new transaction (newTrans()), previous transaction (preTrans()), hash encryption (hashEncryption()), blockchain timestamp [execution], and other related activities performed, as shown in Fig. 5.

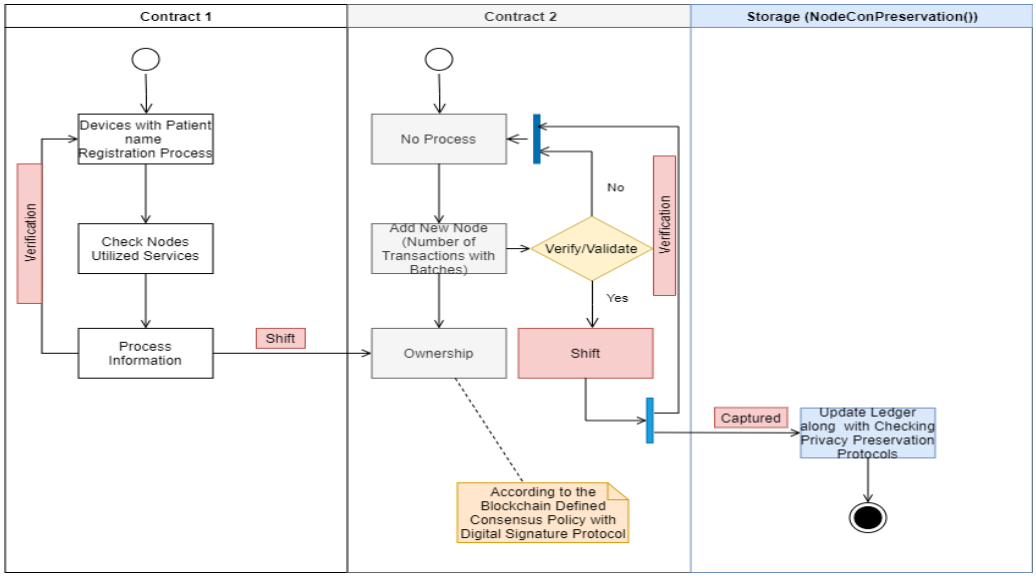

Fig. 5. Smart contracts implementation.

4. Simulations, Results, and Discussion

In this context, we present an extensive simulation and analysis of the proposed blockchain-enabled medical ledger optimization-related results and secure preservation solution in a distributed serverless network environment. It has been presented that there is a correlation between the day-to-day medical services-related transaction and optimization matrices, as shown in Fig. 6. The loss between the collaborative solution for medical industries is represented through the different parameters, such as a collection of preserved data (primary stored), medical service transmission between stakeholders, required transmission power, modulation level, delay, throughput, jitter, duty cycle, and rate of medical ledger optimization (using SGD) and preservation in the serverless private network, as shown in Fig. 6.

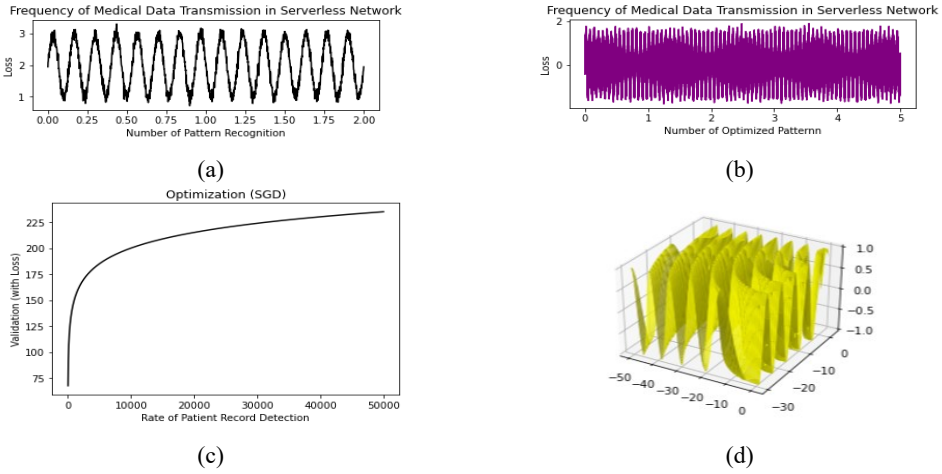

Fig. 6. Frequency measurement medical data transmission in serverless network environment. (a) shows the relationship between the similar patient ledger pattern detection and recognition with loss/cost rate. (b) Evaluate the number of optimized patterns. (c) Number of individuals' ledger optimization. (d) 3D representation of medical ledger optimization using SGD.

It is analyzed that the E-Healthcare application performed efficiently and effectively in terms of modulation and other parameters described in this proposed medical ledger. In this scenario, the two-way (binary) technique is utilized to calculate the transmission fluctuation. Further, we investigate the relationship between the energy bit and bit rate error (per noise ratio); while transmitting the data from source to destination, as depicted in Fig. 7.

However, we also examined the close coordination between the baseline e-Healthcare applications and the proposed distributed e-Healthcare applications. The tuned parameters comparison with 0.087 (non-blockchain-based solution) and 0.061 (blockchain-enabled solution), is far better than the previous centralized server-based systems. After all these procedures, an individual patient's health-related records are examined before being stored in the immutable storage in the serverless environment, where the frequency of medical data transmission (generation to delivery) is measured by the number of patterns recognized (similar features, diagnostics, etc.), and the loss/cost ratio between the time frame of analysis. This distributed medical ledger also provides the ratio of optimized patterns with an accuracy rate of 93.1%, as shown in Fig. 6.

It is observed that the value of state-generated error (loss) increases the number of roll-offs while reducing the energy dissipation. For this purpose, we deal with the transmission power and the power of amplification, the range of transceivers-based tuning strategy is utilized accordingly in this serverless environment for maintaining the medical ledger of medical industries.

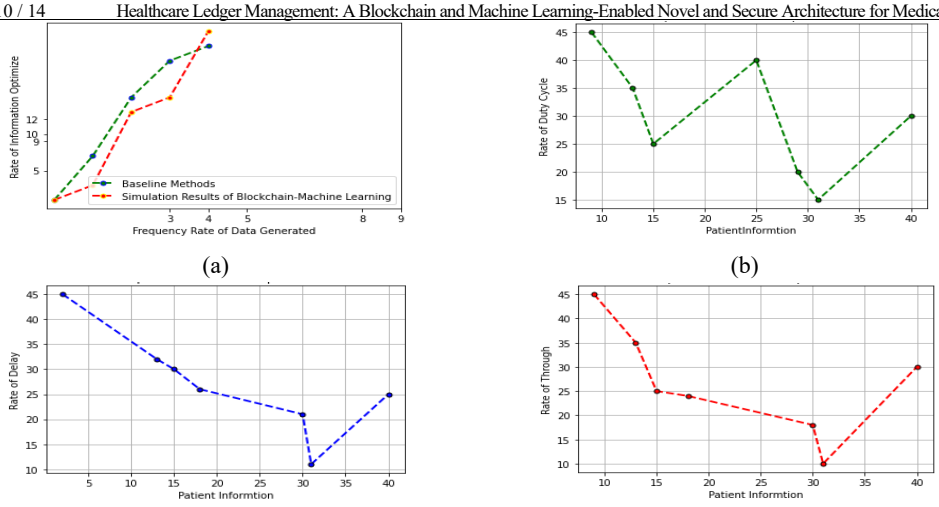

Fig. 7. The relationship between frequency of medical ledger transmission and optimization. (a) shows the frequency rate of data generation and the rate of information organization. (b) shows the relationship between the patient's information and the rate of duty cycle. (c) shows the rate of delay. (d) shows the throughput rate.

Because of the implications in a distributed environment, all details of connected patients and their used services, as well as the events of node transactions, are exchanged over the private network. It is very crucial in the process of extraction, identification, detection, and recognition of all the similar features of patient information for optimization that are traveling over the serverless channel (either off-chain or on-chain). Hence, we calculate the transmission power level with the coordination of linear distance and power drain, respectively.

After all this, we highlight the advantages and benefits of the proposed blockchain ML-enabled distributed application. Include robust security and privacy with efficient data transmission in the permissioned private network. It provides individual medical ledger integrity, confidentiality, transparency, and provenance, and maintains each transaction secure with the use of SHA-256 as shown in Fig. 2, with the reduce loss = 0.7, learning-rate = goldilocks, ledger optimization = 0.23, transmission power = -18 dBm, jitter = 32 ms, delay = 90 ms, throughput = 170 bytes, duty-cycle and delivery = 0.10 (10%), and dynamic serverless response calculation, as shown in Fig. 7.

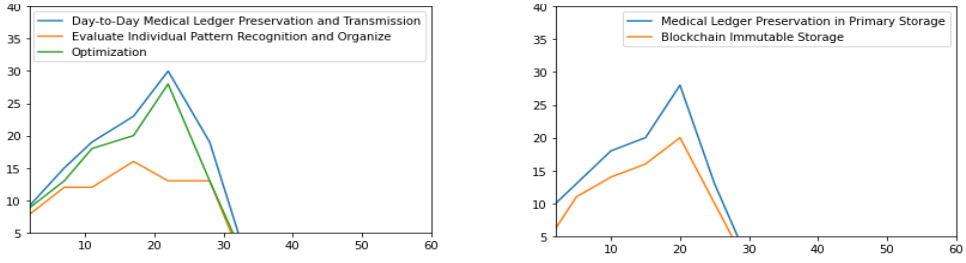

Fig. 8. (a, b) Comparison chart of the proposed e-Healthcare application evaluation matrices.

Fig. 8 presents the comparison chart of the proposed e-Healthcare application. Fig. 8(a) shows the number of transmissions and generated records preserved in the primary storage and the evaluated individual patient's ledger patterns recognition and organization. Fig. 8(b) shows the relationship between medical-ledger preservation in primary storage and blockchain immutable storage. Through the

management of large, processed data, including the patients' requesting services and utilization, medical reports, and complete ecosystems to augment the human-based processes and privacy hazards. Therefore, to overcome such issues, several e-Healthcare solutions are intended. One of the solutions is secure multimedia processing and information management using ML, IoT blockchain, and distributed storage. The collaborative studies came into existence to improve the healthcare system's performance by reducing the cost of medical services in an efficient and effective manner. By implementing this distributed system, it delivers several benefits and associations, but even so, patients are afraid to use the application because of its compromise by different intruders in the public network. To enhance more privacy and protection with system's information optimization in the distributed ledger environment, we compare our proposed architectural solution with other state-of-the-art methods [24-28], as shown in Table 2.

Table 2. Comparison with other state-of-the-art methods, architectures, and models

Research formulation	Research explanation with features	Matrix of the state-of-the-art methods/architectures/models	Evaluation matrix of our proposed distributed serverless architecture
A consortium framework proposed for multimedia-related data scheduling and processing using IoT-Blockchain technology [24–28]	This paper highlighted a few main features that consume less computational cost with limited resources and increase the rate of accuracy in terms of blockchain security. The main features of this paper are: -IoT-enabled resource allocation and utilization -Blockchain public network -Pre-defined hash encryption -Multimedia-based data processing limitation	The evaluation criteria of the paper are discussed as follows: -Blockchain: Permissionless -Network: Public network -Consensus: Pre-define with PoW and PoE -Encryption: Hash-encryption -Node size: Default Batch: Not applicable -Optimization technique: Not applicable -Accuracy: 86% success rate	We proposed a blockchain and machine learning-enabled serverless medical data processing, optimizing, organizing, and preserving distributed ledger solution for medical industries to handle day-to-day huge amounts of health information. The research parameters are mentioned as follows: -Blockchain: Permissioned structure -Network: Private network -Consensus: PBFT with PoET -Encryption: Hash (SHA-256) -Node size: 4 MB fixed size -Batch: Single batch -Optimization technique: SGD -Accuracy: 93.7% (optimize average individual 23%)

5. Conclusion

This paper discusses the privacy and security-related challenges and limitations running on the traditional e-Healthcare applications along with the medical-ledger organization, management, and optimization limitations. For this purpose, in this paper, we proposed a blockchain ML-enabled collaborative architecture for medical industries to handle medical e-Service transmissions and ledger management. The collaborative approach brings ledger optimization, secure management, protection, integrity, forge-resistance, and control access to the health-related chain of information preservation using blockchain SGD. It also facilitates patients of e-Healthcare distributed applications to request, access, and allow authenticated stakeholders to record their electronic medical sensitive transactions through the e-Healthcare distributed application on the distributed ledger. The blockchain private permissioned platform is designed, implemented, and deployed as it provides a modular infrastructure,

which also distinguishes the distributed core system (read/write) and read-only transactions from the applicational environment. For this reason, we designed and created digital (smart) contracts to enable the rules of e-Healthcare governance bodies and accomplish the blockchain consensus based on the predefined policies of PBFT. However, the core systems are evaluated in real-time for fault tolerance and manage the PoET engine to simulate trust events of medical transaction execution for attaining the chain-of-services. The simulation results of the proposed architecture show robustness in terms of efficient performance, including predictive loss = 7%, learning rate = goldilocks (0.5), ledger optimization = 23%, transmission power = -18 dBm, jitter = 32 ms, delay = 90 ms, throughput = 170 bytes, duty-cycle and delivery = 10%, and dynamic serverless responses.

Author's Contributions

Conceptualization, AAK, AAL, MS. Investigation and methodology, AAK, OC, MS, WA, HH, ZAH. Writing of the original draft, AAK. Writing of the review and editing, AAK, AAL, MS. Software, AAK, OC, MS, WA, HH, ZAH. Formal analysis, AAK, OC, MS, WA, HH, ZAH.

Funding

This work was supported by National Natural Science Foundation of China (Grant No. 62250410365) and Taif University Researchers Supporting (Project No. TURSP-2020/107), Taif University, Taif, Saudi Arabia.

Competing Interests

The authors declare that they have no competing interests.

References

[1] Y. Li, B. Shan, B. Li, X. Liu, and Y. Pu, "Literature review on the applications of machine learning and blockchain technology in smart healthcare industry: a bibliometric analysis," *Journal of Healthcare Engineering*, vol. 2021, article no. 9739219, 2021. https://doi.org/10.1155/2021/9739219

[2] T. R. Gadekallu, M. K. Manoj, N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 30-33, 2021.

[3] T. R. Gadekallu, Q. V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W. J. Hwang, "Blockchain for edge of things: applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964-988, 2021.

[4] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242-3254, 2021.

[5] Z. A. Shaikh, A. A. Khan, L. Baitenova, G. Zambinova, N. Yegina, N. Ivolgina, A. A. Laghari, and S. E. Barykin, "Blockchain Hyperledger with non-linear machine learning: a novel and secure educational accreditation registration and distributed ledger preservation architecture," *Applied Sciences*, vol. 12, no. 5, article no. 2534, 2022. https://doi.org/10.3390/app12052534

[6] A. A. Khan, A. A. Shaikh, O. Cheikhrouhou, A. A. Laghari, M. Rashid, M. Shafiq, and H. Hamam, "IMG-forensics: multimedia-enabled information hiding investigation using convolutional neural network," *IET Image Processing*, vol. 16, no. 11, pp. 2854-2862, 2022.

[7] A. Fusco, G. Dicuonzo, V. Dell'Atti, and M. Tatullo, "Blockchain in healthcare: Insights on COVID-19," *International Journal of Environmental Research and Public Health*, vol. 17, no. 19, article no. 7167, 2020. https://doi.org/10.3390/ijerph17197167

[8] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 94, article no. 101863, 2020. https://doi.org/10.1016/j.cose.2020.101863

[9] A. A. Khan, Z. A. Shaikh, L. Belinskaja, L. Baitenova, Y. Vlasova, Z. Gerzelieva, A. A. Laghari, A. A. Abro, and S. Barykin, "A Blockchain and metaheuristic-enabled distributed architecture for smart agricultural analysis and ledger preservation solution: a collaborative approach," *Applied Sciences*, vol. 12, no. 3, article no. 1487, 2022. https://doi.org/10.3390/app12031487

[10] B. Mallikarjuna, G. Shrivastava, and M. Sharma, "Blockchain technology: a DNN token-based approach in healthcare and COVID-19 to generate extracted data," *Expert Systems*, vol. 39, no. 3, article no. e12778, 2022. https://doi.org/10.1111/exsy.12778

[11] A. A. Khan, Z. A. Shaikh, A. A. Laghari, S. Bourouis, A. A. Wagan, and G. A. A. A. Ali, "Blockchain-aware distributed dynamic monitoring: a smart contract for fog-based drone management in land surface changes," *Atmosphere*, vol. 12, no. 11, article no. 1525, 2021. https://doi.org/10.3390/atmos12111525

[12] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: a survey," *Sustainable Cities and Society*, vol. 60, article no. 102177, 2020. https://doi.org/10.1016/j.scs.2020.102177

[13] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196-21214, 2020.

[14] A. A. Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational Blockchain: a secure degree attestation and verification traceability architecture for higher education commission," *Applied Sciences*, vol. 11, no. 22, article no. 10917, 2021. https://doi.org/10.3390/app112210917

[15] F. Zerka, V. Urovi, A. Vaidyanathan, S. Barakat, R. T. Leijenaar, S. Walsh, et al., "Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM)," *IEEE Access*, vol. 8, pp. 183939-183951, 2020.

[16] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: a secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, article no. 108500, 2021. https://doi.org/10.1016/j.comnet.2021.108500

[17] S. Jain, A. Anand, A. Gupta, K. Awasthi, S. Gujrati, and J. Channegowda, "Blockchain and machine learning in health care and management," in *Proceedings of 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, Bengaluru, India, 2020, pp. 1-5.

[18] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and fitness data management using the IoT-based blockchain platform," *Journal of Healthcare Engineering*, vol. 2021, article no. 9978863, 2021. https://doi.org/10.1155/2021/9978863

[19] K. Abbas, M. Afaq, T. Ahmed Khan, and W. C. Song, "A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry," *Electronics*, vol. 9, no. 5, article no. 852, 2020. https://doi.org/10.3390/electronics9050852

[20] M. Y. Jabarulla and H. N. Lee, "A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: opportunities and applications," *Healthcare*, vol. 9, no. 8, article no. 1019, 2021. https://doi.org/10.3390/healthcare9081019

[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, article no. 102407, 2020. https://doi.org/10.1016/j.jisa.2019.102407

[22] M. T. Quasim, F. Algarni, A. A. E. Radwan, and G. M. M. Alshmrani, "A blockchain based secured healthcare framework," in *Proceedings of 2020 International Conference on Computational Performance Evaluation (ComPE)*, Shillong, India, 2020, pp. 386-391.

[23] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey," *IEEE Access*, vol. 9, pp. 95730-95753, 2021.

[24] 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*, vol. 79, 9711-9733, 2020.

[25] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications*, vol. 57, article no. 102686, 2021. https://doi.org/10.1016/j.jisa.2020.102686

[26] S. K. Singh, A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "DeepBlockScheme: a deep learning-based blockchain driven scheme for secure smart city," *Human-centric Computing and Information Sciences*, vol. 11, article no. 12, 2021. https://doi.org/10.22967/HCIS.2021.11.012

[27] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90075-90083, 2021.

[28] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park, "Deep learning enabled secure IoT handover authentication for blockchain networks," *Human-centric Computing and Information Sciences*, vol. 11, article no. 21, 2021. https://doi.org/10.22967/HCIS.2021.11.021