International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Sep-2023)

http://dx.doi.org/10.12785/ijcds/140164

Blockchain for Decentralized Emergency Management System

Ammar Ibrahim El Sayed[1], Mahmoud Abdelaziz[1] and Mohamed Hassan Abdel Azeem[2]

[1]*Avionics Department, Military Technical College, Cairo, Egypt*
[2]*Electronics and Communications Department,Arab Academy for Science, Technology and Maritime Transport,Cairo, Egypt*

Received 27 Nov. 2022, Revised 31 Jul. 2023, Accepted 10 Aug. 2023, Published 01 Sep. 2023

Abstract: Currently, blockchain technology plays a vital role in providing security and trust management in numerous applications such as cryptocurrency. Data monitoring and management in real-time applications require high flexibility and accuracy. Obtaining the necessary information in a timely manner during emergency situations is crucial, as the failure to do so could have fatal consequences. The Intelligent Ambulance Vehicle (IAV) allows the emergency crew to report the patient status through an IoT network, including mobile networks and medical diagnosis equipment. An intelligent ambulance functions as an autonomous network that necessitates high-speed data processing with minimal computations. Implementing trust management through the Client Server Model introduces additional delays to the network. This paper proposes the integration of Internet of Things (IoT), vehicle-to-vehicle (V2V) communication, and Electronic Healthcare (EH) systems to develop an efficient emergency handling system. A software implementation of a decentralized emergency management (DEM) application based on blockchain process provides trust, availability, and transparency.

Keywords: EHR, V2V, IoT, Blockchain, Thrust

1. Introduction

The application of blockchain technology has permeated numerous fields, including the Internet of Things (IoT). Blockchain offers a secure database that does not require third-party consent. Blockchain is a timestamped sequence of data records. Instead of relying on core nodes (servers), blockchain utilizes a Peer-to-Peer (P2P) network model to manage these records. Each group of records is consolidated to form a block. The chain represents the cryptographic concept that links and protects these blocks. Through a distributed P2P scheme, blockchain verifies each transaction on the network. By integrating blockchain technology into the middleware layer, trust, availability, and confidentiality are guaranteed. This combination ensures a high level of security for data sharing and storage across the network [1].

IoT networks comprise intelligent network elements, including sensors, devices, cars, and traffic lights. These networks utilize various sensors to collect essential data. The data collected plays a crucial role in aiding control units in making informed decisions. IoT networks can be classified into three types: centralized, collaborative, or distributed. In emergency situations, IoT networks enable the emergency crew to obtain a comprehensive report on the accident and the patient's condition [2]. The Intelligent Ambulance Vehicle (IAV) is an autonomous vehicle (AV) that leverages Vehicle-to-Vehicle (V2V) communication protocols to make informed decisions and improve safety. V2V and Vehicle-to-Infrastructure (V2I) technologies have a significant impact on traffic safety and congestion avoidance.

Incorporating V2V into the Electronic Healthcare system (EH) enhances the system's efficiency [3]. The EH system consists of two main components: Electronic Medical Records (EMRs) and Electronic Healthcare Records (EHRs). EMRs are a digital version of a patient's paper chart, while EHRs are a more comprehensive record of a patient's health information that includes information from multiple sources, such as doctors, hospitals, and pharmacies. Each patient in the EH system has both an EMR and an EHR. The EMR represents the continuous real-time monitoring of on-body sensor data, which can be accessed by authorized healthcare providers to improve patient care. The EHR, however, allows for remote access to patient medical records. The EH system empowers both patients and healthcare professionals with the ability to monitor and access medical records. This, in turn, improves the efficiency of healthcare services [4].

This paper proposes the integration of IoT, V2V, and EH systems to develop an efficient emergency management system. The proposed system effectively informs the IAV about the accident location and identifies the nearest hospitals capable of handling the emergency situation. Subsequently, the IAV dispatches emergency requests to the closest hospitals. To ensure proper authorization, a legally binding agreement between patients and hospitals is required. This

E-mail address: ammaribrahim177@gmail.com ,mkaremm@mtc.edu.eg, mhabdazeem@aast.edu

agreement utilizes blockchain technology to approve access to the patients' EHRs. By using a hash function on the patient's data, the proposed model concentrates on creating a distinct ID for each patient. The combination of a hash table and blockchain enables the secure access, sharing, and storage of data within the emergency management system. The model's performance is contingent on factors such as encryption and decryption time, hash table operations (storage and retrieval), and the execution of the hash function. The proposed software implementation of the emergency management system, based on blockchain, provides trust, availability, and transparency. This proposed application represents a DEM solution.

A. Contributions

- An individual ID is created for each patient using an anti-collision hash method that is protected against birthday attacks.
- An integration of EH, IoT, and V2V via blockchain, introduces new techniques in handling, storing, and protecting data in a decentralized environment.
- The hash table maps each key to the corresponding encrypted patient's record, after granting the proper access permissions
- Implementing DEM applications based on Blockchain.

B. Outline

This article is organized as follows. Section 1 background discussion. Section 3 describes the system model. Section 4 discusses the deployment and output of the software. Section 5 introduces the complexity calculation and limitation. Finally, Section 6 concludes the article.

2. Background

This section presents a background of IoT, V2V, EH, and blockchain, in addition to employing blockchain in enhancing emergency management system performance.

A. IoT Network

1) Definition

The Internet can be defined as an intelligent network connecting different nodes. These nodes could be computers, sensors, or other peripherals. The internet is built mainly on TCP/IP model. Sensors, RFID, and smart devices play a crucial role in forming the foundation of IoT networks. The IoT network is a diverse network in which different devices communicate to realize a certain purpose or serve a specific application. IoT technology empowers modern applications via the Internet connectivity to acquire the following benefits [5] Patient registration:

- Control of equipment through sensors, actuators, RFID, and intelligent devices, such as smartphones.
- Instant monitoring and detection of any deviations in the vicinity of the connected nodes.

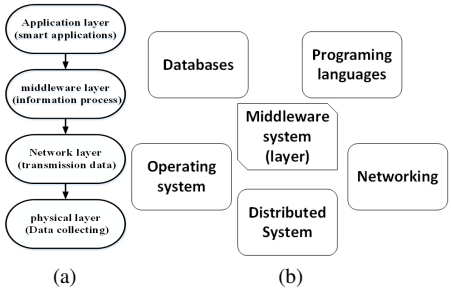


Figure 1. (a) Network layer (b)Middleware system layer

- Immediate reporting of the location of smart devices within the network.

2) The network architecture of IoT

The IoT network has a layered architecture assembled of four layers. It starts with sensors that collects data and end with an application on the central control unit [6]. These four layers as shown in Fig. 1 are:

- Physical layer (Sensor): An edge layer in the network made up of sensors that collects and transmit data across the network. This data is processed into a meaningful information.
- Network layer (Gateway): This layer involves several types of connectivity techniques, including (WANs), Mobile Communication Networks, or (LANs) with Wi-Fi, Bluetooth, ZigBee, LORA, and Ethernet connectivity.
- Middleware layer: this layer offers a full management and control over offered services and acts like a valve between the hardware (e.g., sensor, sink, high level application terminal) and the application.
- Application layer: This layer uses the processed information to supply operators with the anticipated services to support their applications. (e.g., industrial automation, healthcare, education, transportation, logistics, surveillance, and people tracking.)

Our proposed model is implemented on middleware layer and application layer of the above architecture.

3) IoT Network Topology

The IoT network topology can be categorized into three main models, each facing its own set of challenges in terms of safety and resource limitations [7]. (1) Centralized model: In this model, all the devices are connected to a central point (server). (2) Collaborative model: This model involves multiple processing and storage resources. (3) Distributed model: All IoT devices in this architecture have access to the same processing and storage resources. This model helps avoid the single point of failure scenario and offers advantages such as improved bandwidth efficiency and reduced latency.

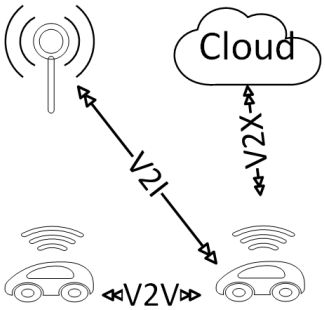


Figure 2. V2V network topology

B. V2V Network

1) Definition

The V2V network refers to a network where vehicles and system infrastructure components (such as mobile base stations) exchange data simultaneously. This data exchange includes information such as emergency alerts and traffic status updates. V2V networks play a significant role in improving traffic control efficiency and reducing traffic congestion and accidents. Vehicular ad hoc networks (VANETs) are commonly utilized in various applications, including safety measures and traffic law enforcement [8].

2) V2V Network Protocol

The standard (IEEE 802.11p) is designed for V2V connectivity. It is an extension of the standard IEEE 802.11, popularly known as Wi-Fi. The IEEE 802.11p Group was established in 2004 to develop protocols specifically for vehicular environments. The Wireless Access in Vehicular Environments (WAVE) and Dedicated Short-Range Communications (DSRC) are built upon this standard protocol. Notably, the IEEE 802.11p standard offers low latency and high availability. These features make it the preferred choice for establishing communication between moving vehicles [9].

3) V2V network topology

Wireless data transmission plays a crucial role in V2V communications. The topology commonly used in V2V networks can be either a fully connected or partially connected mesh network, as shown in Fig. 2. In a fully connected network, all nodes are directly connected to each other through dedicated paths. This topology enhances the overall network structure and ensures operability at all times. On the other hand, in partially connected networks, only some nodes are connected to each other through dedicated paths [10]. The V2I interfaces vehicles on the move to the road management system. The interfacing is facilitated by several modules, including RFID readers, traffic lights, cameras, and more. In Intelligent Transportation Systems (ITS), sensors gather infrastructural data and provide real-time guidance to travelers. This exchange of information occurs through an ad-hoc network between vehicles and the ITS [11].

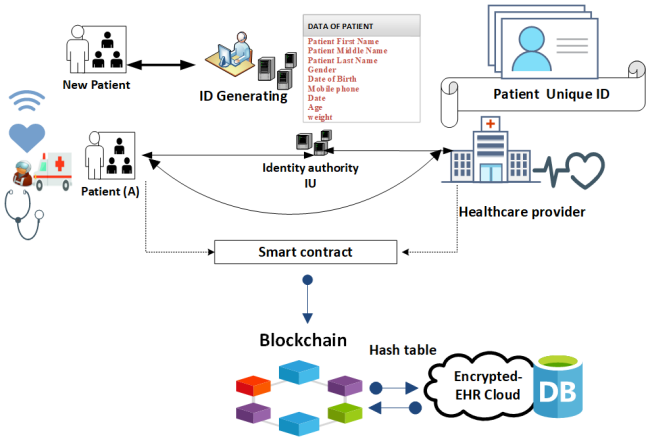


Figure 3. EH system with Blockchain architecture

V2X aims to enable communication between vehicles and various surrounding entities, including pedestrians, other vehicles, application servers, and Road Side Units. The Pedestrian Collision Warning system has been developed to alert pedestrians to imminent danger, highlighting one of the main purposes of V2X, which is to minimize fatal accidents [12].

C. EH System

1) Definition

The EH system aims to enhance the quality of healthcare services. While EMR permits real-time monitoring of on-body sensors, EHR enables remote access to patient records. The EH model consists of four major components: patients, EH providers, identity authority (IA), and storage. Beginning with a registration request and ending with the retrieval of patient data, the EH system follows a set order [13].

2) EH system architecture

The proposed EH system architecture is presented in Fig. 3:

- Patient: This node is responsible for requesting the IU using a unique ID and for the encryption and decryption of the patient's data.
- Healthcare Providers: Each healthcare provider is identified by a unique ID. They perform three main tasks: authentication requests to access the system, requests for access to specific patient data, and the decryption and reencryption of retrieved data before sending it to storage
- Identity Authority: The IA establishes trust between the different parts of the EH system by applying an authentication process.
- Healthcare storage: The Cloud serves as the backbone of the EH system, where data is stored and organized by the data center [14].

D. Blockchain Tecnology

1) Definition

Blockchain is a timestamped sequence of immutable data. It is managed by a cluster of computers instead of a single server, forming a P2P network. Each piece of data is stored in a block, and these blocks are connected through a cryptographic principle known as a chain [15].

2) Network architecture

Centralised and decentralised models are the two main categories. In a centralised network, trust is established through a third party and is based on a single authority. Blockchain technology's basic idea is to do away with the necessity for a third-party intermediary, changing the network model from centralised (client-server) to decentralised P2P. A blockchain system consists of four essential parts. A blockchain network's nodes are connected to one another and constantly update and store their most recent ledgers. These nodes make the network more functional. Second, transactions are used to distribute data around the system. On the blockchain network, these transactions go through hashing, grouping, and publication procedures. The consensus mechanism, which acts as a fault-tolerant mechanism within the blockchain network, is the third element. It enables nodes to unanimously consent to a single transaction, ensuring network consensus. In the end, mining is an end-to-end procedure in charge of ensuring the security of blockchain transactions. In addition to validating transactions, miners also contribute fresh blocks of data to the blockchain's current global public ledger. By putting these components in place, blockchain networks create decentralised trust and make it possible for secure, transparent transactions to take place without the need for middlemen or centralised control. This paradigm shift in network architecture creates new opportunities for innovation and cross-industry collaboration.

3) Blockchain security

Blockchain reduces the necessity for dedicated controls and minimizes extra costs. Trust is established between blockchain nodes. Transactions are signed using the owner's keys (private/public). Once these transactions are verified, the blockchain data cannot be altered. Blockchain ensures data security through cryptography. The cryptographic core of the blockchain is the hash function. Hash is a process in which an algorithm (hash function) detects data inputs of any size and returns a fixed-length output (digest). However, if the input is altered, the output will change [16]. The blockchain uses this hash to identify the block data. The new block contains the hash of the previous block, resulting in a sequence of connected blocks. These obtained hashes are block-specific and hence ensure security and reliability. The Proof of Work (PoW) algorithm is one of the consensus algorithms used for validating transactions as well as generating a new block in the chain. The PoW of bitcoin uses the (SHA-256) hash function. Blockchain utilizes asymmetric cryptography (i.e., public-key), which allows users to generate digital signatures used in sending and receiving transactions [17].

4) Blockchain in IoT, V2V, and EH

The benefits of blockchain technology are extensive and cut across numerous domains. Its capacity to enable secure data processing and delivery, offering a strong method for ensuring data integrity and confidentiality, is one important advantage. Blockchain raises transaction security and trust by removing the need for a central authority. Additionally, the flexibility of blockchain's applications allows it to be used in a variety of industries, including trust management, cryptocurrencies, and smart contracts. Innovation and teamwork are encouraged by its decentralised and open structure. In the healthcare sector, blockchain holds great potential. It enables efficient management and maintenance of medical data, ensuring the accuracy of health information. Healthcare providers can securely access and share data, facilitating improved collaboration and patient care. Moreover, blockchain technology enhances data integrity by preventing single points of failure scenarios. Its distributed ledger system ensures the reliability and trustworthiness of health-related information. Overall, blockchain technology revolutionizes data management, offering secure and transparent solutions. Its impact spans across industries, empowering businesses and organizations with enhanced security, flexibility, and the potential for transformative applications. In healthcare, blockchain holds promise for efficient data management, secure information exchange, and improved healthcare outcomes [18], [19].

3. System model

In blockchain development, it is essential to understand how the main blocks of blockchain (e.g., transactions, consensus algorithms, ledger, trust, and smart contracts) collaborate in a decentralized environment.

A. Model overview

Emergency networks are composed of sensors and devices with divergent resources and capabilities. Some devices have more computational power and memory than others. Utilizing the available resources efficiently helps conserve the energy of less capable nodes. The proposed model recognizes the heterogeneous nature of emergency networks regarding operation and distribution.

The offered trust paradigm is decentralized. This decentralized model is a private permission blockchain utilized in an emergency network. Permissioned blockchain allows different nodes on the network to carry out different tasks and responsibilities.

Transactions are verified before being appended to the blockchain ledger. The verification process is accomplished via several peer nodes on the network. The terms participants and clients are used interchangeably to denote the system vehicles, sensors, and devices.

The proposed model aims to integrate blockchain networks, IoT, V2V, and EH systems to build an emergency

management system. The IAV is notified of the accident location and the closest hospitals ready to handle the case. The IAV sends out these emergency requests to the nearest hospitals. A software implementation utilizing blockchain as an emergency management solution offers trust, availability, and transparency.

1) Identity Management

Joining a blockchain network requires obtaining a unique ID. This ID enables the node (i.e., patient, healthcare provider) to proceed to the registration stage (certificate of registration). Upon successfully completing registration, nodes are approved to join the network.

2) Transaction Integrity

The blockchain database is a shared replicated ledger. The hash connecting the blocks acts as a countermeasure against data alteration and provides the benefit of tracing data back to the genesis block (first block).

3) Data Sensitivity

The clearance required to obtain certain information in an emergency network is crucial. Some information, such as traffic conditions, is made public, while other information, such as patient data, should be kept confidential.

B. Model Concept

1) Blockchain Concept

Blockchain is a distributed database where transactions are verified by nodes without the need for a central authority. This decentralized approach enables the detection of any attacks by maintaining the network's integrity. The blockchain ledger provides equal access rights to all network users. One of the key features of blockchain technology is the decentralization of consensus. Nodes can interact and reach consensus without relying on a central authority. This decentralized consensus mechanism ensures the authenticity and order of transactions in the network.

2) Unpredictability Concept

Unpredictability depends on the randomness of the encryption algorithm used. Instead of relying on a single encryption algorithm, multiple inputs and multiple encryption algorithms are used simultaneously. The hash function utilized in the system is designed to incorporate the concept of unpredictability. The hash elements consist of a one-round AES-256 algorithm, a multiplexer, XOR operation, and the RC4 algorithm.

3) Collision Resistant Concept

Collision Resistance: A hash function h, defined as $h : 0, 1^* \rightarrow \mathrm{m} \in 0, 1$, is considered collision resistant when it becomes arduous to find two distinct messages M_1 and M_2 from the set $0, 1^*$ that result in the same hash value, $H(M_1) = H(M_2)$. In other words, a hash function demonstrates collision resistance when it becomes computationally impracticable to discover two different inputs x_1 and x_2 that produce identical hash outputs, $h(x_1) = h(x_2)$. Collision Attack: An attack that aims to discover two equal hash outputs, which are the digests of two different inputs, i.e., $H_x(M_x \text{ pad } Y_x) = H_n(M_n padY_n)$, where M is the input data to the hash function and pad is the padding appended to message M before hashing. The birthday attack is based on the birthday paradox and states that the probability of a collision for a 256-bit hash function is 0.5 when the number of generated hashes exceeds 5×10^{38}.

4. Software Application and Performance Analysis

This section discusses the implementation of the basic functionality of the blockchain network. It begins with the creation of a block containing mutable data. The mining operation follows, during which the emergency system nodes validate the transactions before they are added to the chain. The Blockchain node join & block creation is illustrated in Figure 4. The published data of the blockchain nodes can be seen in Figure 5. The application frontend is displayed in Figure 6. The blockchain application ledger (chain) is depicted in Figure 7.

A. Operating system software tools

1) Operating system

The specifications of the workstation used is Dell Inspiron Laptop 15.6" with VMware Ubuntu16.04 operating system, Intel Cor $i7-5500U$ CPU@2.40 GHz CPU, and 8 GB RAM.

2) Software Tools

The blockchain network deployment is implemented using Python programming, running on local ports "8000", "8001", and "8002" as nodes. The frontend (Flask) is hosted on local port "5000". A Ubuntu 16.04 virtual machine, powered by VMware version 15, is used for this purpose. This private blockchain network utilizes the fundamentals of Python programming to achieve its functionality. Transactions, index, hash, previous hash, timestamp, and Nonce are the primary elements of a block. The term "Chain" refers to these linked blocks.

B. Healthcare Provider Access and Store Patient Data

The algorithm outlined below (Algorithm 1) describes the process for healthcare providers to access and store patient data using blockchain technology. The steps involve requesting access to the patient's EHR, executing blockchain transactions to obtain the necessary keys, obtaining patient consent, encrypting and sharing keys on the blockchain, accessing and modifying the EHR data, and securely storing the EHR in the cloud. Notifications are sent to both the patient and the healthcare provider throughout the process to ensure transparency and accountability. This algorithm provides a structured approach to facilitate secure and efficient access and storage of patient data in healthcare systems. The complete process for the healthcare provider (HP) to access and store the electronic health record (EHR) is shown in Figure 8. It demonstrates the orderly procedure that HP must adhere to in order to guarantee the secure and effective processing of patient data. A detailed description

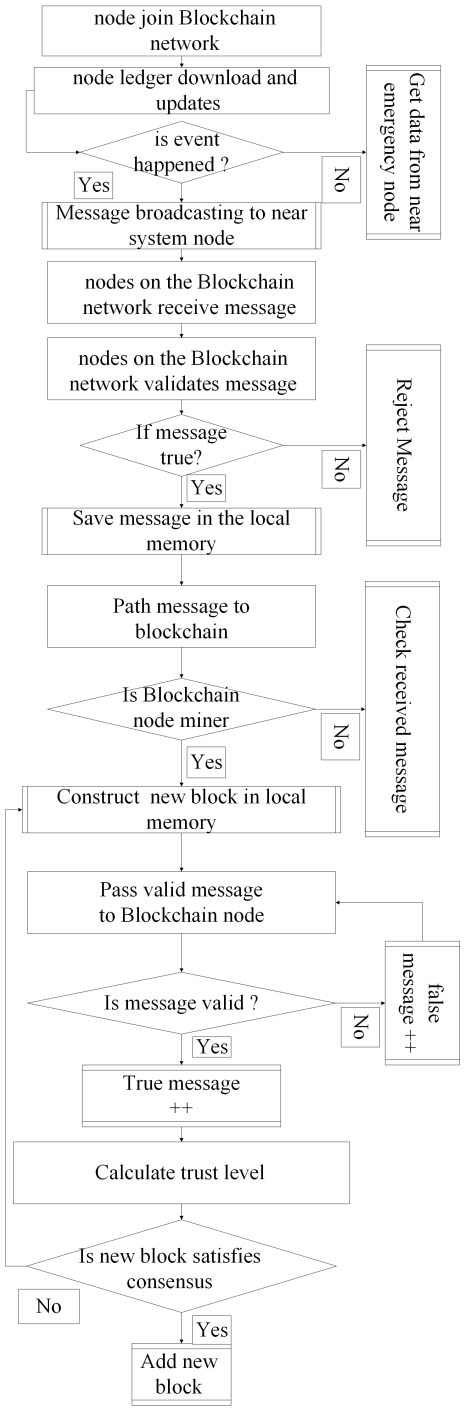


Figure 4. Blockchain node join & block creation

1: **Step 1: Request**
2: Healthcare provider requests access to patient's EHR through client service;
3: **Step 2: Blockchain transaction**
4: Request sent as a blockchain transaction to network node to obtain patient key value;
5: Once the transaction is executed, the peer node sends a notification to another client;
6: **Step 3: Notification**
7: Patient grants consent for provider to access EHR;
8: **Step 4: Display notification**
9: Client service retrieves public key of requesting healthcare provider from network and uses it to encrypt patient key;
10: **Step 5: Provide P_K**
11: Encrypted patient key is shared as a transaction to the blockchain network and committed onto the ledger, updating consent list;
12: **Step 6: Retrieve HP public**
13: Smart contract executed, creating a new asset on the blockchain ledger containing encrypted patient key and adding reference to healthcare provider identity on patient consent list;
14: **Step 7: Encrypt P_K with HP public**
15: PAfter the encrypted patient key is committed to the ledger and the consent list is updated, the peer node initiates the Share Key event;
16: **Step 8: Blockchain transaction**
17: The client of a healthcare provider receives a notification indicating that the patient has shared their key, granting access to their EHR;
18: **Step 9: Share P_K and give consent**
19: Hash function is used to hash EHR data and generate a digest;
20: A digest is used as a key in the hash table to create an index, directing to a bucket where the EHR is encrypted with the PK and stored in the cloud.
21: **Step 10: Find index by hash table**
22: Healthcare provider views/alters patient's EHR;
23: **Step 11: Get EHR**
24: Healthcare provider stores EHR in the cloud;
25: **Step 12: Notification**
26: Peer node triggers Storage event after EHR is stored in the cloud;
27: **Step 13: Display notification**
28: Patient and healthcare provider receive notification that EHR has been successfully stored in the cloud.

Algorithm 1: Algorithm for Health Care Provider Access and Storage of Patient Data

of the algorithm given in Algorithm 1 can be found in the steps shown in the picture.

C. Blockchain Emergency Application

1) Blockchain Data storage

The blockchain emergency network stores transactions as JSON files. The block number, timestamp, and name of the emergency system unit are all included in each transaction's information concerning the emergency system. Multiple transactions are grouped together in a block. The created blocks are then published on the network. In blockchain networks, each block is identified by a unique hash, which represents its content.

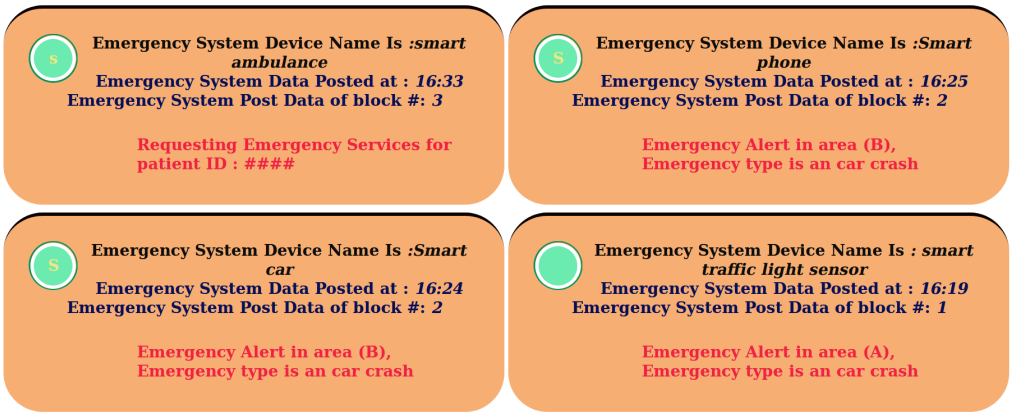


Figure 5. Node publication on system

Figure 6. Application frontend

2) Hash Calculation

The cryptographic hash ensures the integrity of the block data. A hash function is applied to the payload data, generating a digest. This digest serves as the first step in verifying any alterations made to the block data. The hash function is known for its simplicity, determinism, and random nature. While these features make the hash function irreversible, the output of the hash remains the same as long as the data remains unchanged.

3) Chain the block of emergency transactions

In the DEM, the blocks are stored in a Python list. Initially, the genesis block is manually created, and each subsequent block includes the hash of the previous block. If any alteration is made to the block data, the previous hash stored in the following block will be modified. This modification would impact the entire chain, potentially breaking it. Breaking the chain would require recalculating the hashes for the entire chain. Additionally, an attacker would need to convince as many network nodes as possible to approve the modification. This scenario is highly unlikely to occur and extremely complicated to achieve. The likelihood of successfully executing this scenario decreases as the number of network nodes increases.

4) PoW Algorithm

The concept of PoW involves the intricate calculation of the hash function to prevent potential attacks. To ensure security, a specific condition is imposed on the computational process, known as the difficulty level. A commonly used condition is ”n leading zeroes,” where n represents a positive integer. Within the block, there is a data element called the nonce, which serves as a placeholder and undergoes continuous alteration. The nonce keeps changing until a hash is found that meets the required condition. The complexity of the PoW algorithm depends on the number of zeroes specified in the condition. Once a suitable nonce is discovered, the computational process concludes.

5) Block Adding to Chain

The PoW algorithm must be utilized by each node to ensure the integrity of the data and prevent alterations. The processed data is stored as a sequence of unverified transactions. The block is not mined until the nonce is calculated with the PoW constraints. The implementation of the emergency system begins with (1) the emergency system unit joining the blockchain network, such as smart ambulances, EH systems, and smart cars; (2) downloading the blockchain ledger; and (3) linking the new block to the chain.

D. Trust consensus and decentralization

Up until this point, the blockchain has been running on a single device. However, even with the blocks connected by hashes and the application of the proof-of-work restriction, trust cannot be ensured with just a single entity or machine. Trust requires data distribution and the involvement of multiple nodes to manage the blockchain. The presence of multiple ledger copies on different nodes is illustrated in Fig. 9. To transition from a single-node scenario to a P2P network model, a mechanism is implemented to allow a new node to become aware of other network peers. The registry can invoke the presence of a new node in the network, enabling existing nodes to be aware of the addition of a new node through the ”/register” endpoint. It will support the system with the following:

{"length": 4, "peers": [], "chain": [{"nonce": 0, "index": 0, "hash": "6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9", "transactions": [], "timestamp": 0, "previous_hash": "0"}, {"nonce": 883, "index": 1, "hash": "005aa97a63d9d8d7bc6259757a58853ce4e6f8317d13ae6d132321fd8f00bb80", "transactions": [{"content": "Emergency Alert in area (A), Emergency type is an car crash \r\n", "timestamp": 1602026364.659397, "author": " smart traffic light sensor "}], "timestamp": 1602026372.176669, "previous_hash": "6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9"}, {"nonce": 62, "index": 2, "hash": "001dc2d5786bf860489813c23873f93da269266c6e5b5818c6de9c2be0e1ddc7", "transactions": [{"content": "Emergency Alert in area (B), Emergency type is an car crash\r\n", "timestamp": 1602026688.454297, "author": "Smart car "}, {"content": "Emergency Alert in area (B), Emergency type is an car crash\r\n", "timestamp": 1602026735.074364, "author": "Smart phone"}], "timestamp": 1602026740.151255, "previous_hash": "005aa97a63d9d8d7bc6259757a58853ce4e6f8317d13ae6d132321fd8f00bb80"}, {"nonce": 193, "index": 3, "hash": "00d86ecd37d031847ff16e0fa8b89ddcefb7f52563f6a2a99b3de84daeb291b3", "transactions": [{"content": "Requesting Emergency Services for patient ID : ####", "timestamp": 1602027239.757415, "author": "smart ambulance"}], "timestamp": 1602027245.328451, "previous_hash": "001dc2d5786bf860489813c23873f93da269266c6e5b5818c6de9c2be0e1ddc7"}]}

Figure 7. Network nodes application chain

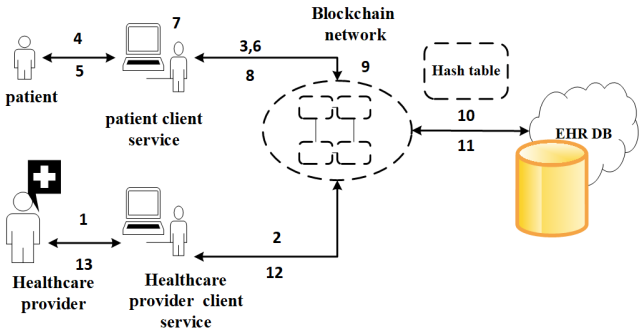


Figure 8. Healthcare Provider Access and Store Patient Data

- Inform the existing nodes to add a new peer to its list of connected peers.
- The new node obtains the exact copy of the existing network ledger.
- Resynchronization occurs on the network if any node goes off the grid.

However, a concern must be taken into account in a multiple node topology. The replication of chains across different nodes may vary due to deliberate exploitation or accidental reasons, such as network latency. In order to maintain data integrity, the nodes need to reach a consensus when faced with chain variations. In other words, consensus must be achieved among the network nodes. When the chains of multiple participating network nodes start to diverge, a simple consensus algorithm is enforced to converge on the longest valid chain. This choice is justified by the assumption that the longest chain represents the most completed work.

Once a new block is successfully mined, the responsible node should report this event to the entire network. The newly mined block is then verified by the rest of the network peers. Once the mining operation outcome is validated by the network peers, they update their ledgers accordingly. The verification process becomes easier since the nonce is known, eliminating the need for additional computational overhead.

E. Performance Analysis

The emergency system involves a subprocess that assists in ensuring data sharing security and flexibility, particularly in terms of reading from and writing to the cloud. The performance of the system is measured by the efficiency of data communication between the various system nodes, including patients, EH providers, smart ambulances, and IoT devices. The performance assessment encompasses two phases: data retrieval and storing.

Obtaining the required authorizations to access and decode the patient's record is a step in the data retrieval procedure. Re-encrypting the patient's record is necessary when storing the data back in the cloud. The emergency system's operation may be impacted by the encryption and decryption procedures, which are crucial and have a big influence.

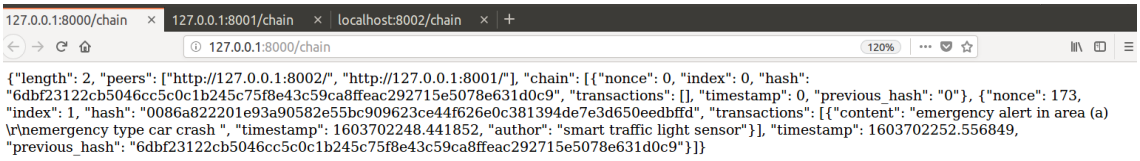
Since it generates a distinct ID for every patient, the hash function is an essential part of the system. The ID is hashed to create an index, which is then used to create the hash table, a data structure. The related value of this index, which links to an empty slot in the hash table, is the address of the encrypted patient records' cloud storage location. Two stages have an impact on the performance of the hash table. Data (key and value) insertion is the initial step. For instance, it takes 49 milliseconds to insert 10,000 in keys using 749 KB of RAM. The second stage involves fetching the encrypted data from the cloud. It takes 7 milliseconds for the system to scan the hash table and retrieve the desired data.

F. Encryption and decryption

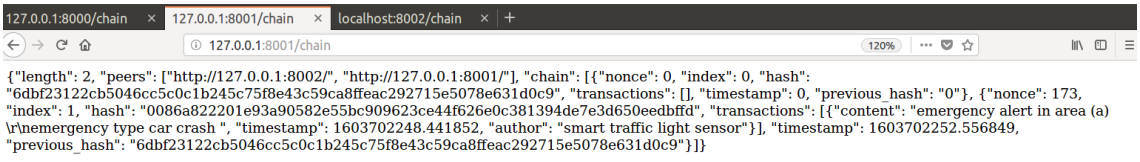
This subsection demonstrates the time it takes for a healthcare provider to encrypt and decrypt an EHR record. The algorithm utilized is the Advanced Encryption Standard (AES), and its efficiency is measured using the Crypto-Js JavaScript library. The encryption and decryption times for a 10 MB file are calculated as 4.67374 seconds and 5.19314 seconds, respectively.

5. Blockchain Complexity, and Limitation

Blockchain technology is currently being extensively utilized, especially in industrial applications, due to its innovative nature. However, there are certain drawbacks associated with blockchain that raise concerns about its performance and reliability. Despite these drawbacks, its innovative features remain intact. Blockchain is a secure distributed data structure consisting of an unchangeable chain of blocks that grows continuously. It provides a direct and secure method for customers and vendors to



(a)



(b)

(c)

Figure 9. Same copy the chain on different running nodes (a) localhost:8000 (b) localhost:8001(c) localhost:8002

communicate and exchange data. Its reach has expanded into various sectors, including wealth management and digital currency.

A. *Verification of Signatures*

Every transaction in a blockchain must undergo signature verification using a cryptographic scheme based on public or private keys. This process of authenticating signatures can be intricate and time-consuming.

B. *Redundancy*

In a blockchain network, the nodes of the chain are processed sequentially, and each intermediate node must be traversed and processed individually to reach the target node. On the other hand, a unified database system processes nodes simultaneously without relying on other nodes. Consequently, the redundancy in blockchain technology affects its efficiency.

C. *Achieving Consensus*

In decentralized environments like blockchain, ensuring shared consensus on every transaction within a block is crucial. The process of reaching mutual consensus can be time-consuming and energy-intensive, particularly considering the network's complexity and the number of participating nodes.

D. *Energy and Resource Consumption*

The rapid growth of the blockchain network may require significant resources. Each block in the blockchain network needs to undergo extensive mining and testing, which demands efficient hardware and results in high energy consumption.

E. *Security Vulnerabilities*

The security risks associated with blockchain tend to increase as the network grows larger. There is an inherent vulnerability wherein if over half of the nodes in a blockchain network agree on something, regardless of its accuracy, it will be considered valid by the entire network. This vulnerability is known as a 51 percent attack and is considered the most severe limitation of blockchain and its implementations.

F. *Limited Scalability and Storage Challenges*

The operational mode adopted by a blockchain network restricts the number of concurrent transactions. Distributed Ledger Technology (DLT) is employed to maximize simultaneous transactions. While blockchain is composed of an unchangeable chain of blocks, the data requiring processing will continue to grow indefinitely. Consequently, storage capacity issues will eventually arise due to limited storage space.

G. *Complexity*

The complexity of blockchain technology is closely connected to the size of the network. Distributed networks, including blockchain, are not completely immune to issues like poor operational conditions or unreliable users/nodes. These challenges can potentially lead to network problems. The key to maintaining blockchain security and preventing network issues lies in creating a strong network that can handle a large number of connected users/nodes.

6. Conclusions

The emergency management system provides a real-time technique for acquiring the necessary information needed in

a life-threatening situation. The inability to obtain such data may be fatal. The integration of IoT, V2V, and EH systems aims to develop an efficient emergency management system. However, these systems might be exposed to vulnerabilities (such as authentication, registration, authorization, and rejection of authorization) and threats (including operation attacks, sniffing attacks, replay attacks, denial-of-service attacks, and man-in-the-middle attacks). That is why trust is a crucial aspect of system security. This paper aims to increase the trust level and security of the overall system. These benefits are achieved through a distributed system topology by employing the blockchain concept. The proposed DEM application can be implemented in a clustered or decentralized manner. The implemented decentralized blockchain allows the DEM program to operate on separate Python nodes, while the front end of the DEM application displays the processed data. The combination of nodes and the front end forms the structure of a distributed ledger.

References

[1] S. Namasudra, G. Deka, P. Johri, M. Hosseinpour, and A. Gandomi, "The revolution of blockchain: State-of-the-art and research challenges," *Archives of Computational Methods in Engineering*, vol. 27, no. 3, pp. 711–734, May 2020.

[2] M. Saqlain, M. Piao, Y. Shim, and J. Lee, "Framework of an iot-based industrial data management for smart manufacturing," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 25, Apr 2019.

[3] S. Mostowfi and W. Buttlar, "Vehicle-to-infrastructure and human-to-infrastructure models for smart civil infrastructure systems," in *International Conference on Applied Human Factors and Ergonomics*. Springer, Jul 2020, pp. 147–155.

[4] F. Colombo, J. Oderkirk, and L. Slawomirski, "Health information systems, electronic medical records, and big data in global healthcare: Progress and challenges in oecd countries," in *Handbook of Global Health*. Springer, 2020, pp. 1–31.

[5] P. Ray, "A survey on internet of things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, Jul 2018.

[6] S. Mukherjee and G. Biswas, "Networking for iot and applications using existing communication technology," *Egyptian Informatics Journal*, vol. 19, no. 2, pp. 107–127, Jul 2018.

[7] M. Fotros, J. Rezazadeh, and O. Sianaki, "A survey on vanets routing protocols for iot intelligent transportation systems," in *Workshops of the International Conference on Advanced Information Networking and Applications*. Springer, Mar 2020, pp. 1097–1115.

[8] B. Dubey, N. Chauhan, N. Chand, and L. Awasthi, "Analyzing and reducing impact of dynamic obstacles in vehicular ad-hoc networks," *Wireless Networks*, vol. 21, no. 5, pp. 1631–1645, Jul 2015.

[9] V. Harigovindan, A. Babu, and L. Jacob, "Improving aggregate utility in ieee 802.11 p based vehicle-to-infrastructure networks," *Telecommunication Systems*, vol. 61, no. 2, pp. 359–385, Feb 2016.

[10] F. Arena and G. Pau, "An overview of vehicular communications," *Future Internet*, vol. 11, no. 2, p. 27, Feb 2019.

[11] P. Geaquinto, "Territorial distinction between transit and automobile topologies," *Applied Spatial Analysis and Policy*, pp. 1–30, Aug 2020.

[12] P. Sewalkar and J. Seitz, "Vehicle-to-pedestrian communication for vulnerable road users: Survey, design considerations, and challenges," *Sensors*, vol. 19, no. 2, p. 358, Jan 2019.

[13] J. Zhang, K. Kowsari, M. Boukhechba, J. Harrison, J. Lobo, and L. Barnes, "Sparse longitudinal representations of electronic health record data for the early detection of chronic kidney disease in diabetic patients," *arXiv preprint arXiv:2011.04802*, Nov 2020.

[14] A. El Sayed, M. Abdelaziz, M. Megahed, and M. Azeem, "A new supervision strategy based on blockchain for electronic health records," in *International Conference on Electrical Engineering (ICEENG)*. IEEE, Jul 2020, pp. 151–156.

[15] B. Hu, Z. Zhang, J. Liu, Y. Liu, J. Yin, R. Lu, and X. Lin, "A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, p. 100179, Aug 2021.

[16] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, vol. 36, no. 9, pp. 155–181, Mar 2019.

[17] R. Shrestha, R. Bajracharya, A. Shrestha, and S. Namb, "A new type of blockchain for secure message exchange in vanet," *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, May 2020.

[18] B. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

[19] H. Noura, R. Melki, A. Chehab, and J. Fernandez, "Efficient and secure message authentication algorithm at the physical layer," *Wireless Networks*, Jun 2020.

Ammar Ibrahim El-Saye completed his Bachelor's degree in Electrical Engineering at the Military Technical College, Egypt, in 2016. He pursued his Master's degree at the Arab Academy for Science, Technology, and Maritime Transport, Egypt, specializing in the Department of Electronics and Communications, which he obtained in 2021. Currently, he is a Ph.D. student at MTC, focusing on various research topics such as encryption, data integrity, distributed databases, electronic health records, security of communications, networks, vehicles, and wireless channels.

Mahmoud Abdelaziz holds a Bachelor's degree in Electrical Engineering from the Military Technical College in Cairo, Egypt, which he obtained in 2002. He then pursued a Master's degree in Electrical Engineering from the same college in 2011, followed by a Ph.D. degree in Electrical Engineering from the University of Victoria in Victoria, BC, Canada, in 2017. Currently, he serves as a Lecturer in the Department of Avionics at the Military Technical College. His research interests encompass wireless communication systems, modulation techniques, channel coding, cybersecurity, and networking.

Mohamed Hassan Abdel Azeem is the Dean of the Engineering college and a distinguished Professor in the Communication and Electronic Department at the Arab Academy for Science, Technology, and Maritime Transport. He holds a Bachelor's degree in Electrical Engineering the Military Technical College in Cairo, Egypt (1985), and further a Master's degree in Electrical Engineering from the same college. In 1996, he earned his PhD. in Electrical Engineering from the University of Kent at Canterbury, UK. With his exceptional contributions to the field, he achieved the title of Associate Professor in 2006 and later became a Professor of Electronic Engineering in 2013. He published over 115 papers in an international journals and conferences.