Research Article

Blockchain-Enabled Smart Surveillance System with Artificial Intelligence

Paras Jain, Sunita Dwivedi, Adel R. Alharbi, R. Sureshbabu, Devesh Pratap Singh, Sajjad Shaukat Jamal, and Daniel Krah

1School of Computing Science and Engineering, VIT Bhopal University, Kothrikanal, Sehore, Madhya Pradesh-466114, India
2Department of Computer Science and Applications, Mankalanlal Chaturvedi National University of Journalism and Communication Bhopal, 462011, Madhya Pradesh, India
3College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
4Department of ECE, Kamaraj College of Engineering and Technology, Virudhunagar, India
5Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand 248002, India
6Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
7Tamale Technical University, Ghana

Correspondence should be addressed to Daniel Krah; dkrah@tatu.edu.gh

Received 16 February 2022; Revised 6 March 2022; Accepted 9 March 2022; Published 6 May 2022

Abstract

Through the use of blockchain technology, sensitive information may be securely communicated without the need to replicate it, which can assist in decreasing medical record mistakes and saving time by eliminating the need to duplicate information. Furthermore, the information is timestamped, which further enhances the security of the data even further. The deployment of blockchain technology in a range of healthcare situations may enhance the security and efficiency of payment transactions. In this way, only those who have been allowed access to patient medical information can see or modify such information. It is proposed in this study that blockchain technology be used to provide an accessible data storage and retrieval mechanism for patients and healthcare professionals in a healthcare system that is both safe and efficient. As of 1970, a variety of traditional knowledge-based approaches such as Personal Identification Recognition Number (PIRN), passwords, and other similar methods have been made available; however, many token-based approaches such as drivers’ licenses, passports, credit cards, bank accounts, ID cards, and keys have also been made available; however, they have all failed to establish a secure and reliable transaction channel. Because they are easily misplaced, stolen, or lost, they are usually unable to protect secrecy or authenticate the identity of a legitimate claimant. Aside from that, personally identifiable information such as passwords and PINs is very prone to fraud since they are easily forgotten or guessed by an impostor. Biometric identification and authentication (commonly known as biometrics) are attracting a great deal of attention these days, particularly in the realm of information security systems, due to its inherent potential and advantages over other conventional ways for identifying and authenticating. As a result of the device’s unique biological characteristics, which include features such as fingerprints, faceprints, hand geometry (including the iris), and the device’s iris, it can be used in a variety of contexts, such as consumer banking kiosks, airport security systems, international ports of entry, universities, office buildings, and forensics, to name a few. It is also used in several other contexts, including forensics and law enforcement. Consequently, every layer of the system—sensed data, computation, and processing of data, as well as the storage and administration of data—is susceptible to a broad variety of threats and weaknesses (cloud). There does not seem to be any suitable methods for dealing with the large volumes of data created by the fog computing architecture when normal data storage and security technologies are used. Because of this, the major objective of this research is to design security countermeasures against medical data mining vulnerabilities that originate from the sensing layer and data storage in the Internet of Things’ cloud database, both of which are discussed in more depth further down. A key allows for the creation of a distributed ledger database and provides an immutable security solution, transaction transparency, and the prohibition of tampering with patient information. This mechanism is particularly useful in healthcare settings, where patient information must be kept confidential. When used in a hospital environment, this method is extremely beneficial. As a result of incorporating blockchain technology into the fog paradigm, it is possible to alleviate some of the current concerns associated with latency, centralization, and scalability.
1. Introduction

[1] Amongst other things, blockchain technology is a revolutionary technology that is being used to develop creative solutions across a broad range of disciplines, including the field of healthcare. Patient data is being saved and transmitted across the healthcare sector, including hospitals, diagnostic labs, pharmacies, and physicians’ offices, via the use of a Blockchain network. With the use of blockchain technology, medical practitioners may be able to spot large-scale, potentially deadly mistakes with greater accuracy [2]. The efficiency, security, and openness of medical data exchange in the healthcare system may all be improved in this way, according to the researchers. Medical institutions may gain insight into and improve their appraisal of medical data as a result of the application of this technological advancement. It is only through the implementation of blockchain technology that clinical trial fraud can be detected and prevented. Blockchain technology also has the potential to improve data efficiency in the healthcare industry. If a one-of-a-kind data storage pattern is used in conjunction with the greatest degree of security, it is feasible that worries about data tampering in the healthcare industry may be alleviated. It increases the number of data access methods that are available, as well as the connection, accountability, and authentication of those approaches. For several reasons, it is critical to ensure the confidentiality and security of health information at all times and under all circumstances. Using blockchain technology, healthcare organizations may benefit from the decentralized data security afforded by the technology while also avoiding some of the risks connected with blockchain technology [3]. Alternatively, the study’s major goal was to design a cure for the security and intrusion vulnerabilities that had been discovered throughout its investigation. A blockchain-based Internet of Things paradigm is now being created as a result of this, to achieve the desired result. It is possible to compute and gather medical data on a patient in real-time by using a biosensor and then store this information on a distributed ledger using this method (blockchain). In their biosensor-enabled system, the researchers assert that the system is capable of recording and tamper-proofing data storage in a more accurate and time-efficient manner than other technologies that are currently available on the market. The large amount of sensitive and personal information acquired by these sensors makes them especially susceptible to data breaches and other sorts of privacy invasions. Typical smart health ecosystems, as seen in Figure 1, analyze data before storing it in cloud-based storage systems [4].

Aside from that, it offers the possibility of centrally storing and analyzing data. When dealing with time-sensitive conditions, such as a heart attack or a hypertensive crisis, there should be no slack. When immediate assistance is required, there should be no waiting. This length of time is inadequate when a physician requires quick access to data or when a rapid response and action are necessary [5]. A novel simulation-driven framework for delivering homecare services to the elderly was decided after a significant study. Because of the integration of edge and cloud models [3, 6], this technology has the potential to be used to develop unique Ambient-Assisted Living (AAL) services that may be used in a variety of healthcare settings [4]. This was made feasible by the adoption of blockchain technology, which enabled them to ensure that decentralization was carried out in a secure manner [4, 5]. Security difficulties might arise due to the reliance on data acquired from sensors (edge layer) and keep in cloud computing databases (cloud layer) [7], typical data storage and security protocols are ineffective for dealing with such a vast volume of freshly generated data.

In this study, one of the main goals is to have a better understanding of how to deal with difficulties like latency and security that arise in fog computing systems, in addition to concerns like centralization and scalability that arise in other types of computing systems. According to some, a digital signature based on the ECC algorithm may be employed as part of the hashing process on a blockchain that has received widespread public support. [8] In the case of medical data, our security technology provides an impervious solution that cannot be compromised by human interference. Anyone with the authority to request the data will be provided with an encrypted hash of the file linked with the sharing link, as well as a certificate that can only be seen by the person who initiated the request [9].

It was required to deploy a fog-enabled blockchain ledger as part of the process of recording the detected data to complete the task. On top of creating and preserving greater data security, it is believed that this performance would ease latency issues at the fog layer levels [9].

This research also adopted a decentralized and distributed ledger blockchain record management system paradigm to handle all of the system’s scalability and centralization challenges, as well as to maintain transparency and prevent intruders from tampering with patient information [10]. Authorized medical personnel, on the other hand, may be able to get access to the information stored on these blockchains, which are scattered among several fog levels. Generally speaking, the proposed blockchain technology, which makes records, was evaluated in the time it took for transactions to complete in a typical transaction, which was around one second.

To make development in this sector in the future, specialized decentralized software may be developed that will enable a facility to access and analyze health-related papers without the need for an individual’s private key. As an alternative, it will request the sender’s public key from the user, following which the program will search the system for the private key (Pvt key) that matches the public key [11]. In other words, it is possible to prevent the exploitation of medical privacy data while simultaneously shielding the data from being accessed by compromised users, simply by creating the private key from a crypto hash ciphertext generated by a trusted third party.

An identification block is identified by a cryptographic hash, which is analogous to a digital signature in certain ways. It is possible to get this outcome by hashing the block header twice.

The main contribution of this paper includes:
(i) A permission-based public blockchain system is proposed and being developed.

(ii) Using blockchain technology, we were able to address the challenges of latency, concentration, and scalability that were linked with the idea of fog.

2. Literature Review

It is a collection of resources or services that are made available over the Internet that is referred to as a cloud computing environment. Their goal was to provide cloud computing manufacturers, researchers, and consumers with a better understanding of the most susceptible cloud computing security problems, as well as the many frameworks available to solve these concerns, among other things. As reported in [12], a mechanism for distinguishing Distributed Denial of Service (DDoS) attacks has been discovered [13].

In this paper, we provide a security model for cloud computing data transmission that accurately analyses the empirical capacity of a competing authentication system for protecting data transmission. This is a good news since the results of the experiment reveal that the suggested architecture is more efficient than the frameworks now in use [12].

In their work, they described an approach based on the I-AES algorithm, as well as a private database architecture that was developed by them. This paper also offers a theoretical foundation, which is critical when considering the vast number of 5G devices that may be deployed in the Internet of Things. According to the findings of the study, the suggested algorithm beat the already utilized algorithms in terms of execution time and throughput [14].

When it comes to data security and performance, the authors of [15] tackled the issue by proposing a paradigm for trust translation, including fog node access control, and developing a service for managing changes in users and their locations. The authors of [16] investigated several artificial intelligence systems, including one that assigns distinct responsibilities to cloud and fog servers to save response time and network traffic. According to experimental data, as compared to typical procedures, this strategy results in a considerable reduction in response time [17].

The authors of [18] went into great detail on data storage, accessibility, integrity, and service quality, as well as how their suggested architecture will affect fog computing (which was also covered), the cloud framework, and mobile edge computing (also discussed).

With the use of blockchain technology, the authors of [19] were able to propose a solution to the issue of data leakage in security management. The number of nodes and power connections were increased, which increased the efficiency of data collecting. The authors presented in [20] a system that intelligently creates, receives, and saves data on...
the blockchain, hence improving security. They did this by using a blockchain-based security management paradigm. Based on blockchain technology, the authors of [21] proposed a privacy-protection strategy for surveillance cameras that may be implemented. While keeping a tight check on people who are being observed, they aim to protect the privacy of those who are being monitored by disguising their images while maintaining constant surveillance.

To make the transmission of patient health information easier for everyone concerned, the authors developed a blockchain-based sharing protocol.

According to the researchers, when the suggested protocol was assessed on the Ethereum platform, it was observed that it had very high computing efficiency, which was unexpected. Detailed information on blockchain technology’s use in healthcare was released by the authors of [22], in which they also described an implementation architecture for blockchain-based technologies inside electronic health records.

Even with IoT-related systems like ours, there will always be some level of danger associated with them. Generally speaking, the risk is the underlying likelihood that an event may occur, regardless of whether it is beneficial or detrimental. The researchers devised and executed a quality estimation technique for commercial cyber insurance that is relevant to the industry [23] when it comes to the Internet of Things cyberhazards. As an alternative to taking into account time considerations and data retrieval procedures, the authors created a model of an anticipated electronic intrusion that was in a stable condition. The emphasis of our research is on developing a technique that is efficient in terms of data recovery size and key generation management, which is in contrast to this. Our proposed method makes use of a decentralized and distributed ledger blockchain record management system architecture to mitigate any system scalability and centralization issues that may arise in the future. In contrast, authorized medical workers may be granted access to the information held in these blockchains, which are dispersed among a variety of different fog layers.

Also, to meet the high accuracy requirements of real-time decision making, geographically scattered edge devices collect data at the place of collection and distribute it across service providers from a variety of domains. However, traditional security and management systems have a centralized design, which may be seen as a negative in certain situations.

A single point of failure may result in a performance bottleneck and render the system useless, as shown in the diagram below. Using a decentralized system architecture such as this one, system performance may be improved while single point of failure issues can be reduced, which is beneficial in a system architecture that uses a centralized control system. Furthermore, via the use of consensus processes and publicly available distributed ledgers, Blockchain transactions are recorded in a chained data structure that is verifiable, traceable, and append-only, as opposed to traditional databases. Implementing Blockchain technology into the SPS framework, on the other hand, not only helps to build confidence between members but also helps to improve the overall efficiency of the system. Furthermore, it assures the availability, correctness, and auditability of data for participants, as well as the immutability and auditability of the data itself. In addition to provenance, a Blockchain-Enabled Decentralized Smart Public Safety (BlendSPS) system that is both decentralized and smart has been proposed in this study, and it is capable of enabling decentralized, efficient, and secure information exchange and services. Operations in SPS situations are also described in this study, which is a first in the field. The BlendSPS decouples functionality into several containerized functions, allowing for fine-granularity and lose coupling. It does this by using the advanced capabilities of the architecture microservices. This kind of computationally efficient microservice may be installed and executed on the cloud. IoT devices that are resource-constrained and have little overhead are preferred. Hybrid blockchain fabrics are those that are designed to be both secure and scalable at the same time. A fundamental security architecture makes it feasible to have both immutability and decentralization. Because of the trustless nature of the Internet of Things network environment, suitability and traceability for data exchange are required.

3. Proposed Methodology

Figure 2 displays a possible medical data security solution that might be implemented at the fog layer of a cloud computing paradigm based on the Internet of Things and which makes use of public permission blockchain technology and an electronic digital signature as a security solution. This is accomplished via the use of the SHA-256 secure hashing technique in conjunction with the elliptical curve cryptography digital signature to create the certificate hash. A key component of bitcoin security is extensively used to safeguard messaging apps as well as other types of online transactions, including e-commerce. The introduction of blockchain technology was necessitated by flaws in conventional WSN-IoT security countermeasures, resulting in increased computational complexity, memory difficulties, processor power consumption, latency, and vulnerability to social attacks, among other challenges. The adoption of a hash algorithm in the blockchain was suggested by the idea to guarantee security, immutability, and transparency among chain participants, among other benefits. When compared to RSA, which uses a key size of 256 bits (which is similar to the 2048 and 3072 bits used in RSA), this elliptic curve cryptography hashing is 10,000 times quicker, more efficient, and safer than RSA, according to the researchers. In particular, the fall effect outperforms random number generation in terms of efficiency when it comes to hashing.

Instead of using an interprocess communication (IPC) mechanism to communicate between service units as in a monolithic architecture, microservices units are geographically dispersed across the network and communicate with one another through a remote procedure call (RPC) mechanism, such as the HTTP RESTful API, to avoid duplication of effort.

Because such fine-grained microservices units are independent of each other’s growing technologies, microservice
architecture can provide loose coupling and flexibility. Because of this, developers may work on their projects continuously, while deployment is quick and maintenance is straightforward.

As a result of its advanced characteristics, such as scalability, reusability, extensibility, and ease of maintenance, the microservice architecture has been adopted by much smart application development. To provide effective and safe video surveillance services at the edge network, which comprises large numbers of distributed Internet of Things devices, a robust smart surveillance system that blends microservices architecture with blockchain technology has been developed and demonstrated.

It has been shown via experimental findings that the prototype design [14] is a security architecture that is lightweight and decentralized, and it is used on the Internet of Things-based data marketing systems.

In a blockchain record that is fog-enabled, the observed data is recorded, with a copy of the record being communicated to the cloud across numerous fogs. Data security (immutability) and latency reduction will be enhanced through the use of decentralized records at the fog level levels, as a result of this paradigm.

The usage of a crypto hash-based blockchain and a private key that has been established and distributed throughout the fog layers, on the other hand, may allow doctors to get access to encrypted distributed ledger data. A copy of this transaction is securely kept and readily accessed on the cloud layer, where it will be available for long-term retention and retrieval. Figure 3 also depicts the overall flow process, the internal process transaction for the proposed paradigm, and the overall flow process.

Figure 4 depicts several potential dangers that might arise during routine operations in an SPS. The participants are separated into four groups: those who operate the camera, those who operate the edge device, those who operate the fog server, and those who operate the human user. Using real-time video feeds generated by the camera, the camera delivers them to edge devices that are either on-site or nearby. When raw frames are received, the edge devices decode them and extract lower-level characteristics from them, which are then sent to a more powerful fog layer for
aggregation and processing. Depending on the powers that have been granted to him or her, the user has the option to query surveillance visualization services for information that protects his or her privacy.

Attacks using False Frame Injection are the first kind of danger to be handled by security professionals. To conduct operations such as feature extraction and decision-making based on data collected by cameras, the authenticity of raw video feeds from cameras is essential. An opponent initiating visual layer attacks against the infrastructure, on the other hand, might constitute a threat to the infrastructure’s safety and security. When an attacker employs a false frame injection, he or she may cause erroneous features to be generated at the network edge by sending fraudulent frames to it. While the decision-making process is underway, the attacker can swap out original frames with duplicate frames to reduce system detection accuracy and so compromise the system’s security.

3.1. Basic Layer-Based Input Layer. In addition to being a distinguishing characteristic that enables it to be used in public-permission blockchain application, it also has another distinguishing characteristic. Additionally, it has the following features in addition to being deterministic: quick calculation, resistance to preimages, collision resistance, and avalanche effects are some of the characteristics of this algorithm (gives the same answers every time you parse an input through a hash function). Figure 4 represents the peer to peer architecture of proposed work.

It was also distributed across the network of decentralized records using public-permissioned blockchain technology, with nodes being able to monitor each other and any unauthorized administrators being denied access to the information. As seen in Figure 4 is each node architecture.

3.2. Secured Stage of Proposed Work. It was important to perform transactions in a cluster to properly configure this distributed sensor node. For purposes of security, the records (block) are hashed. Another way of putting it is to say that the transaction method in this model is made up of the body parameters that were obtained. The previous transaction, which used SHA-256 to generate a public and private key pair, serves as the basis for the initialization of this hashing operation.

Figures 5 and 6 depicts the flowchart of this proposed methodology.

To save data to the distributed ledger, the security microservices make use of a set of transaction commit RPC calls. As a result, in addition to the usual service operation, the execution of the consensus protocol and the recording of data into the distributed ledger would always cause additional delays.
4. Discussion and Conclusion

One of the goals of this study is to understand how to deal with concerns like latency and security, as well as centralization and scalability that arise in fog computing systems. According to some, using an ECC digital signature as part of the hashing technique on a blockchain that has received widespread public support is possible. In the case of medical data, our security system provides an impenetrable solution that cannot be breached by human interference. Meanwhile, anybody who can request the files will be presented with an encrypted hash of the file connected with the sharing link, as well as a certificate that can only be seen by the individual who made the original request.

In addition to developing and maintaining high levels of data security, this performance will solve latency difficulties in the fog layer.

Moreover, to solve the challenges of scalability and centralization, a decentralized and distributed ledger blockchain system paradigm was used in this study. All of this was carried out to increase openness, secure patient information from attackers, and maintain the integrity of the whole system. Authorized medical workers can view several blockchains that have been dispersed across a range of fog layers. On a broad level, the proposed blockchain technology was assessed based on the amount of time it took for transactions to complete in a typical transaction.

The creation of specialized decentralized software that allows a facility to read and review health-related documents without the requirement for a private key might be a component of future progress in this field. Because of this, it is feasible to prevent the exploitation of patient medical privacy data and the data itself from being accessed by a compromised user by building the private key from a crypto hash ciphertext.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors of this manuscript declared that they do not have any conflict of interest.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through the research group program under grant number R. G. P. 1/85/42.

References


