Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 3440–3452, DOI 10.12694/scpe.v25i5.3164

IMPROVING DATA SECURITY AND SCALABILITY IN HEALTHCARE SYSTEM USING BLOCKCHAIN TECHNOLOGY

K.R.ROHINI [*], DR.P.S.RAJAKUMAR [†], AND DR.S.GEETHA [‡]

Abstract. The wearable tech revolution and the proliferation of Internet of Things (IoT) gadgets have created exciting new opportunities for remote patient monitoring. Healthcare providers are increasingly utilizing wearable technologies to expedite the process of diagnosis and treatment. The healthcare and research fields have been substantially impacted by emerging technologies. On the other hand, there are legitimate worries regarding the security of data transfers and transaction recording upon using these technologies. Healthcare departments need easy data interchange for interoperability. Protecting data security and integrity is crucial when exchanging information with authorized parties. In many existing solutions, patients' sensitive data is collected and stored in smart healthcare systems. Scalability, breach or unauthorized access to this data can compromise privacy. The adoption of blockchain technology is one way to safeguard patient privacy in healthcare. Also, by facilitating the safe and secure exchange of data, blockchain technology is revolutionizing the healthcare industry by making traditional methods of diagnosis and treatment more reliable. However, blockchain has serious problems with its highly limited scalability. This article suggests a new method "SHORTBLOCKS" depending on blockchain technology for the safe administration and analysis of data. To circumvent the security-scalability issue and achieve high throughput, this study employs the newly introduced protocol "SHORTBLOCKS", which extends blockchain concept to a direct acyclic graph of blocks. The proposed system uses both a private and a public blockchain that are created on the new protocol. In order to analyze patient health data, a system using smart contracts and a private blockchain is built. The system logs the occurrence to the public blockchain in the case that the smart contract raises an alarm due to an unusual reading. This will fix the scalability issue with initial blockchain as well as the security and privacy issues involved in remote patient monitoring. Simulation results shows the performance of the proposed system by comparing with existing solutions, SPECTRE protocol and GHOSTDAG protocol.

Key words: Healthcare, Remote patient monitoring, Security and privacy, interoperability, Private blockchain, Public blockchain, Smart contracts, Shortblocks.

1. Introduction.

Clinical data is abundant in the healthcare industry due to the regular generation, access, and dissemination of enormous volumes of data. Due to privacy and security concerns, as well as the sensitive nature of the data, storing and distributing this enormous amount of data is not only necessary but also extremely challenging [1].

A wide variety of resources are available to various healthcare providers, including hospitals, pharmacies, and insurance providers [2]. The rapid development of ICT has allowed for the widespread use of wearable sensors to link many physical objects. Data processing, collecting, and creation on a massive scale are made possible by the electrical devices and software employed for this purpose. Although there are many healthcare facilities, the prevalence of lethal diseases such as pneumonia, influenza, cancer, heart diseases, etc. has risen dramatically [3]. Constant vigilance and tracking of vital signs has been made possible with the use of sensing devices that can gather, and analyze patient data, due to the technological revolution. Hospitals and other related departments receive this data for the purpose of delivering healthcare. Problems with legal interoperability are present here. Healthcare service delivery will be more efficient with a centralized system for managing and exchanging medical data [4].

In healthcare and clinical settings, safe, secure, and scalable (SSS) data-sharing is critically necessary for diagnosis and integrated clinical decision making. The ability for medical professionals to transmit patient

[*]Research Scholar, Dept. of CSE, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India (rohinimay19@gmail.com)

[†]Professor, Dept. of CSE, , Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India. (*rajakumar.subramanian@drmgrdu.ac.in)

[‡]Professor, Dept. of CSE, , Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India. (*somangeetha@drmgrdu.ac.in)

medical records to the relevant authority for expedited follow-up makes sharing of data, a crucial activity. Both primary care physicians and other medical professionals should have the ability to securely and quickly transmit their patients' clinical data to one another, so that everyone involved has access to the most current and accurate information regarding their patients' health. During treatment, doctors and hospitals need access to patients' medical records, but individuals also have a right to feel safe sharing their personal information with these institutions.

Conversely, e-health and tele-medicine are two popular areas where patients can get their clinical data reviewed by a specialist located far away. A "store-and-forward technology" or online healthcare monitoring in real-time (e.g., tele-monitoring, telemetry, and the like) is used to transmit patient data in these two online clinical setups [5]. Clinical specialists are able to remotely perform patient diagnosis and treatment in these online clinical contexts by exchanging clinical data. Because patient data is unique to each individual case, ensuring its confidentiality, integrity, and availability in all such therapeutic arrangements is a top priority. In order to facilitate relevant and healthy therapeutic discussions pertaining to instances involving faraway patients, the capacity to securely and scalablely transmit data is of the utmost importance. For the simple reason that better diagnosis and more efficient treatment are the outcomes of secure data transmission, which aids in clinical communication by soliciting opinions or confirmations from a group of clinical experts [6].

Additionally, several interoperability problems crop up frequently in this domain. The secure and reliable transfer of patient records between hospitals and universities, for instance, can be fraught with practical difficulties. Such exchanges of clinical data need considerable, trustworthy, and healthy collaboration between the entities involved. Difficult patient matching algorithms, ethical policies, legislation, and processes; sensitive clinical data; and data sharing agreements are all potential roadblocks. Prior to establishing a clinical data exchange, it is essential that all stakeholders agree on these and other important matters [7].

The proliferation of remote devices linked to the internet for data and access transfer has been greatly enhanced by the persistent developments in the IoT domain. Thus, from the field of education to that of supply chain management, the Internet of Things (IoT) has transformed and shaken up nearly every industry on the planet. Internet of Things (IoT) has also shown to be highly effective in the healthcare industry, streamlining diagnostic processes and effectively tracking patients' activities. In addition, the main point we want to make about the Internet of Things is that it helps with patient monitoring even when the patient isn't actively using their devices, which may be a real challenge with the current system. Additionally, there are vast opportunities for improved diagnostic and treatment efficiency that arise from remote access to data and ongoing analysis of it.

Blockchain applications have recently garnered a lot of interest for safe healthcare data transmission [8], biological data sharing [9], e-health data sharing [10], and general activities. A peer-to-peer (P2P) network is the foundation of a blockchain. In essence, it is a cryptographic, algorithmic, and mathematically expressed multi-field network architecture that aims to address the constraints of standard distributed database synchronization methods through the use of distributed consensus techniques.

With the introduction of blockchain, the technology recently assumed full control of all storage, transactions, and access. Additionally, blockchain technology has demonstrated tremendous promise in a variety of industries, that includes retail, healthcare, supply-chain management, finance, and more. The privacy and security of data is a constant concern in healthcare because many parties rely on it to carry out their own objectives. For instance, insurance companies play a crucial role in the delivery of a specific service to patients; in order to do their jobs properly, they need access to patients' data for analysis and service planning. Unfortunately, it is not uncommon for companies to manipulate or even leak this data. Consequently, this system is an authentic answer to the problem of data misuse and to the problem of keeping the many stakeholders' faith in one another. With the use of Blockchain technology, healthcare organizations may eliminate the need for reconciliation, rework, and repetition. We can find the optimal level of service intensity in a predictive healthcare setting with the help of artificial intelligence (AI). It is important to communicate with patients, professionals, and careers in a way that is appropriate for each setting.

Consider a case study pertaining to the COVID-19 case as an example. When it comes to COVID-19-safe clinical practice, blockchain technology is crucial. The integration of Blockchain technology with AI has the ability to speed up the process of diagnosing and treating COVID-19 patients, while also helping to create therapeutic guidelines for future outbreaks that could be similar to coronavirus.

Blockchain technology allows for the secure and private sharing of data from many sources, including hospitals, primary care physicians, pediatricians, clinical laboratories, and others. Artificial intelligence solutions are utilized for data analysis.

Take the COVID-19 case study as an example. Cryptography is the backbone of Covid-19-safe medical practice. Rapid diagnosis and treatment of COVID-19 patients is possible with the use of Blockchain and AI, which also assists in developing treatment recommendations for future outbreaks (like coronavirus). With a blockchain-based system, pediatricians, primary care physicians, hospitals, and clinical laboratories may all securely share patient data. Data analysis makes use of AI solutions. The paradigm promotes research into appropriate medicines, helps with risk management, and inspires the development of new drugs.

The use of Internet of Things and Blockchain technologies for secure data transmission in smart health care systems is proved to be effective. However, with the concept of blockchain, scalability problem arises. Many existing solutions are not addressing properly the problem of scalability and secure communication in smart health care system. Hence, a sophisticated method is required to console the problem of scalability while transferring the data security using Internet of Things and Blockchain in Smart health care Systems.

This study proposes a novel approach called ”SHORTBLOCKS” that incorporates the blockchain concept. Its purpose is to offer scalable and secure communication in the healthcare domain using blockchain as a paradigm. Here is the breakdown of the remaining sections of the paper: Section 2 provides a synopsis of relevant background material and related work in the healthcare domain that makes use of blockchain technology. In Section 3, the proposed method's framework is described in terms of how healthcare and the medical industry might use blockchain technology. Section 4 lays out the strategy that has been suggested. The suggested protocol is demonstrated in Section 5. In Section 6, we go over the findings from comparing the current state of blockchain technology with the suggested technique ”SHORTBLOCKS” that incorporates blockchain technology. In Section 7, we lay out the final thoughts, and in Section 8, we look forward to the potential applications of blockchain technology in healthcare, and finally, we provide a list of references.

2. Related Work. The paper's primary rationale for investigating blockchain technology's potential use in healthcare is based on the work of [11], who comprehensively outlined several current tendencies in this field of study. Since Bitcoin's inception in [12], the potential applications of the underlying technology have been practically limitless, even beyond the financial sector.

Public blockchains are decentralized database systems that let anyone with an internet connection to determine who may access the data stored on them. Ivan [13] also showed how to encrypt health data using this method. This approach creates a PHR (personal health record) based on blockchain by publicly storing encrypted healthcare data. The patients were able to gain improved access to their clinical data through the way they suggested. Patients can now freely observe and manage their information, as well as take part in maintaining their data and making it available to any associated healthcare provider. Another study by Chen et al. [14] suggested a system for managing and sharing patients' confidential medical data that incorporated blockchain technology with cloud storage. Ensuring the secure storage and communication of personal medical data is a potential use case for the suggested approach. The proposed method is novel because it eliminates the need for a middleman by providing patients full access to and management of their own medical records.

In order to streamline the administration of electronic health record transactions, Dey et al. [15] suggested a blockchain-based Internet of Things model. As a principal agent for linking the bio-sensors to the IoT platform, the architecture suggested using the MQTT protocol. In addition, the design included the IPFS (InterPlanetary File System), which may identify state entries or block modifications caused by certain transactions appended to blocks in order to decrease stored transaction deduplication. In [16], Gem, a provider of enterprise blockchain solutions, announced that Philips Blockchain Lab, a research and development centre of healthcare massive Philips, would be the first major healthcare operator to join the Gem Health network. Gem Health is an Ethereum-powered network for developing healthcare applications and shared infrastructure.

To assess the current state of patient healthcare, Wang et al. [17] laid forth a blockchain architecture that uses AI healthcare systems and parallel execution instead. In order to aid in clinical decision-making, the suggested method evaluates the patient's general status, diagnosis, and treatment plan while also analyzing the related therapeutic processes carrying out computational trials in parallel. To assess the precision of diagnosis and efficacy of therapy, the suggested approach has undergone testing on real and virtual healthcare networks.

The use of blockchain technology to verify the achievement of clinical trial endpoints was introduced in [18]. The method was put to the test by Irving and Holden using a clinical trial methodology that had previously documented result switching. Scientific research' credibility and the application of blockchain technology as an inexpensive, independently verifiable auditing tool were both validated.

A healthcare system controlled by the Internet of Things was suggested by Budida et al. [19] in an interactive environment. The suggested design is based on generative data ingestion from biosensors and smart wearables, which then provides patients with clear feedback and simple solutions. In order to provide patients with quicker and more accurate recommendations, A Smart Hospital system, proposed by Sivagami et al. [20], would combine human reaction suggestions with the efficiency of sensors. The proposal proposes a system that uses radio frequency identification (RFID), wireless sensor networks (WSN), and smart wearables to accomplish a number of goals. These goals include smart sensing of the patient's environment, ward allocation according to doctor placement requirements, movement monitoring, and report analysis based on calculated data, after data has been uploaded by the sensors.

An innovative platform for the exchange of healthcare information, BloCHIE was created by Jiang et al. [21]. Using blockchain technology embedded in many sources, the proposed platform assesses the needs for healthcare data exchange, particularly with regard to electronic medical records and personal healthcare data, but also handles a wide range of other data types. They integrated on-chain and off-chain verification procedures into the platform to ensure it met the desired standards of privacy and authenticity. All parties involved in the healthcare system, from payers to providers to patients, stand to benefit from blockchain technology's revolutionary potential in the areas highlighted by Nichol in [22]. In order to transform healthcare, Nichol amplifies the principles and applies examples that are at the forefront of a new frontier. Written in the style of his articles, blogs, and thoughts, the book lays forth the groundwork for an internal revolution in healthcare.

Discussing the foundations of all the different kinds of blockchains and how they might be utilized in the healthcare industry for data maintenance, validation, and storage. The various blockchain designs that are currently available were discussed by Zainab Alhadhrami et al. [23]. Furthermore, the consortium blockchain was found to be the solution that was essentially pre-built for healthcare data storage. To put it simply, a consortium blockchain is a valid blockchain in which the node owner and miners share control of access. Furthermore, the operation of the consortium blockchain is predicated on the consensus principle, which requires the approval of the majority of stakeholders or blockchain nodes.

Clinical professionals and healthcare entities can significantly enhance medical data sharing, privacy, and security by utilizing blockchain technology. In a similar vein, Cryan, M.A. [24] suggested a novel and methodical design based on blockchain technology to secure private patient information, resolve pressing data security concerns, and integrate blockchain software into an entire healthcare organization's infrastructure.

In order to address the privacy requirement imposed by HIPAA, Ahram et al. [25] created a healthcare blockchain that controlled the access to patients' demographic and racial information. The study also demonstrated the generative design of a blockchain network that included three distinct kinds of nodes: those for primary care physicians, referral services, and urgent care.

For the purpose of diagnosing and treating malignant tumors in distant patients, Shubbar introduced a healthcare framework based on blockchain technology in [26]. Patients' data at both specialty medical centers and their homes may be reliably and securely verified using the proposed protocol's use of smart contracts and blockchains. As a last point, Taylor unveils a new initiative in [27] that will utilize blockchain technology to strengthen the safety of the pharmaceutical distribution network. Still in its early phases of development, the initiative aims to streamline the process of tracing the origin and manufacturing date of medicines by utilizing blockchain monitoring and time stamps.

Healthcare applications serve a variety of objectives, including but not limited to pharmaceuticals, biomedical research, neurology, genomics, EHRs, clinical facts, processes, and decision-making [28]. By standardizing data and establishing communication protocols, Internet of Things (IoT) technology can improve healthcare efficiency. More effective healthcare services lead to less data interoperability, safer patient data, improved connectivity, and user interfaces. The healthcare industry and the development of trustworthy healthcare applications receive a lot of attention from researchers [29]. Ensuring that stakeholders, such as pharmacies,

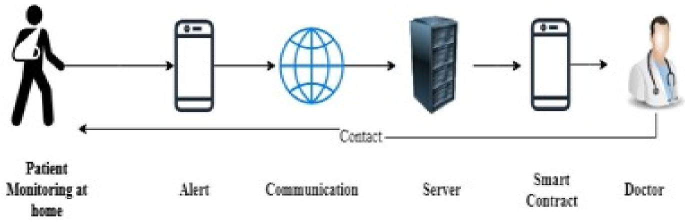

Fig. 3.1: Smart Patient Health Care Monitoring

hospitals, and patients, can access healthcare records securely and without data tampering is of the utmost importance. It is possible to overcome these obstacles with blockchain technology [30].

Omar et al. (2019) [31] suggested a blockchain-based system for EMR maintenance. A par acentric healthcare data management system was created by the authors. This system uses block chain technology as a storage method to promote privacy. Under this system, patients will have full authority over their information. This method improves privacy, security, accountability, and integrity while increasing patient interest in EMRs.

In [32], GHOSTDAG protocol is employed which uses a public and a private blockchain. The authors proposed a method that utilizes a private blockchain, the system logs the event to the public blockchain for data transfer. The drawback of this system is privacy and security concerns surrounding remote patient monitoring. In [33], the use of blockchain technology to verify the achievement of clinical trial endpoints was introduced with SPECTRE protocol. By analyzing a clinical trial protocol that has previously documented outcome switching, Irving and Holden conducted an empirical evaluation of this strategy. They validated the validity of scientific research and the usage of blockchain technology as an inexpensive, independently verifiable auditing technique. However the security and privacy concerns remain still unanswered.

With the introduction of smart contracts, Blockchains can now store data that can be retrieved at will (Li et al., 2019) [34]. Nevertheless, smart contracts necessitate expert assistance for administration and maintenance and might be a pain to set up. Several scholarly articles present potential frameworks for health-related IoT applications. Due to the extra permission-based security they provide, private Blockchains form the basis of these concept designs. One such approach was to develop and manage a separate set of smart contracts for each Internet of Things (IoT) device.

3. Framework. Patients are finding it increasingly difficult to get an appointment with a primary care physician or other healthcare provider due to the massive growth in the patient population in many nations. The proliferation of Internet of Things (IoT) and wearable technology in the last several years has enhanced the care quality for patients using remote patient monitoring. More people can be treated by doctors because of this. Patients can be monitored and cared for outside of the typical clinical setting (such as at home) with smart patient monitoring. The primary benefit is the inherent ease of service it provides to patients. Patients have the option to remain in touch with their healthcare providers as needed. Additionally, it enhances the quality of care while decreasing medical expenses. This is the primary motivation for healthcare providers looking at ways to make remote patient monitoring accessible to everyone. A remote patient monitoring system could primarily consist of a smartphone, an app for remote patient monitoring, and a specifically developed device that can record and send health data to smart contracts as shown in Fig 3.1. When it comes to remote patient monitoring, wearable technology and the internet of things are crucial. For the purpose of health monitoring, illness diagnosis, and treatment, wearable devices transmit data collected from patients to healthcare facilities.

Smart electronic devices with microcontrollers that may be worn as accessories or implanted into garments are known as wearable gadgets in healthcare. They have sophisticated capabilities including built-in alerting systems, real-time feedback, and wireless data transmission, and they are easy to use and barely noticeable. A variety of vital signs, including respiration rate, blood sugar, and pressure, can be transmitted to medical professionals by means of these devices.

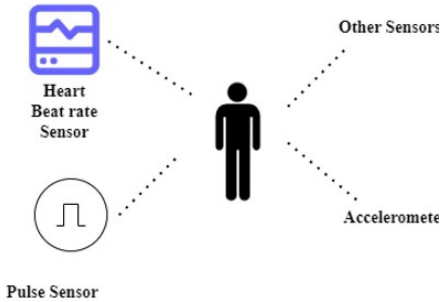

Fig. 3.2: Different Wearable Devices

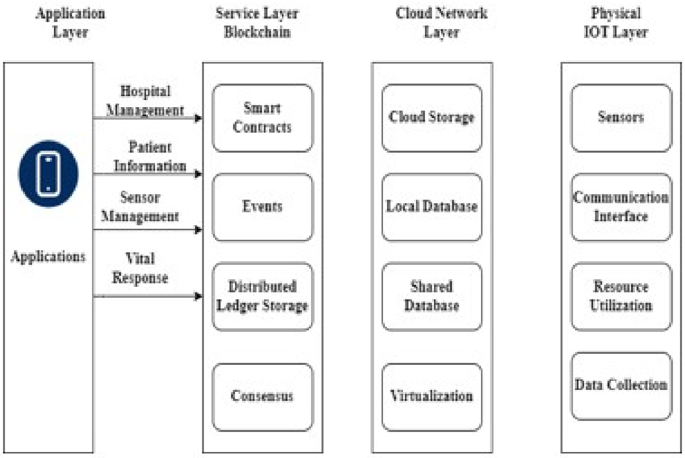

Fig. 3.3: Proposed Framework

Wearable devices are a part of the Internet of Things (IoT). These devices can connect to each other and share data through the software, electronics, sensors, actuators, and connectivity they contain as shown in Fig 3.2. Such infrastructure necessitates secure data sharing in order to manage such patient data with other institutions. The risk of exposure can increase if health data is shared, and the data is very sensitive. The second issue is that trust must be centralized in the present data sharing system because of its centralized architecture.

Blockchain technology may hold the key to ensuring the privacy and security of personal information. Blockchain technology ensures that data is secure and resistant to failures. In terms of data storage, it's a decentralized architecture. The healthcare system is the ideal fit for blockchain technology since data cannot be removed or altered from blocks. Nevertheless, blockchain's scalability and security remain unresolved. Blocks must propagate to all miners promptly for blockchain to be scalable and secure. Before the next block is formed, all honest nodes receive a message from the miner, who is responsible for maintaining the blocks, extending it to the blockchain. The scalability and processing performance issues are brought about by the proliferation of such lengthy blockchains in the existing approach. Consequently, we present a more sophisticated and extensible blockchain solution for the Remote Patient Monitoring system. For this purpose, we have adopted the SHORTBLOCKS protocol [33], a safe method of transaction confirmation that works at any network rate.

As an alternative to lengthy blockchains, SHORTBLOCKS organizes all blocks into a DAG, which is a Directed Acyclic Graph. The suggested healthcare system's design is shown in Fig. 3.3, where each layer represents the integration of multiple technologies. With the decoupled capability, developers can add or remove modules from the system as needed without impacting other modules or the system as a whole. Application, cloud-based network blockchain-based service, and Internet of Things (IoT) physical layers make up the suggested paradigm [34]. Computing healthcare equipment, data storage, and communication infrastructure make up the Internet of Things (IoT) layer. Connectivity, storage, a blockchain engine, and virtualization capabilities are all provided by the cloud-based network layer. Services such as consensus, identity management, distributed ledger technology (DLT), peer-to-peer (P2P) communication, and blockchain are provided by the blockchain-based service layer.

4. Proposed Methodology. The scalability and security of blockchain, however, remain unresolved. Fast block propagation to all miners is crucial to blockchain's scalability and security. Prior to the creation of the next block, any new blocks that are extended to the blockchain by a miner (the node responsible for maintaining them) are broadcast to all honest nodes. The issue of scalability and poor computational performance arises with the proliferation of such lengthy blockchains. As a result, we provide a blockchain system that is both more sophisticated and more scalable for use in smart health care system. The proposed method 'Smart Transfer" employs a new protocol, SHORTBLOCKS. It is a secure mechanism for transaction confirmation that can withstand any network throughput. The existing system uses traditional lengthy blocks whereas the proposed new protocol, SHORTBLOCKS integrates all blocks into a Directed Acyclic Graph.

As part of the proposed system, patients can access a variety of wearable medical equipment, including insulin pumps, blood pressure monitors, and more. A smartphone or tablet receives the health records and sends them to an application that formats and aggregates them. The finalized data, along with the specified threshold value, is transmitted to the appropriate smart contract on the private blockchain for thorough investigation. If the value is less than or equal to the threshold, the health reading is considered to be outside the normal range.

A public blockchain event will be created and alerted to smart devices and hospitals via the smart contract if the health reading is aberrant. Oracle [2] is one example of a smart contract that can talk to smartphones and other Oracle smart devices directly.

When an alert is issued, the public blockchain will only store the event. Certain Electronic Health Record (EHR) storage will receive the health data measured by wearable devices. Furthermore, electronic health record storage will receive treatment instructions from smart contracts or hospitals, and the blockchain will record the transactions. Integrating blockchain transactions with EHR ensures the integrity of patient medical records. As a result, it's easier to keep patient records in EHRs confidentially and to spot any unauthorized changes. Only designated nodes are able to execute smart contracts. Another responsibility of these selected nodes is to validate the new block. Care professionals, device manufacturers, and patients themselves are some of the potential viewers who could assist in limiting data exposure.

4.1. Components. The proposed system 'SHORTBLOCKS' consists of the following components:

a) Wearable Sensors: In order to communicate medical history, people are increasingly turning to wearable health devices. Smartphones link these devices, and raw health data is sent to them. These cutting-edge gadgets will soon be able to detect heartbeats, breast cancer through an implant worn in clothing, and glucose readings without ever collecting blood.

b) Patient: When a patient uses the system, it will record all of their medical history. Such information could include, among other things, heart rates, sleeping circumstances, and distance travelled. The onus for authorizing, rejecting, or revoking data access from third parties like insurance companies or healthcare providers should be on the patients themselves. After all, patients are the rightful owners of their personal data. In the event that medical attention is required, the patient will divulge their personal health information to the doctor of their choice. A patient has the right to cut off any communication with their healthcare provider, insurance company, or doctor once treatment has ended.

c) Health care Assistant: Health organizations and insurance companies employ healthcare providers to conduct diagnostic tests and treatments. The healthcare provider can initiate a request for access to patient's medical records and treatment history. They treat them as soon as they receive the signal alert from the organization.

d) Proposed SHORTBLOCKS: We employ two protocols based on blockchain technology: first, a private blockchain where all experiments involving patient health data are executed using smart contracts; second, a public blockchain where alerts are written and sent to smart devices and hospitals in the event that smart contracts issue them. These blockchains are built on proposed protocol.

e) Healthcare organization: Any time a patient needs medical attention or would need a competitive price for future coverage, they can contact their health insurance provider. The insurance provider may request access to customer data, such as health data from wearable devices and medical treatment history, in order to offer the finest healthcare facilities. It is also possible to store insurance claim occurrences in the blockchain.

4.2. Requirements. The following are the essentials in the proposed method:

- Health or treatment data stored on the blockchain can only be accessed by authorized entities. Secure logging of Internet of Things (IoT) devices, such as smart contracts, is essential for maintaining an accurate timeline of events and safeguarding the integrity of patient care. The patient must grant access to their healthcare provider or insurance company before they can see their medical records or treatment information.
- Accurate and hacker-proof medical gadgets and health data are essential. Blockchain is the ideal technology for healthcare systems since it is impossible to remove or alter data from individual blocks. Unfortunately, blockchain's poor processing speed means it cannot be relied upon in isolation. To achieve this goal, we are utilizing the SHORTBLOCKS protocol, which outperforms the original blockchain technology in terms of speed and security.

4.3. Algorithm. Patient information is collected through wearable devices and the information is sent to smart applications for processing. The processed information is sent to smart contract for further examination using private blockchain. If the readings exceed the abnormal value, then alert is raised. The alert event is then stored in public blockchain and alert is sent to the patient.
Shorblocks method will work as

1. Patient information is collected from wearable devices implanted in patients body
2. Smart Devices placed in the hospitals will collect the patients data. This information is placed in private blockchain.
3. After full examination of the patients data, if any emergency found, an event is raised.
4. An event is written in public block chain and alert is raised to the hospital(H), patient and mobile device for information.
5. Thus Shortblocks ensures the scalability, security and privacy of smart health care system.

Algorithm SHORTBLOCKS
procedure SHORTBLOCKS (P, PrB, PuB, H)
{
// P = Patient
// PrB= Private Blockchain
// Pub= Prublic Blockchain
// H=Hospital
Step:1 Patient(P) information is collected using wearable smart devices.
Step:2 Information is sent to the Smart devices, smart contracts
Step:3 The formatted information from the smart contract is sent to the private blockchain (PrB) for full examination
Step:4 If the information received, after full examination is found above the threshold, then it is declared as abnormal condition of the patient, needs treatment.
Step:5 An event is written in the public block chain(Pub) and alert is raised to the hospital(H), patient and mobile device for information.
}
end procedure

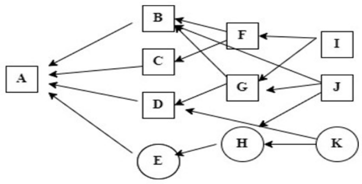

Fig. 5.1: SHORTBLOCKS cluster arrangement

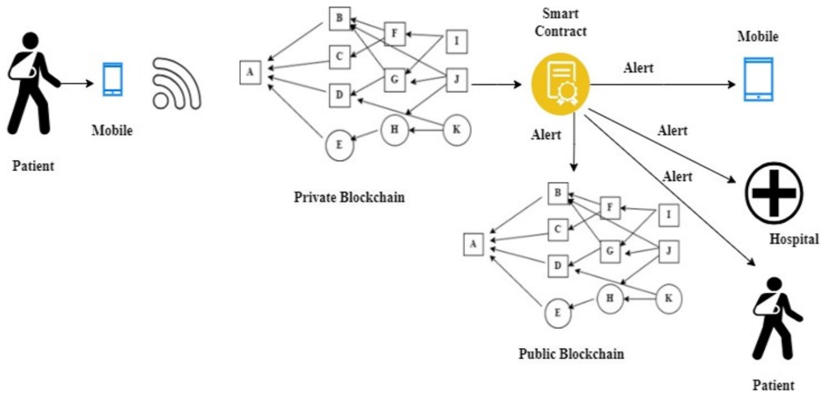

Fig. 5.2: SHORTBLOCKS process

5. Implementation. The efficiency with which each block is sent to all network miners prior to its creation determines the protocol's security. The process of creating blocks is tedious because a proof-of-work is required for each new block. A secure blockchain will have a block propagation time that is less than or equal to the time it takes for the entire network to generate a new block. With only three to seven transactions per second, blockchain is severely limited in its throughput.

The proposed SHORTBLOCKS protocol, on the other hand, is more suited to blockchain deployment in practice. A Directed Acyclic Graph, is used to arrange blocks in the proposed new protocol instead of a lengthy chain of blocks. The blocks are organised into a k-cluster via SHORTBLOCKS protocol, with blocks outside the cluster being indicated by square and those inside the cluster being indicated by oval, as depicted in Fig 5.1.

Patients in our proposed system use a variety of wearable medical devices, including but not limited to blood pressure monitors, insulin pumps, and others. The application formats and aggregates the health information that is provided to smart devices like smartphones and tablets. After finishing, the applicable smart contract receives the formatted information and sends it to the private blockchain for full examination, together with the threshold value as shown in Fig. 5.2. If the health reading is below the threshold value, it is considered abnormal compared to standard readings. Appropriate treatment will be suggested. An event will be created on the public blockchain and alerts smart devices and hospitals if the health reading is aberrant.

When an alert is issued, the public blockchain will only store the event. The data collected from wearable health monitors will be sent to a specific Electronic Health Record, EHR system for storage. Along with the transaction event being saved on the blockchain, smart contracts or hospitals will also transmit treatment commands to EHR storage. The integration of blockchain technology with electronic health records (EHR) allows for the verification of personal health information. Protecting and identifying changes to patient records in electronic health records is made easier with this. Not all nodes can execute smart contracts. Additionally, it is the responsibility of these selected nodes to validate the new block. One way to limit the exposure of data

Table 6.1: Input Patient Data for the Experimental Analysis

Patient	**A**	**Threshold**
Heartbeat	80	>100
Blood Group	A	-
Blood Pressure	130/75	150/100
Diabetic Level	320	>200
Temperature	99	>103

Table 6.2: Avg Time Compariso

Data Type	Proposed method – 'SHORTBLOCKS' protocol (with Blockchain Avg Time in Sec)	SPECTRE protocol Avg Time in Sec	GHOSTDAG protocol Avg Time in Sec	Simple – Blockchain Avg Time in Sec
Block creation	0.643	0.665	0.687	0.736
Block updating	0.476	0.492	0.517	0.537
Block sharing	0.491	0.503	0.512	0.523
Block deleting	0.679	0.702	0.728	0.754

is to limit who can view it. This includes healthcare practitioners, manufacturer of the devices, and patients themselves.

6. Result Analysis. The proposed method "SHORTBLOCKS' and the existing simple blockchain method are compared in terms of performance parameters viz. Avg. time, Latency, Processing Overhead .The input data collected form the Patient A, using wearable devices for the experimental analysis is tabulated below in Table 6.1.

As the diabetic levels are above the threshold from the above input data, alert will be raised to the patient, using the public block chain for preserving the event.

a) Avg. Time. Based on the change in treatment registration requests (Transactions count) received, Fig 6.1 shows the time-to-mine comparison of two ways on existing method of using blockchain and proposed method of blockchain with SHORTBLOCKS protocol. The results are shown in seconds. On one side, we have processing time, and on the other, we have the number of treatment registration requests, transaction count. From the graph, it is clear that both methods show a trend towards increasing treatment registration requests after the first 100 or so numbers. By lowering the waiting time in the mining queue, the proposed method with SHORTBLOCKS protocol offers higher performance as compared. The Avg. time comparison between the proposed and existing methods is tabulated in Table 6.2.

b) Latency. Figure 6.2 and Table 6.3 shows the results of an investigation on the invoke transaction execution latency for the suggested system, and the existing system, broken down by user groups: 10, 20, 30, 40, and 50 users. Increasing the average latency in relation to the number of users makes change.

c) Processing Time. The results of the simulations for evaluating the systems' performance in terms of processing overhead are shown in Figure 6.3. Many resource metrics, such as processing time, bandwidth, indirect memory, and an excess memory, may be necessary for the validation of new blocks in blockchain. The technical term for this is processing overhead. This value is discovered to be less in the suggested model when contrasted with certain current approaches. In contrast to the present models, the suggested solution outperforms them in terms of processing speed and data security. Table 6.4 depicts the statistics.

7. Conclusion. This article proposed that smart contracts built on the 'SHORTBLOCKS' blockchain be used to analyze patients' health data in real-time. Using the 'SHORTBLOCKS' protocol, the system records the data of transactions on the blocks and utilizes smart contracts to generate notifications for the healthcare provider and patient as needed. This methodology ensures that health-related notifications are sent in a secure way in compliance with safety regulations. This method provides safe and secure patient data transmission and

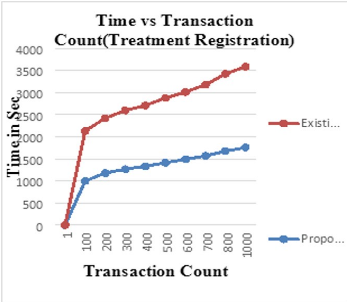

Fig. 6.1: SHORTBLOCKS avg time comparison

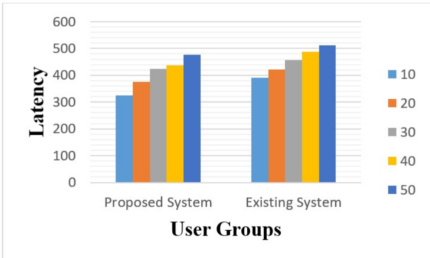

Fig. 6.2: Latency

Table 6.3: Latency Comparison

No of Patients	Proposed method – 'SHORTBLOCKS' protocol with Blockchain	SPECTRE protocol	GHOSTDAG protocol	Simple - Blockchain
10	325	345	363	390
20	375	387	403	421
30	423	438	446	456
40	436	452	467	487
50	476	489	498	512

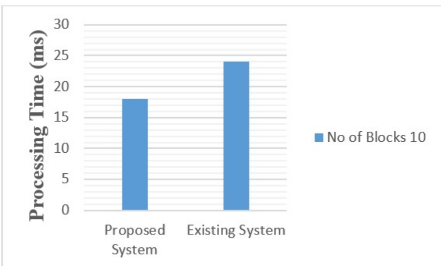

Fig. 6.3: Processing Overhead comparison

Table 6.4: Processing Overhead

Processing Time	Proposed System SHORTBLOCKS	SPECTRE protocol	GHOSTDAG protocol	Simple-Blockchain
No of Blocks (10)	18 ms	21 ms	23 ms	28 ms

communication using two blockchian viz. private and public blockchain. Due to the enormous size inflation that would result from storing complete health records on a blockchain, which would necessitate substantially more storage space at each node, we do not keep patient health information in the blockchain. Only the event raised will be facilitated in the public blokchain.

As a result, EHR (Electronic health record) gets the health data. The use of blockchain technology as a ledger and the integration of electronic health records (EHR) for the purpose of authenticating patient medical history data is only documenting the occurrence of events. Consequently, this will aid in the detection and prevention of data tampering with patient records in EHR. When energy consumption and sluggish computing are big issues, our model offers a quick, secure, and high-throughput alternative to standard blockchain-based remote patient monitoring.

Acknowledgment. The authors acknowledge the support and cooperation rendered by all the members directly and indirectly.

REFERENCES

[1] Griebel, Lena, et al. "A scoping review of cloud computing in healthcare." BMC medical informatics and decision making 15.1 (2015): 1-16.
[2] Siyal, Asad Ali, et al. "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives." Cryptography 3.1 (2019): 3.
[3] Dwivedi, Ashutosh Dhar, et al. "A decentralized privacy-preserving healthcare blockchain for IoT." Sensors 19.2 (2019): 326.
[4] Dubovitskaya, Alevtina, et al. "Secure and trustable electronic medical records sharing using blockchain." AMIA annual symposium proceedings. Vol. 2017. American Medical Informatics Association, 2017.
[5] Bhatti, Anam, et al. "Development of cost-effective tele-monitoring system for remote area patients." 2018 International Conference on Engineering and Emerging Technologies (ICEET). IEEE, 2018.
[6] Zhang, Peng, et al. "FHIRChain: applying blockchain to securely and scalably share clinical data." Computational and structural biotechnology journal 16 (2018): 267-278.
[7] Jayasuruthi, L., A. Shalini, and V. Vinoth Kumar. "Application of rough set theory in data mining market analysis using rough sets data explorer." Journal of Computational and Theoretical Nanoscience 15, no. 6-7 (2018): 2126-2130..
[8] Zhang, Jie, Nian Xue, and Xin Huang. "A secure system for pervasive social network-based healthcare." Ieee Access 4 (2016): 9239-9250.
[9] Ahmed, Syed Thouheed, Vinoth Kumar, and JungYoon Kim. "AITel: eHealth Augmented Intelligence based Telemedicine Resource Recommendation Framework for IoT devices in Smart cities." IEEE Internet of Things Journal (2023)..
[10] Nagaraj, J., & Leema, A. Light weight multi-branch network-based extraction and classification of myocardial infarction from 12 lead electrocardiogram images. The Imaging Science Journal, 71(2), 188-198 (2023).
[11] Mettler, Matthias. "Blockchain technology in healthcare: The revolution starts here." 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom). IEEE, 2016.
[12] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).
[13] Ivan, Drew. "Moving toward a blockchain-based method for the secure storage of patient records." ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. Vol. 1170. sn, 2016.
[14] Chen, Yi, et al. "Blockchain-based medical records secure storage and medical service framework." Journal of medical systems 43 (2019): 1-9.
[15] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0." Infrastructures 8, no. 2 (2023): 22.
[16] Prisco, Giulio. "The blockchain for healthcare: Gem launches gem health network with philips blockchain lab." Bitcoin Magazine 26 (2016).
[17] Wang, Shuai, et al. "Blockchain-powered parallel healthcare systems based on the ACP approach." IEEE Transactions on Computational Social Systems 5.4 (2018): 942-950.
[18] Talesh, Shauhin A. "Data breach, privacy, and cyber insurance: How insurance companies act as “compliance managers” for businesses." Law & Social Inquiry 43.2 (2018): 417-440.

[19] Budida, Durga Amarnath M., and Ram S. Mangrulkar. ”Design and implementation of smart HealthCare system using IoT.” 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). Ieee, 2017.
[20] Sivagami, S., D. Revathy, and L. Nithyabharathi. ”Smart health care system implemented using IoT.” International Journal of Contemporary Research in Computer Science and Technology 2.3 (2016): 641-646.
[21] Jiang, Shan, et al. ”Blochie: a blockchain-based platform for healthcare information exchange.” 2018 ieee international conference on smart computing (smartcomp). IEEE, 2018.
[22] Nichol, P. B. ”Blockchain applications for healthcare: Blockchain opportunities are changing healthcare globally-innovative leaders see the change.” (2016).
[23] Dhiman, Gaurav, V. Vinoth Kumar, Amandeep Kaur, and Ashutosh Sharma. ”Don: deep learning and optimization-based framework for detection of novel coronavirus disease using x-ray images.” Interdisciplinary Sciences: Computational Life Sciences 13 (2021): 260-272
[24] Cyran, Marek A. ”Blockchain as a foundation for sharing healthcare data.” Blockchain in Healthcare Today (2018).
[25] Ahram, Tareq, et al. ”Blockchain technology innovations.” 2017 IEEE technology & engineering management conference (TEMSCON). IEEE, 2017.
[26] Shubbar, Safa. Ultrasound medical imaging systems using telemedicine and blockchain for remote monitoring of responses to neoadjuvant chemotherapy in women’s breast cancer: concept and implementation. Diss. Kent State University, 2017.
[27] Prisco, Giulio. ”The blockchain for healthcare: Gem launches gem health network with philips blockchain lab.” Bitcoin Magazine 26 (2016).
[28] Haoxiang, Wang. ”Trust management of communication architectures of internet of things.” Journal of trends in Computer Science and Smart technology (TCSST) 1.02 (2019): 121-130.
[29] Shakya, Prof. ”Efficient security and privacy mechanism for block chain application.” Journal of Information Technology and Digital World 1.2 (2019): 58-67.
[30] Sivaganesan, Dr D. ”Block chain enabled internet of things.” Journal of Information Technology and Digital World 1.1 (2019): 1-8.
[31] Maithili, K., V. Vinothkumar, and P. Latha. ”Analyzing the security mechanisms to prevent unauthorized access in cloud and network security.” Journal of Computational and Theoretical Nanoscience 15, no. 6-7 (2018): 2059-2063.
[32] Li, Mengyi, Lirong Xia, and Oshani Seneviratne. ”Leveraging standards based ontological concepts in distributed ledgers: a healthcare smart contract example.” 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE, 2019.
[33] Sompolinsky, Yonatan, and Aviv Zohar. ”Phantom.” IACR Cryptology ePrint Archive, Report 2018/104 (2018).
[34] Shen, Meng, et al. ”Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach.” IEEE Network 33.5 (2019): 27-33.

Edited by: Polinpapilinho F. Katina
Special issue on: Scalable Computing in Online and Blended Learning Environments: Challenges and Solutions
Received: Jan 7, 2024
Accepted: Mar 21, 2024