Alexandria Engineering Journal (2022) xxx, xxx–xxx

HOSTED BY

ELSEVIER

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare

Ahmed I. Taloba [a,*], Ahmed Elhadad [a,f], Alanazi Rayan [a], Rasha M. Abd El-Aziz [a,b], Mostafa Salem [b], Ahmad A. Alzahrani [c], Fahd S. Alharithi [d], Choonkil Park [e,*]

[a] *Department of Computer Science, College of Science and Arts in Qurayyat, Jouf University, Saudi Arabia*
[b] *Department of Computer Science, Faculty of Computers and Information, Assiut University, Assiut, Egypt*
[c] *Department of Information Systems, College of Computers and Information Systems, Umm-AlQura University, P.O. Box 8XH2+XVP, Mecca 24382, MK, Saudi Arabia*
[d] *Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[e] *Research Institute for Natural Sciences, Hanyang University, Seoul 04763, Republic of Korea*
[f] *Department of Computer Science, Faculty of Computers and Information, South Valley University, Egypt*

Received 13 August 2022; revised 8 September 2022; accepted 15 September 2022

KEYWORDS

Blockchain;
Multimedia;
Data processing;
Internet of Things (IoT);
Healthcare system;
Data security

Abstract Blockchain technology must have sparked widespread interest, applications associated with data monitoring, banking sectors, computer security, the Internet of Things, and food chemistry to the healthcare sector and cognitive science. The use of multimedia in the healthcare architecture also allows for the storage, processing and transmission of patient information in a wide range of formats such as images, text and audio over the Internet using various smart particles. However, managing large amounts of data, including findings and images of each individual, increases human effort and increases protection risks. In this paper, to address these problems by using IoT in healthcare improves the performance of patient care while lowering costs by efficiently distributing healthcare resources. Nevertheless, various attackers can cause a variety of risks in IoT devices. To avoid these problems, Blockchain technology has been identified as the most effective method for maintaining the secrecy and security of control systems in real-time. This should provide a security architecture for healthcare multimedia content using blockchain technology by producing the hash of every information so that any transition or modification in information, as well as any breaches of medicines, would be evidenced across the whole blockchain platform.

* Corresponding authors at: Department of Computer Science, College of Science and Arts in Qurayyat, Jouf University, Saudi Arabia and Research Institute for Natural Sciences, Hanyang University, Seoul 04763, Republic of Korea.
E-mail addresses: aitaloba@ju.edu.sa (A.I. Taloba), aaelhadad@ju.edu.sa (A. Elhadad), rmalanazi@ju.edu.sa (A. Rayan), rmhassanien@ju.edu.sa (R.M. Abd El-Aziz), mostafasalem@aun.edu.eg (M. Salem), aalzahrani@uqu.edu.sa (A.A. Alzahrani), f.alshalawi@tu.edu.sa (F.S. Alharithi), baak@hanyang.ac.kr (C. Park).

Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2022.09.031
1110-0168 © 2022 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Engineering, Alexandria University.

1. Introduction

Smart healthcare and biomedicine development always seems to be significant concerns that should be discussed in any possible manner also with technological advancements that are enveloping the world [1]. The only thing that matters is improving the framework, confidence, process, and effectiveness of health services, as well as providing qualified nutrition and care to patients. In today's world, people are becoming increasingly hesitant to seek individual health services until a major crisis occurs. This is commonly considered a section of over-engagement with the traditional busy living and lifestyle framework [2]. Accordingly, if a framework is established that initiatives or identifies typical problems in a human's care package and can inform a person's assigned personalized care manager, the entire scenario will be even more useful, and an easy discussion on the patient could be accomplished at the right time and within a safe timeframe.

The extent of communication between remote equipment connected to the Internet to transmit information and access has improved greatly thanks to the continuous developments in the Internet of Things (IoT) sector. As a result, IoT has innovated and interrupted nearly every sector on that planet, from learning to the supply chain [3]. IoT also has performed admirably in the healthcare sector, facilitating diagnostic tests and effectively monitoring patient operations. Furthermore, one of the main benefits of IoT is that it allows for healthcare management during the person's non-active minutes, which can be challenging to attain in a traditional system. Advanced access to the system, as well as constant improvement of it, reveals a wealth of possibilities for faster diagnostic tests and therapy [4].

People interact in a variety of ways such as through multimedia thanks to the spread of technological advances in the latest decades. Due to a pairing of various formats, resolutions, information sources, and media, multimedia interaction is classified as very complex nature [5]. The medical domain is now regarded as the most complicated, important, and fast-expanding component of multimedia applications, providing a method to increase the performance of interplay among the patient and a doctor while also advancing their participation in the healing procedure [6]. The utilization of multimedia in healthcare schemes also allows for the storage, processing, and transmission of patient information in a range of formats, including images, text, and audio, via internet services utilizing different smart artifacts. Healthcare organizations all over the world have been converting themself into more effective, synchronized, and user-centered processes in today's world. Nevertheless, as the world's population grows, provider power is reduced, resulting in lower service quality [7]. Traditionally, researchers and scientists have proposed a significant change to the current healthcare approach to solving such circumstances; however, today's healthcare has become such a data-intensive area in which large amounts of data have been generated, distributed, deposited, and obtained daily [8]. As a result, managing large amounts of multimedia content and images of each individual requires more human work and privacy issues.

Furthermore, rapid advances in health care procedure strategies and operations may lead to a variety of communication and storage issues between different vendors, including physicians, health insurance agents, pharmacists, and patients [9]. As a result, security must be at the forefront of future IoT discussions, with transparency playing a key role in enhancing the security of patient data. Furthermore, automated recording and transmission of medical records have been regarded as a critical form of healthcare data, with online data storing and exchanging of patient documents putting the patient's privacy and security in danger in terms of reducing medical costs [10]. Multimedia references that decrease manual intervention may encourage numerous security problems, in which vendors cooperate with several types of equipment and modify records and reports in an attempt to benefit from service users [11].

Blockchain technologies have recently captured the focus of business assistants from a wide range of industries, including healthcare, real estate, administration, and financial services [12]. The numerous healthcare applications connected with blockchain technological advancements are shown in Fig. 1. It has been growing at an incredible rate in an attempt to offer users transparency. Furthermore, it is capable of ensuring security services or visibility even when IoT artifacts or equipment are exploited by a large number of intruders. Furthermore, by storing data from a large number of gadgets and enabling the creation of parties even without a governmental fog, blockchain networks can track, arrange, and bear out interactions. Blockchain technology encrypts all transactions and tracks data from IoT nearby objects returns as the shipment moves from one location to some other [13]. When a pharmaceutical corporation manufactures medicinal products, blockchain technology is used to keep track of them as they are shipped to store locations [6]. Moreover, blockchain's use in healthcare will indeed capture advanced operation, health records data and patient records availability information. Furthermore, the occurrence of medicine delivery from IoT objects engaged to elements where its overstock movements from one location to others can be updated regularly both by the transmitter and the recipient.

As a result, the goal of this study is to recognize multimedia data processing in such an IoT healthcare ecosystem which helps secure healthcare management programs by capturing every person's everyday task [14]. Furthermore, the use of Blockchain Technology in healthcare structures benefited society in a range of methods, including maintaining the security and accountability of patient records, as well as allowing patients to choose who has significant exposure to their findings. Furthermore, file availability and shipping procedure between supplier and the customer, allowing customers to track their product's position and transmitting actions. However, the presented framework's exploratory evaluation was based on the criminal activities or communication services carried out by malevolent IoT particles [15]. These have been explored what percentage of diagnosis data security is compromised when IoT devices are hacked. Furthermore, wormhole and falsification threats, as well as probability situations for measuring verification and content drop proportion, have already been tested.

This study would then offer a healthcare security architecture using blockchain technology by creating hashes of each information, with the contribution of the hash being to offer protection chains of data that should be collected in each of the person's network [16]. Any information violations or healthcare breaches could affect the entire blockchain network's users. Enough that no one in the scheme can engage in both illegal activities during the healthcare scheme.

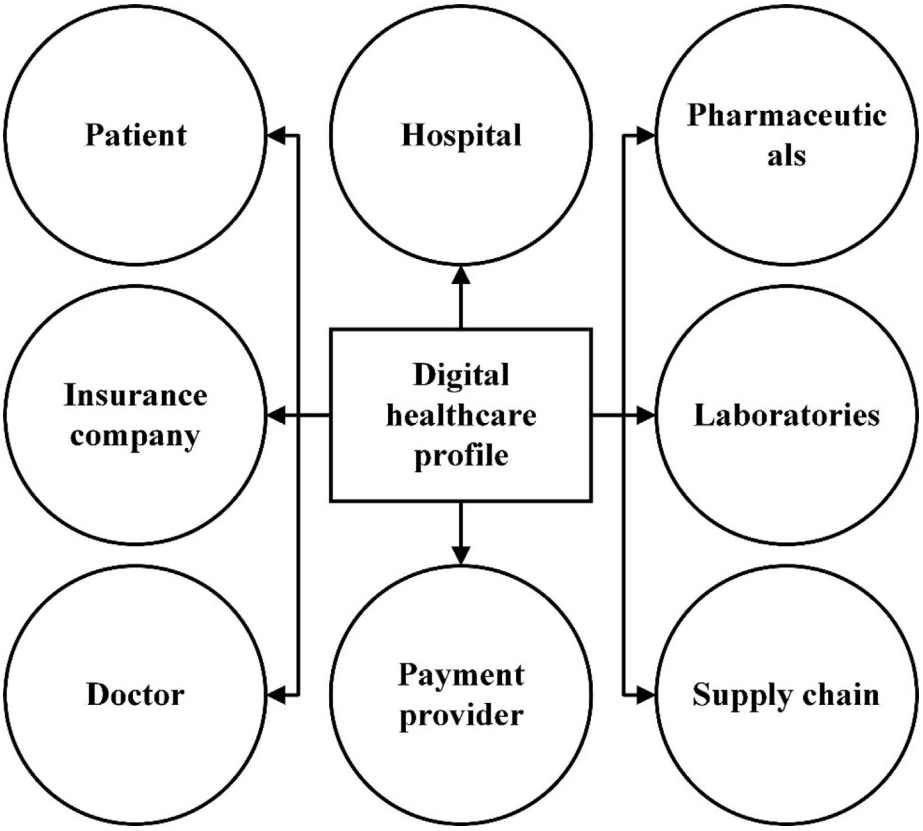

Fig. 1 Healthcare applications based on blockchain technology.

2. Related works

Cyber attackers have always been drawn to the information stored in a cloud server. Healthcare information in a cloud must have recently stimulated their involvement. Threats to health information can have catastrophic implications for healthcare associations. Decentralization of cloud information can help to reduce the impact of threats. Decentralization, facilitated by such a peer-to-peer (P2P) system, allows for the storage and data processing of responsive private healthcare information in the cloud. The blockchain method guarantees integrity and accountability by utilizing the advanced or dispersed property. Various decentralized measures have been developed to regulate the impact of attacks, but these alternatives have so far failed to satisfy the total private data of patient processes. This paper, delivers a patient-centric healthcare information management framework utilizing blockchain-based technology for storage, allowing for greater confidentiality. To encrypt patient information to verify pseudonymity, cryptographic features have been used. This examines the data processing processes as well as the platform's smart contractual agreements' cost efficiency [17].

Every day, large amounts of multimedia information were also created. Multimedia information is traditionally controlled by systems preserved by multimedia service suppliers, that are typically designed with a centralized system. However, a centralized architecture could result in system failure and royalty payments, or other protection disagreements. It's difficult to maintain the integrity of data and path compliance with copyright contract commitments. To address these concerns, introduce a blockchain-based system architectural design for multimedia information administration in this study. For identity verification, use self-sovereign identity and create a multi-level capability-based authentication process. Be using the suggested process to develop a proof-of-concept design and analyze this using a utilization situation. The results demonstrate that the proposed system is appropriate and expandable [18].

The number of wirelessly connected equipment has increased rapidly in recent years, and it is anticipated to achieve billions in coming years. Whereas cloud computing should bring a unique answer to processing this information, security issues cannot be solved solely through these advanced technologies. Blockchain is the technique that undergirds Bitcoin; it uses smart agreements to provide a completely autonomous and ensure security scheme. Multi-layer BC is an effective solution for many IoT issues. This paper explains how Blockchain performs, what IoT difficulties there seem to be, and how they can be addressed with Blockchain. This paper, suggests a multi IoT/blockchain-based structure that is personalized and planned for medical applications. Many groups, which include doctors, healthcare providers, insurance firms, and health centers, communicate with just this data. The greatest goal is to resolve the performance and scalability issues [19].

Smart healthcare also necessitates the facility's ability to diagnose patients who are situated in a remote location. Information security, expenditures, recollection, extensibility, confi-

dence, and accountability among platforms are all major concerns for the smart medical structure. Because the user's integrity has been in discussion due to its open online platform, it's critical to manage information privacy and integrity. Numerous techniques exist to address security problems such as forgery, timescale, rejection of service, and theft smartcard threats, among others. To recognize the consumers associated with issuing, blockchain technology understands the guidelines of complete privacy. The disposal of a centrally controlled third party, range of characteristics, enhanced information sharing, improved security, and lower operating expenses in distributed systems are all reasons for using Blockchain in medical informatics. Healthcare informatics seems to have some unique protection and confidentiality demands, as well as some additional legal demands. Using a probabilistic model, this paper proposes a novel authentication and authorization structure for Blockchain-enabled IoT connections. In the authentication system, the suggested scheme employs random numbers, which are then linked via joint probabilistic reasoning. As a result, it creates a secure correlation between IoT devices for data collection. Extensive simulations with the AVISPA device and the Cooja simulation game are used to verify and analyze the suggested model. In comparison to other frameworks, experimental experiments demonstrated that the suggested model supports robust collaborative validity, improved security systems, and lowers both information exchange and computational operating expenses [20].

Patients' personal information, including their names, addresses, and diseases, is regularly compromised in today's smart urban centers and residences, which is partially attributable to the stability of electronic health records (EHRs). The current state-of-the-art security mechanisms for EHRs have rendered data unreachable to service users. These strategies struggle to strike an effective balance between privacy protection, a need for patient populations, and suppliers to communicate with information daily. Since this shares information in a distributed and operational manner, blockchain technology addresses the aforementioned problems. This can be used in the healthcare industry to keep the balance between EHR privacy and availability. This study, suggests a Blockchain-based structure for storing and maintaining EHRs efficiently. This also allows patients, suppliers, and third parties to have convenient and effective electronic health records while protecting patient privacy. The purpose of this document is to examine how the suggested scheme meets the requirements of patient populations, providers, and third parties while also addressing security and privacy issues in the healthcare 4.0 environment [21].

Advanced healthcare processes rely on a third-party financial intermediary to share medical imaging information electronically, but the present equipment for cross-site transferring information is based on confidence. This looks at the blockchain construct in this paper, which allows parties to reach a consensus without a centralized authority. This creates a platform for cross-domain image information exchange that employs blockchain technology as a decentralized information store to create a balance of radioactivity research with patient-defined privileged availability. The blockchain structure has been demonstrated to remove third-party significant exposure to secured patient information, meet many requirements for an integrated healthcare system, and is easily generalizable to domains other than diagnostic imaging. The framework has some flaws, such as the difficulty of the security and privacy designs and an ambiguous regulatory system. Finally, the large-scale evaluation of such a methodology must be illustrated, which will be dependent on a variety of variables mentioned [22].

3. Methodology

3.1. Blockchain in medical research

In medical studies, a variety of issues such as information privacy, the integrity of information, information sharing, records management, patient enrollment, and so on may emerge. Blockchain, as another internet generation, has the potential to solve these issues [23]. With the assistance of blockchain emerging technologies, healthcare investigators have been working to resolve these problems. Blockchain technologies, combined with artificial intelligence (AI) and machine learning, would then eventually take a healthcare industry that is growing rapidly. Permissioned Cryptocurrency, a blockchain procedure that offers self-executing capabilities, is being used in tandem with hospital-based database management systems in research design.

The main purpose of this study has been to tackle the issue of the diagnosis enrolment problem. The findings of this study revealed that Ethereum enabled faster transactions than bitcoin, leading to the conclusion that Ethereum network agreements could be used to improve the predictability of database management systems in medical studies. The traditional healthcare method of the patient record is represented in Fig. 2. As seen in Fig. 2, many organizations act independently [24]. Even while all departments' operations including doctor diagnostics or prescriptions, laboratory testing, and medicines indicated by doctors are documented or managed distantly, it is vital to track every action of the patient data. As a result, one of the current applications of blockchain technological advances in medical research is patient engagement. Another study was performed, in which a structure was executed to obtain patients' explicit consent for monitoring and storage it in a safe, publicly reliable, and unverifiable manner. The workflow was created using blockchain solutions.

3.2. Blockchains in medical recognition of fraud

The organization of medicinal drug supply chains is one of the most important applications of blockchains in the medical industry. Providing organization is important in all industries, but it is especially important in healthcare due to the increasing difficulty [25]. This is because any disruption in the healthcare supply chain has an impact on a patient's health. As a result of the numerous moving components and people involved, supply chains were also susceptible and contain holes for fraudulent threats.

By having to introduce increased data accessibility and enhanced product reliability, blockchains include a secure and safe framework to overcome such issues and, in certain instances, protect fraud from occurring. Manipulation of the blockchain is difficult because a record could only be confirmed and modified through a blockchain network.

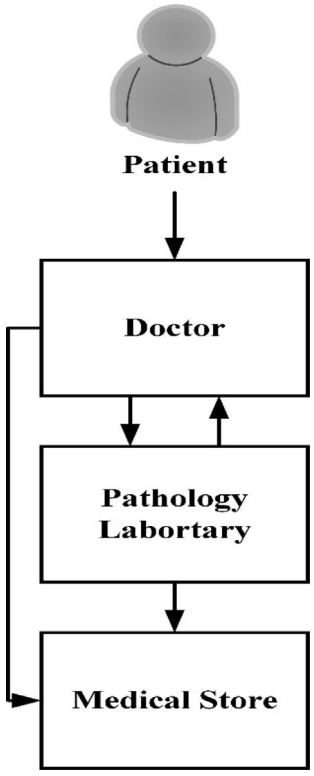

Fig. 2 Managing medical records in a traditional manner.

3.3. Blockchain-based healthcare system framework

The suggested healthcare platform's architecture of the system is depicted in Fig. 3, which involves a web-based application having two sides: a front end that connects among patients and a back end that enables the communication process via blockchain. The specific request serves as a link between these goals [26]. The suggested healthcare system is easy to comprehend because it includes web-based communications between patients and suppliers. There were organizations which are already connected like a network of networks during the operation of a back end in which the blockchain communications process takes place. This utilized two sorts of networks to study the healthcare blockchain procedure: miners or an authentication node and the remaining were executing nodes [27].

The miner's job is to verify if a transaction is right or wrong to duplicate the database information after it is committed or rejected. The role of the execution node, on the other hand, is to check if the transactions accumulated in the miners are genuine or not. If the quantity is correct, the miner's amount will be acquired and executed into the transaction [28]. To imitate a true blockchain process, have provided two virtual machines (VM) systems, as illustrated in Fig. 4. The executing network is hosted on device 1, whereas both miner and execution nodes are executed on device 2.

3.4. Blockchain-based in healthcare: Functional requirements

The invention of blockchain technologies has piqued the interest of many users. Many soon realized that the methodology might be utilized for a variety of purposes, including industry, tax collection, and unitary. This part discussed how blockchain technology might be used in healthcare in terms of report traceability and cost accuracy for diseases [29].

When a patient visits a doctor for therapy, there is a chance that after the diagnosis, the doctor will recommend needless tests or pressure the patient to a customer is buying from certain medical centers. Furthermore, a patient may wish to replace his or her primary doctor and begin therapy with someone else [30]. If a patient switches doctors, all records, laboratory tests, and medicines including proper billing must be kept in the blockchain such that the patient or doctor knows how much money was spent on a method involved. Although all records are kept also on the blockchain, no supplier could modify drugs or expenses bills without such patient's authorization. If a patient has several tests or pills during therapy, the invoice or record of every document should be maintained on the blockchain. So that even if medical shops or laboratory tests generate high expenditures for treatments and afterward update the records during surveillance checks. If every other behavior of the patient is saved within the blockchain, it will be impossible to make any more alterations than once the bill has already been created and placed within the blockchain. The following material discussed two distinct instances.

- Instances 1: Patient reports traceability from the circulating system

Consider a scenario in which a large number of patients are aided in maintaining their records on the blockchain. Reports are automatically recorded during development and stored in the appropriate locations. Every chunk/blockchain contains three parts: hash, data, and the previous chunk's hash. The amount of data stored in a blockchain varies depending on the model of blockchain, such as the health records blockchain, that maintains transaction records as shown in Table 1. The second component, hash, recognizes a block including its data, and it is always distinctive, exactly like a person's [31]. Moreover, the utilization of these advanced technologies aids in the protection of record transactions (distributed ledger databases), attempting to avoid record manipulation by primary individuality or fraudulent participants, creating unchanging (challenging for a personal contributor to harmful interference or customize), and providing protection. Fig. 5 depicts a transactions schematic diagram of blockchain technologies.

The second component, hash, recognizes a block including its data, and it is always distinctive, exactly like a person's fingerprints. When a block is created, its hash is calculated, and changing any data inside this block will change the hash. In other words, when it comes to identifying modifications to blockchains, the hashing of a blockchain system is quite significant [32]. The hash of the previous blocks has been the third aspect within every block. In its structure, blockchain technology is a collection of blocks. Except for the origin transaction, which has no preceding hashing, every block consists of data and also the hash of the preceding block, as seen in Fig. 6. This generates a chain of blocks, and it is thanks to this technique that a blockchain is so safe. Let's look at an example where have a series of three blocks to properly comprehend it in the context of healthcare.

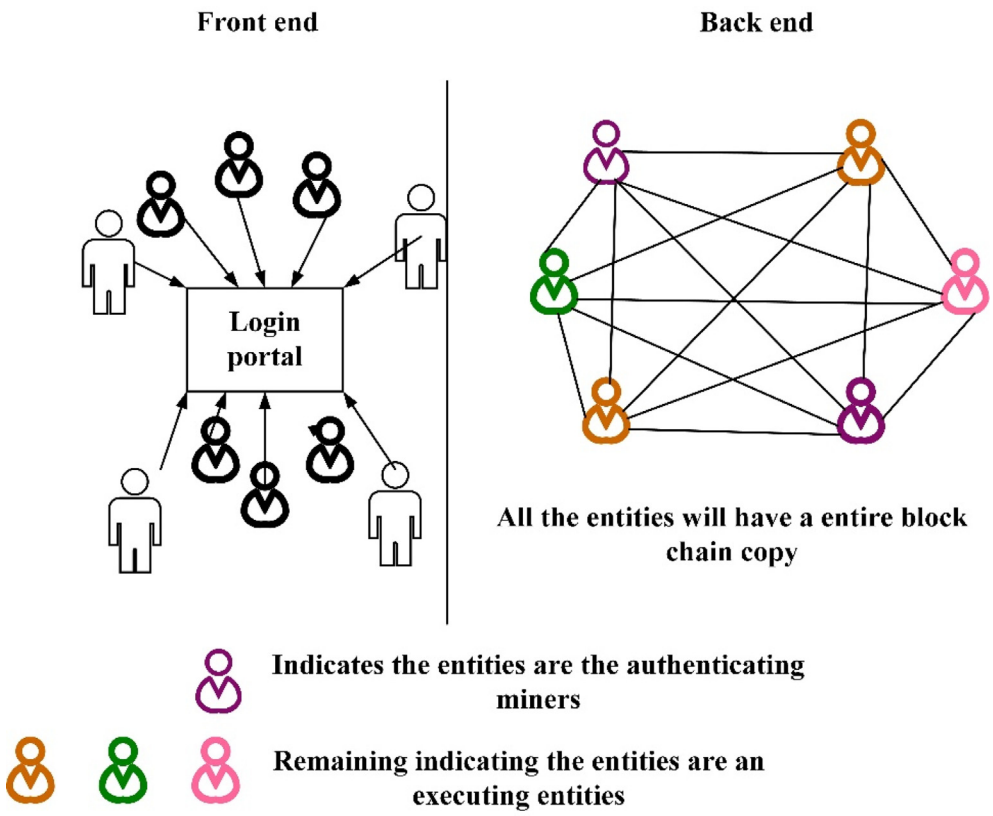

Fig. 3 Proposed framework architecture.

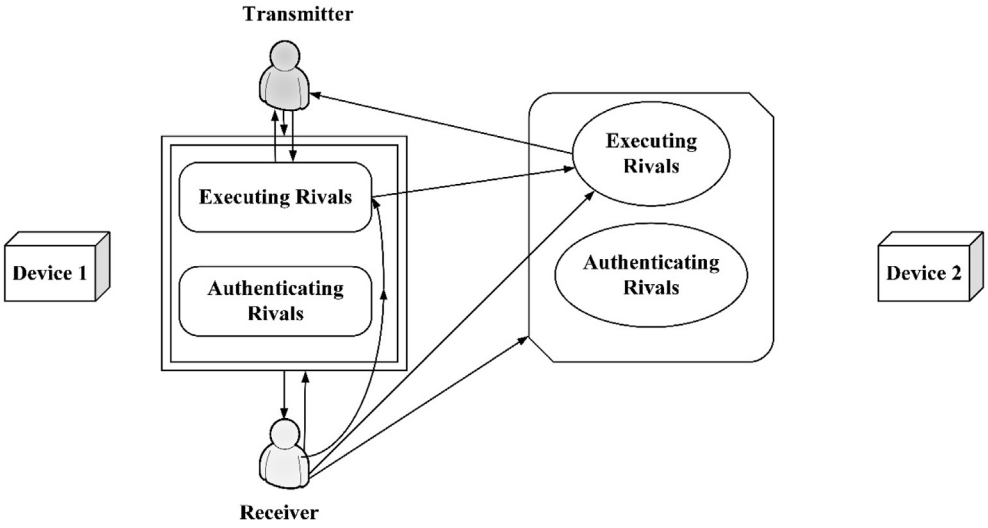

Fig. 4 VM system components.

As seen in Fig. 7, each block represents a distinct seller. Furthermore, each block contains three elements: quality of the products, hash, and the hash for every block. Let's imagine a patient visits a doctor for a specific medical therapy, and all of the events associated with that patient are recorded in the blockchain. Consider that any doctor assisting also with patient laboratory testing could try to tamper also with the second frame, including once the information or testing counts were saved, any alteration in counts may result in a modification in the product's hash. This causes the hash of a transaction to change, rendering block 3 and all following blocks nonsensical since they no more collect a proper hash of the previous block [33]. As a result, changing a single chunk renders all subsequent blocks unusable. To properly manipulate a blockchain, an attacker must manipulate all of the segments on the chain. Only by identifying the above points can the intruder-adjusted blocks be recognized by others, which is extremely difficult.

Table 1 Industrial transaction record block.

Patient Name	Record
Patient	Doctor Recommended Medicines Recommended Tests Insurance abc

- Instances 2:

Another possibility is that even if transmitting prescriptions to medical stores, intermediaries engage in harmful behavior. This indicates so if a corporation delivers 1000 units of drug 'A,' all 1000 units should be transferred to the recipient. Traditionally, if a firm 'A' needs to transport pharmaceuticals to a recipient 'B,' say from INDIA to the United States, this method is carried out through the use of any strong authentication authorities. However, this method incurs higher costs, requires longer time, and compromises the privacy of individual user's 'A' and 'B.' All of these concerns, however, could be easily handled using blockchain approaches. The blockchain assisted in shipping the merchandise without the assistance of a third entity and also more quickly and less expensively [34]. The following describes how blockchain manages product shipment. Assume this have such a connection of three entities that would like to transport the goods from one end to another. 'A' is the transmitter or supplier, 'B' is the dealer who accepts the shipping request and recipient, and 'C' is the eventual recipient who receives the products.

i. Initially, the corporation or sender 'A' who commences the goods shipment procedure will hash a transaction from the first network A → B and disseminate the demand to accessible dealers.
ii. The distributor, 'B,' will then approve the 'A' demand and add a new block to an existing process including its new hash and prior hash.
iii. Furthermore, the trader or deliverer, 'B,' will transmit their item to an individual 'C,' i.e., the recipient, with such a different hash value and prior hash function, and the ultimate blockchain would be marked as completed.

Blockchain is a commercial transactions chain that is transparent and open to everybody, which implies that most blockchain clients have such a complete version of the networks [35]. It gives users transparency by allowing every-one in the network to know where the item is and how long it will require to be distributed.

3.5. *Analysis of performance*

Earlier, the validity of the proposed architecture utilizing blockchain technology was verified utilizing the NS2 simulator before giving the simulation tests. The protection design is run in the NS2 setting mostly on a maximum level of security to aid intermediate visibility of several aspects. As previously stated, the internal workings of the suggested scheme have been examined in this study [36]. Although it is a difficult problem to secure network and security testing at the same time, proposed a respected security architecture that not only maintains a high level of trust between nodes but also provides valid network support to consumers. Three businesses are using an NS2 edition with a set number of customers. Three machine effects on access are functioning in the scenario. As shown in Table 2, a 400 m × 400 m able to fully utilize is formed with small and large network dimensions of 25 and 250 nodes, correspondingly.

Users were transportable in the sense that they can leave their connection and join another system at any time. Furthermore, the MAC layer protocol is 802.11, and the MAP router

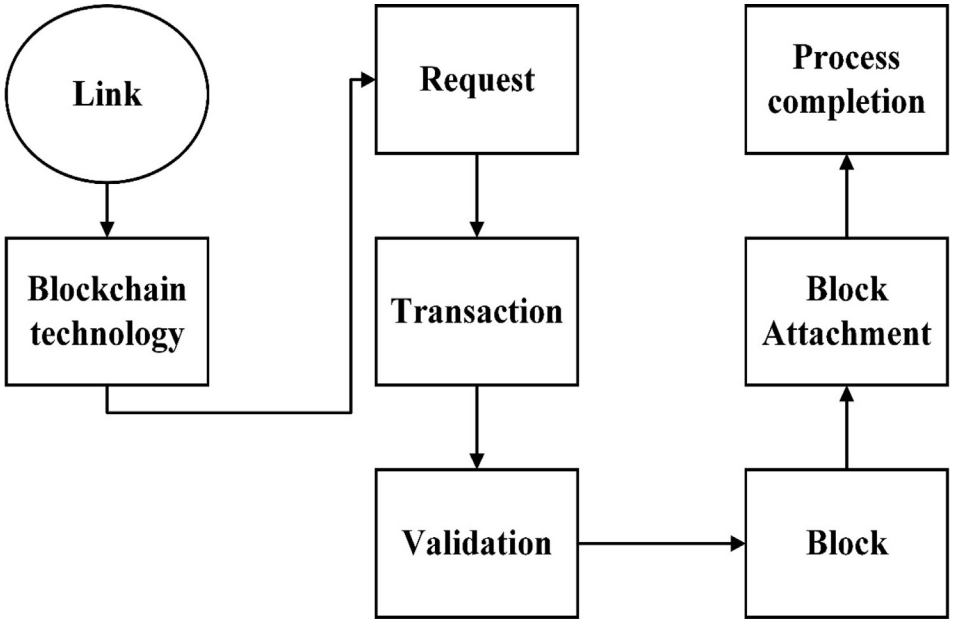

Fig. 5 Transaction blockchain diagram.

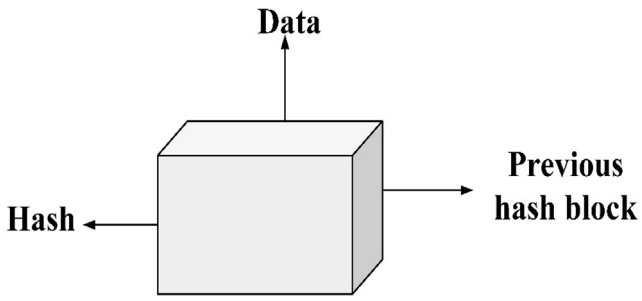

Fig. 6 Block of Hash.

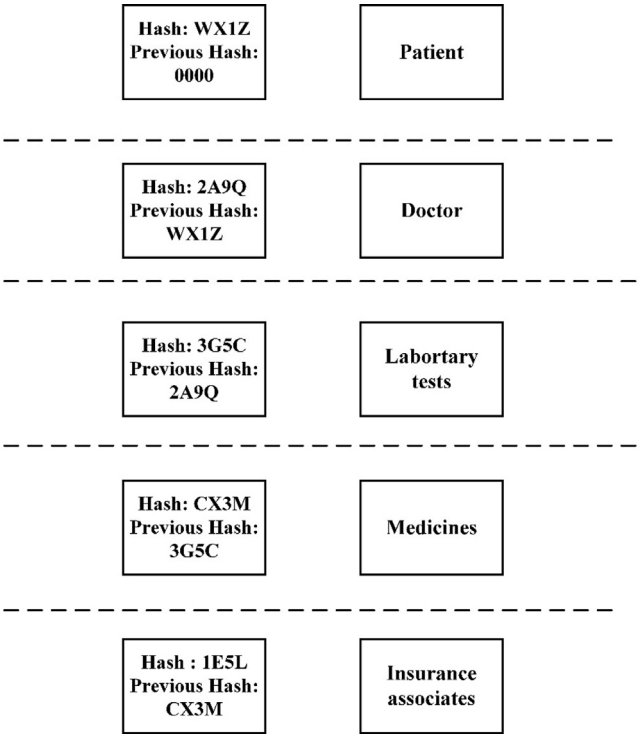

Fig. 7 Blockchain formation.

has communication distances of 120 m/s. Each node also was allocated a randomly initialized TV. At first, 25 nodes are constructed to serve as blockchain nodes. In addition, a simulated data producer is worn, which generates data utilizing a normal pattern of distribution [37]. To assess security, quality is defined in terms of metrics at which IoT devices are penetrated by attackers. During communications, network packets or users are introduced into the system depending on a posterior distribution. Wormholes and falsifying are considered serious routing concerns since the former reduces system performance by informing the transmission paths of users' requests, whereas the latter arbitrarily drops packets and could be detected too early. The introduction of compromised nodes, miners, and network transformation to compromised nodes is dependent on the probability indicated in Table 3, which is that 20 of the 250 installed IoT devices and networks are malicious. Furthermore, a falsification attack is examined, where one of the transmitting entities is compromised by attackers that attempt to disrupt the communication. The falsification nodes indicate that 5 out of 25 sensor nodes, 45 out of 100 sensor nodes, and 150 out of 250 sensor nodes were corrupted in a particular unit time.

Furthermore, the transformation of a trusted device to malicious after falsifying attack indicates that among 10 miners, 25 nodes (in terms of low network density) are transformed to malicious, as shown in Table 4. Taking all of these parameters into account, effectiveness analysis is completed in 60 s [38]. The proposed framework's design includes a blockchain network accountable for certifying the authenticity of users, two gateway gateways that provide communication between the internet and devices, and gateways that provide services to users who primarily use internet providers. The performing nodes are in charge of providing services to their clients, whilst miners or validating networks are in charge of validating the authenticity of network entities [39].

Table 2 Parameter of simulation.

Grid facet	400 m × 400 m
Number of nodes in CRN	10, 250
Size of data or request of the user	128 Bytes
Physical layer	PHY 802.11
Transmission Range	120 m
Simulation time	60 *sec*

3.6. Parameter for performance

Several parameters are collected to compare the proposed framework's effectiveness to that of the present technique [40]. The existing approach does not detect rogue devices depending on TV; however, the suggested scheme analyzes three separate aspects:

- Whenever a false developer created a false product demand at work.
- The security features of corrupted IoT devices, including falsification assault, wormhole intrusion, and item decrease percentage
- Probabilistic identification situations in the presence of compromised mining

Fig. 8 compares the proposed system's effectiveness to existing approaches for detecting Malicious Nodes (MN) in networks related to corresponding nodes, including the probability of a falsification operation.

Furthermore, attack resistance against wormhole attacks is studied for networks with 25 nodes. Furthermore, Figs. 9, and 10 demonstrate the verification possibility, probabilistic possibilities depending on the trust factor, and past historical interaction examined by authenticating networks [41]. In comparison to MN predictions, the suggested framework provides 86 percent accuracy, which can be increased if the experiment is repeated over a longer length of time. In comparison to existing systems, the measurement variables in the conceptual methodology perform more effectively [42].

Table 3 NS2 configuration for various network environment.

Sl.no	Virtual Machine (VM)	Compromised nodes	Transmitting nodes	Miners
1	Node 1	5	25	10
2	Node 2	45	100	50
3	Node 3	150	150	100

Table 4 Various probability utilized for performance analysis.

Sl.no	Action	Probabilities
1	Malicious node addition	5%
2	Compromised node	10%

4. Result and discussion

The suggested framework was evaluated using numerous users, and a modified reference model was proposed. The experimental assessment was effective, and multiple findings for various parameters were recorded. The findings of system condition and test results indicated are reported in the preceding subsections. The system operated as expected, and all measured values for the suggested solution for every healthcare method are positive.

The experimental analysis of proposed and traditional procedures was effective, and multiple findings for different parameters were recorded. The findings of the design and performance suitable to analyze are reported in preceding subgroups of a performance evaluation. The system performed as intended, and all performance requirements for every healthcare information for the suggested framework were acceptable. Furthermore, the proposed approach's efficiency is close to 86 %, which would continue to enhance when detected MNs are removed from the network. The identification of MNs is predicated on trust, with the removal of discovered MNs having no negative impact on the performance of other nodes. The suggested mechanism evaluates the confidence of all other networks at regular intervals, and nodes that are affected and operate deliberately will have a poor rating and confidence due to a high production residual value, black hole, and falsified assault, but will always be recognized in the long term. As shown in Fig. 9, the suggested scheme has a lower product loss ratio than the present methodology. The explanation for this enhancement is increased transparency between networks that monitor the actions of neighboring nodes. Fig. 9 depicts the enhanced performance from a wormhole and falsifying assaults. The Blockchain records the specifics of each node's activity, which eliminates the possibility of editing or changing any data during transfer from one location to the next.

Furthermore, Fig. 10 depicts the greatest and median verification latency in the event of an intrusion assault, as well as how the current and planned methodology can access legitimate networks in the event of an intrusion assault. The existing process used many security measures at several levels of interaction, making it exceedingly easy for hackers to brute–force assault the security measures used individually at the transit, perceptual, and application levels.

However, the suggested system keeps the Blockchain for such an existing system, making it difficult to anticipate the hashed of all nodes (modules) at once. Fig. 9 depicts the prob-

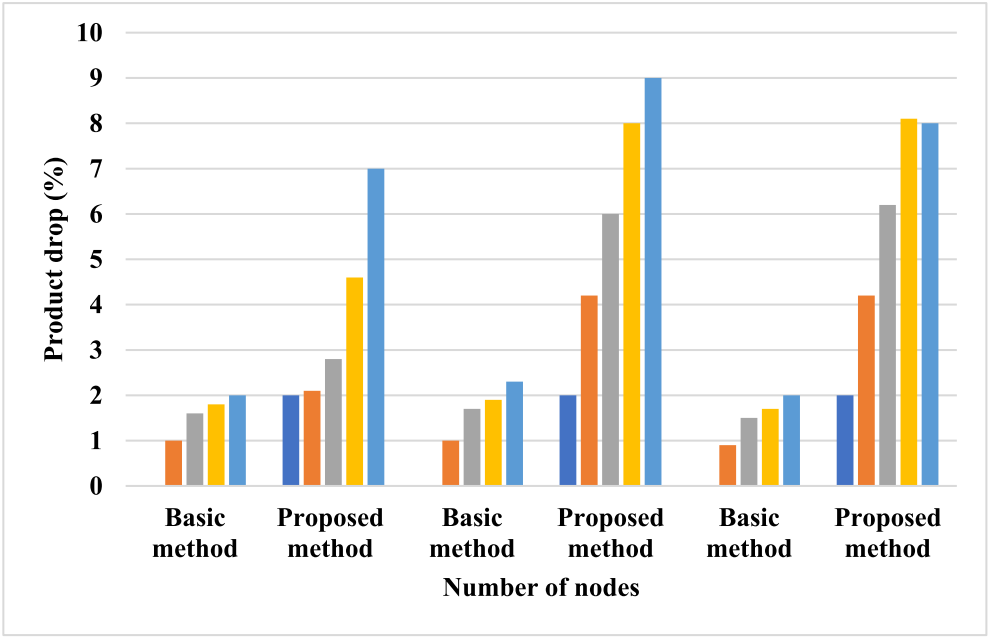

Fig. 8 Wormhole, falsification, and product drop possibility over a minimum network dimension.

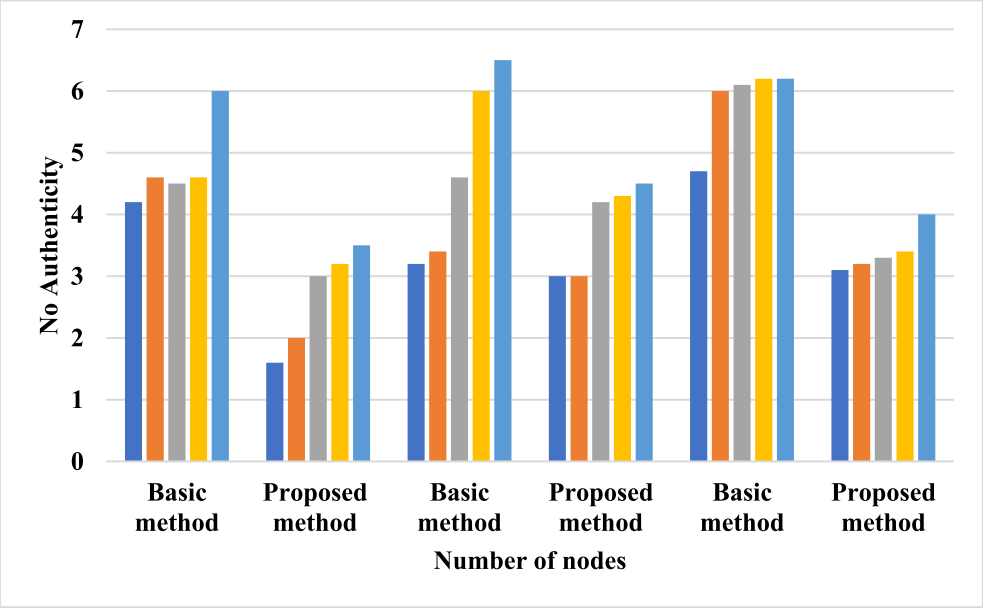

Fig. 9 Probability situations to measure the node's authentication.

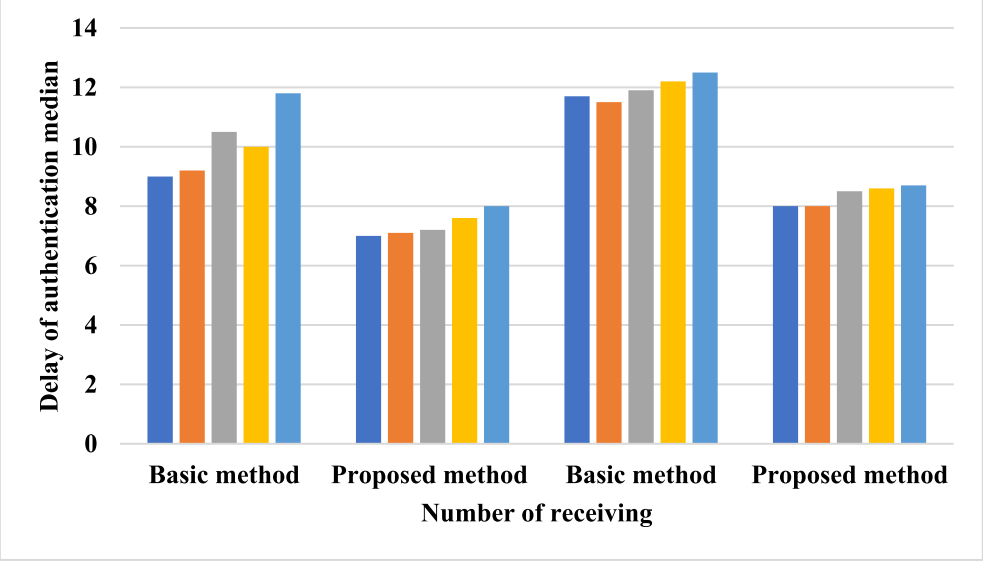

Fig. 10 The impact of having more mobile clients than usual and having maximal verification.

ability situations of an authentication method in which, as the quantity of MNs (namely, mining or peer stations) increases with node density, both techniques recognize the valid node. The suggested system, which preserves a Blockchain between each node, may determine the trusted node. Furthermore, the accuracy is near to 86 %, which will improve overtime as recognized MNs are removed from the system. The identification and segmentation of MNs depending on confidence do not impair the functioning of other networks.

After a certain amount of time, the suggested mechanism evaluates the trust and ratings of their networks. Endpoints that have been attacked and are acting aggressively will get a poor grade and trust (due to a lower product drop percentage, wormhole, and falsified attack) and can never be evaluated again.

5. Conclusion

This paper evaluates multimedia data processing in IoT healthcare systems and offered a robust healthcare architecture based on blockchain technologies. Individual activity acquired by IoT devices is saved inside the Blockchain to guarantee confidentiality and visibility between patients, and intermediaries, and to track every behavior of the pathways. The suggested framework expands on the Blockchain movement to maintain the protection and integrity of patient records, document avail-

ability, and the shipment procedure between provider and client. Furthermore, the necessity for blockchain in healthcare is it could collect intermediary activities, health records data, or drug shipment phenomena from IoT sensors dedicated to elements moving from one location to another after from supplier to client. Illegal behavior could be directly detected at every point in the communication chain. However, the suggested framework's operational study was based on the illicit acts or communications performed by hostile IoT devices. The experimental examination of hostile IoT devices from illegal behavior including over-product drop percentage, falsified assault, wormhole intrusion, and probability verification situations reveals an 86 percent success percentage in the proposed technique versus existing alternatives. In addition, the transaction duration or estimated cost during multimedia information transfer procedures in healthcare would be investigated in future research.

Funding Statement

This work was funded by the Deanship of Scientific Research at Jouf University under Grant No (DSR-2021-02-0375).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors would like to thank the Deanship of Scientific Research at Jouf University for supporting this work by Grant Code: (DSR-2021-02-0375).

References

[1] A.A. Abdellatif, A.Z. Al-Marridi, A. Mohamed, A. Erbad, C.F. Chiasserini, A. Refaey, SsHealth: Toward Secure, Blockchain-Enabled Healthcare Systems, IEEE Network 34 (4) (2020) 312–319.

[2] Chakraborty, Sabyasachi, Satyabrata Aich, and Hee-Cheol Kim. 2019. "A Secure Healthcare System Design Framework Using Blockchain Technology." In 2019 21st International Conference on Advanced Communication Technology (ICACT), 260–64. PyeongChang Kwangwoon_Do, Korea (South): IEEE. https://doi.org/10.23919/ICACT.2019.8701983.

[3] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives, Cryptography 3 (1) (2019) 3, https://doi.org/10.3390/cryptography3010003.

[4] A.I. Taloba, I.A. Mohamed, A.B. Aissa, L.F. Hussein, IoT enabled modulated residential surveillance system using Fuzzy logic, Mater. Today:. Proc. (2021).

[5] Rayan, Alanazi, Ahmed I. Taloba, Abd El-Aziz, M. Rasha, and Amr Abozeid, IoT enabled secured fog based cloud server management using task prioritization strategies, Int. J. Adv. Res. Eng. Technol. 11(9) (2020).

[6] H. Wang, IoT based clinical sensor data management and transfer using blockchain technology, J. ISMAC 2 (03) (2020) 154–159.

[7] Srivastava, Gautam, Reza M. Parizi, Ali Dehghantanha, The Future of Blockchain Technology in Healthcare Internet of Things Security, in: Kim-Kwang Raymond Choo, Ali Dehghantanha, Reza M. Parizi (Eds.), Blockchain Cybersecurity, Trust and Privacy, Advances in Information Security. Springer International Publishing, Cham, 79 (2020) 161–84. https://doi.org/10.1007/978-3-030-38181-3_9.

[8] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations, Neural Comput. Appl. (2021) 1–16.

[9] Ahmed I. Taloba, Alanazi Rayan, Ahmed Elhadad, Amr Abozeid, Osama R. Shahin, Rasha M. Abd El-Aziz, A Framework for Secure Healthcare Data Management Using Blockchain Technology, Int. J. Adv. Comput. Sci. Appl. 12 (12) (2021). https://doi.org/10.14569/IJACSA.2021.0121280.

[10] P.N. Srinivasu, A.K. Bhoi, S.R. Nayak, M.R. Bhutta, M. Woźniak, Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network, Electronics 10 (12) (2021) 1437.

[11] Ismail, Safaa SI, Romany F. Mansour, Abd El-Aziz, M. Rasha, Ahmed I. Taloba, Efficient E-Mail Spam Detection Strategy Using Genetic Decision Tree Processing with NLP Features, Computational Intelligence and Neuroscience 2022, 2022.

[12] Quasim, Mohammad Tabrez, Alaa Abd Elhamid Radwan, Goram Mufareh M. Alshmrani, Mohammad Meraj, A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry, in: 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), IEEE, 2020, 605–609.

[13] A.I. Taloba, An Artificial Neural Network Mechanism for Optimizing the Water Treatment Process and Desalination Process, Alexandria Eng. J. 61 (12) (2022) 9287–9295.

[14] G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A Hybrid Framework for Multimedia Data Processing in IoT-Healthcare Using Blockchain Technology, Multimedia Tools Appl. 79 (15–16) (2020) 9711–9733, https://doi.org/10.1007/s11042-019-07835-3.

[15] R. Arul, Y.D. Al-Otaibi, W.S. Alnumay, U. Tariq, U. Shoaib, M.D. Piran, Multi-Modal Secure Healthcare Data Dissemination Framework Using Blockchain in IoMT, Pers. Ubiquit. Comput. (2021) 1–13.

[16] P. Hemalatha et al, Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology, Turkish J. Comput. Math. Educ. (TURCOMAT) 12 (2) (2021) 2554–2561.

[17] A.A. Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S. Rahman, Privacy-Friendly Platform for Healthcare Data in Cloud Based on Blockchain Environment, Future Gener. Comput. Syst. 95 (June) (2019) 511–521, https://doi.org/10.1016/j.future.2018.12.044.

[18] Liu, Yue, Qinghua Lu, Chunsheng Zhu, Qiuyu Yu, A Blockchain-Based Platform Architecture for Multimedia Data Management, ArXiv:2009.03012 [Cs], 2020, September. http://arxiv.org/abs/2009.03012.

[19] Chendeb, Nada, Nour Khaled, Nazim Agoulmine, Integrating blockchain with iot for a secure healthcare digital system, in: 8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020), pp. 1-8. 2020.

[20] M. Tahir, M. Sardaraz, S. Muhammad, M.S. Khan, A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics, Sustainability 12 (17) (2020) 6960, https://doi.org/10.3390/su12176960.

[21] Vora, Jayneel, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M.S. Obaidat, Joel J.P.C. Rodrigues, "BHEEM: A Blockchain-Based Framework for Securing

Electronic Health Records, in: 2018 IEEE Globecom Workshops (GC Wkshps), 1–6. Abu Dhabi, United Arab Emirates: IEEE, 2018. https://doi.org/10.1109/GLOCOMW.2018.8644088.
[22] V. Patel, A Framework for Secure and Decentralized Sharing of Medical Imaging Data via Blockchain Consensus, Health Inform. J. 25 (4) (2019) 1398–1411, https://doi.org/10.1177/1460458218769699.
[23] Y.i. Chen, S. Ding, X.u. Zheng, H. Zheng, S. Yang, Blockchain-Based Medical Records Secure Storage and Medical Service Framework, J. Med. Syst. 43 (1) (2019) 1–9.
[24] M. Du, Q. Chen, J. Chen, X. Ma, An Optimized Consortium Blockchain for Medical Information Sharing, IEEE Trans. Eng. Manage. 68 (6) (2020) 1677–1689.
[25] G. Zhang, X. Zhang, M. Bilal, W. Dou, X.u. Xiaolong, J.J. Rodrigues, Identifying Fraud in Medical Insurance Based on Blockchain and Deep Learning, Future Generation Comput. Syst. 130 (2022) 140–154.
[26] Tripathi, Gautami, Mohd Abdul Ahad, Sara Paiva, "S2HS-A Blockchain Based Approach for Smart Healthcare System, in: Healthcare, 8:100391. Elsevier, 2020.
[27] G. Xue, F. Lin, S. Li, H. Liu, Adaptive dynamic surface control for finite-time tracking of uncertain nonlinear systems with dead-zone inputs and actuator faults, Int. J. Control Autom. Syst. (2021), https://doi.org/10.1007/s12555-020-0441-6.
[28] H.B. Mahajan, A.S. Rashid, A.A. Junnarkar, N. Uke, S.D. Deshpande, P.R. Futane, A. Alkhayyat, B. Alhayani, Integration of Healthcare 4.0 and Blockchain into Secure Cloud-Based Electronic Health Records Systems, Appl. Nanosci. (2022) 1–14.
[29] S. Ha, L. Chen, H. Liu, Adaptive fuzzy variable structure control of fractional-order nonlinear systems with input nonlinearities, Int. J. Fuzzy Syst. (2021), https://doi.org/10.1007/s40815-021-01105-x.
[30] K. Khatter et al, Non-Functional Requirements for Blockchain Enabled Medical Supply Chain, Int. J. Syst. Assurance Eng. Manage. (2021) 1–13.
[31] A. Hasselgren, J.-A. Rensaa, K. Kralevska, D. Gligoroski, A. Faxvaag, et al, Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study, J. Med. Internet Res. 23 (7) (2021) e28496.
[32] T. Justinia, Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences, Acta Informatica Medica 27 (4) (2019) 284.
[33] Sharma, Bhavye, Raju Halder, Jawar Singh, Blockchain-Based Interoperable Healthcare Using Zero-Knowledge Proofs and Proxy Re-Encryption, in: 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), IEEE, 2020, 1–6.
[34] R. Angeles, Blockchain-Based Healthcare: Three Successful Proof-of-Concept Pilots Worth Considering, J. Int. Technol. Inform. Manage. 27 (3) (2019) 47–83.
[35] Qahtan, Sara, Khaironi Yatim, A.A. Zaidan, H.A. Alsattar, O. S. Albahri, B.B. Zaidan, A.H. Alamoodi, H. Zulzalil, M.H. Osman, R.T. Mohammed, Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems, IEEE Transactions on Industrial Informatics, 2022.
[36] Abou-Nassar, M. Eman, Abdullah M. Iliyasu, Passent M. El-Kafrawy, Oh-Young Song, Ali Kashif Bashir, Ahmed A. Abd El-Latif, DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems, IEEE Access 8 (2020) 111223–38.
[37] A. Yogeshwar, S. Kamalakkannan, Healthcare Domain in IoT with Blockchain Based Security-A Researcher's Perspectives, in: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2021, 1–9.
[38] Rathi, Vipin Kumar, Nikhil Kumar Rajput, Shubham Mishra, Bhavya Ahuja Grover, Prayag Tiwari, Amit Kumar Jaiswal, M. Shamim Hossain, An Edge AI-Enabled IoT Healthcare Monitoring System for Smart Cities, Comput. Electr. Eng. 96 (2021) 107524.
[39] M. Elloumi, M.A. Ahmad, A.H. Samak, A.M. Al-Sharafi, D. Kihara, A.I. Taloba, Error correction algorithms in non-null aspheric testing next generation sequencing data, Alexandria Eng. J. 61 (12) (2022) 9819–9829.
[40] A. Panwar, V. Bhatnagar, Analyzing the Performance of Data Processing in Private Blockchain Based Distributed Ledger, J. Inform. Optimiz. Sci. 41 (6) (2020) 1407–1418.
[41] K. Srinivasan, Geetanjali Rathee, M. Ramkumar Raja, Naveen Jaglan, T.V. Mahendiran, Thangam Palaniswamy, Secure Multimedia Data Processing Scheme in Medical Applications, Multimedia Tools Appl. 81(7) (2022) 9079–9090.
[42] A. Elhadad, F. Alanazi, A.I. Taloba, A. Abozeid, Fog Computing Service in the Healthcare Monitoring System for Managing the Real-Time Notification, J. Healthcare Eng. 2022 (2022).