STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Secure Blockchain-Based Tracking Storage and Permission Verification of Electronic Health Records

Theyazn H. H. Aldhyani[1] , Mohamed Chahine Ghanem[2], ,Mohammad Almaayah[3]

[1]*Applied College, King Faisal University, Al-Ahsa, Saudi Arabia*
[2] *Department of Computer Science, The University of Liverpool, Liverpool, UK.*
[3] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*

ARTICLE INFO

Article History

Received: 17-03-2025
Revised: 30-05-2025
Accepted: 11-08-2025
Published: 12-08-2025

Vol.2025, No.3

DOI:

***Corresponding author.**
Email:
taldhyani@kfu.edu.sa

Orcid:

https://orcid.org/0000-0003-1822-1357

ABSTRACT

Blockchains provide a unique approach to storing healthcare data, conducting healthcare transactions, and proving the trustworthiness of healthcare data in the context of a decentralized and open healthcare network ecosystem. Blockchain technology for healthcare businesses, whether for internal operations or collaborative research, is causing continuing debate regarding the potential risks to user data security and privacy. Despite considerable interest and attention from the corporate, government, and academic sectors, blockchain technology deployment in the healthcare business is still in its early stages. Blockchain technology has the potential to greatly boost patient data security in the healthcare industry. We not only understand the problems and expectations associated with security and privacy, but we also provide effective ways and procedures for overcoming these concerns via the use of technology. The first stage in using blockchains in the healthcare business is determining what features and standards are required to ensure the secure and effective transfer of electronic health information. Then we look at the technologies that may be utilized to offer the essential security and privacy aspects for each of the three potential blockchain uses in the healthcare business. In terms of the sharing of electronic medical records, blockchain technology has three potential uses blockchain technology to validate a patient's identity is standard. The previous work highlighted numerous potential uses of blockchain technology in healthcare. Many various types of information will be exchanged, including ideas, risks, requirements, development tools, system designs, and deployment strategies. Based on the findings of our poll, we were able to make some plausible assumptions regarding the problem.

Keywords: Blockchain, Healthcare, electronic medical records, Internet of things, electronic Health record.

How to cite the article

1. Introduction

Many organizations and departments in the healthcare industry generate and manage critical patient data and information. They may need to use one of the many different healthcare information systems that are currently available. When practitioners lack timely access to essential information, their ability to provide high-quality services such as diagnosis, treatment selection, and referral. There aren't many dependable electronic medical records (EMRs) sharing systems or platforms that provide immediate, on-demand access to dependable, well-managed EMR data. This is a problem when patients require the expertise of many specialists from various institutions. It is difficult to exchange enough EMRs due to a lack of technology and services that aid in the transmission of EMRs.

The lack of reliable EMR sharing platforms and methods exacerbates the problem. Mobile and desktop computers, as well as a plethora of software programs built exclusively for the healthcare business, are just a few examples of cutting-edge technological tools now available to a diverse range of medical professionals and organizations. The increased popularity of Internet of things (IoT) devices in the healthcare business is directly responsible for this trend. Nonetheless, it has been widely accepted [1] that healthcare providers' inability to capture, analyze, and send EMR data on demand with the appropriate level of security and privacy guarantee may significantly impede the quality of real-time healthcare services. Similarly, requesting that their pertinent history data be included in the EMR may cost patients whether they have health insurance or not more money on medical costs [2]. This is due to healthcare providers' inability to collect, analyze, and exchange EMR data on a timely basis. These real-time data transmission examples in the healthcare industry show the critical need for reliable, decentralized EMR data sharing infrastructure and medical information. This infrastructure must be in place to enable both real-time and on-demand data exchange among electronic medical records.

To offer the best possible care, a healthcare information system requires timely and secure access to patient records. This is because patient records contain personally identifying information. The blockchain, a decentralized and secure distributed ledger, has the potential to be used to simplify the sharing of medical information between multiple platforms. To begin, patient records should be organized chronologically. These papers are saved and organized chronologically for the patient's and their doctors' convenience. As a result, it is possible that patients may receive better care. Second, data verification in the absence of a centralized authority Consensus does not need the presence of a centralized authority, and the blockchain allows for the issue of public validation statements whenever this occurs. Third, the original should be preserved in a safe place where it cannot be altered in any way without voiding the warranty [3].

Due to improvements in blockchain technology, it is now feasible to store private medical records on the hash chain without fear of corruption. Interoperability, or the ability of different computer systems to communicate and share data, is the fourth need. Future blockchain technology advancements, including smart contracts and user-friendly app interfaces, may contribute to this expansion. Blockchain technology in healthcare offers a lot of untapped potential, particularly in terms of decreasing or eliminating the administrative barriers, expenditures, and delays that are presently associated with the coordination and sharing of medical data among multiple healthcare organizations. This implies that patient data transfers could benefit from a secure and decentralized environment enabled by blockchain technology. Although it was initially used primarily by the Bitcoin community, the blockchain technology it enables is now being used in a variety of fields, including healthcare [4]. This is happening as blockchain technology gains popularity across a variety of industries and uses, including digital money, the financial industry, and conventional business processes. Instead, we believe that future generations of the ecosystem will benefit from a complete understanding of the difficulties that healthcare blockchains are facing, as well as potential solutions. Future generations will benefit from our awareness of the ecological sustainability of healthcare.

Despite the fact that numerous academic and commercial organizations have developed projects and products in this field, the majority of the products currently available are in the healthcare blockchain space. Even though various organizations and enterprises have created blockchain-related initiatives and solutions for the healthcare industry, this remains the case. The fact that various academic and for-profit organizations have developed blockchain efforts and solutions for the healthcare business does not invalidate this assertion.

There have also been recommendations to use cryptographic technologies to provide extra security barriers, such as protecting the confidentiality of patient medical records. In view of recent discoveries and achievements in this sector, we propose the following: However, little effort has been dedicated to fully analyzing and describing the privacy and security benefits that healthcare blockchain provides [5]. One of the primary difficulties addressed in the process of developing the blockchain for use in the healthcare business was the need to protect the privacy of both patients and professionals. This is because knowing the blockchain's security and privacy is required to address the key challenges with existing healthcare blockchain solutions.

We are certain that this will be beneficial. This is because a greater knowledge of the healthcare blockchain's privacy and security characteristics will make it simpler to address the basic concerns with blockchain-based healthcare systems [6]. It will initially assist non-security professionals in understanding the healthcare blockchain's privacy and security standards, as well as the risks associated with them. Second, specialists in the blockchain-based healthcare business will have access to cutting-edge security and privacy technologies. Furthermore, it will analyze the most critical privacy and security problems for blockchain in healthcare, suggest solutions that agree with these security objectives, and identify any flaws or concerns that remain. It may also assist those working in the technological and medical research industries in developing blockchain healthcare systems and practices suited to specific use cases.

2. Methodology

The advantages of using EMR in healthcare facilities where and why are electronic health records used? To get things started, let's establish a few terms that will be used throughout this essay to characterize blockchain technology as it pertains to the medical field. Please consult [7] for a more in-depth examination of each of these ideas. Hospitals and clinics are included on the list of facilities used by Chief Data Officer (CDO) because of their ability to provide direct patient care.

Every patient seen at a CDO receives an EMR, regardless of whether they are hospitalized as inpatients or treated as outpatients. EMRs are electronic medical records that CDO physicians create to document their patient’s medical histories and treatments. Furthermore, these records serve as a record of every element of each patient's care. The CDO is responsible for supervising the EMR and ensuring that patients receive the best possible care.

Each CDO is responsible for developing and maintaining its own EMRs, which also include EHRs. An electronic health record is an EMR that may be shared between CDOs and the patient. The patient decides who else has access to their electronic health information and under what conditions. A "personal health record," often known as a "PHR," is a person's medical history file that is kept up to date. The document's title already implies this. This record may include data from a variety of sources, including an EMR, an electronic health record (EHR) or a wearable for home monitoring. A comprehensive PHR can assist doctors in developing more tailored treatment regimens for their patients. Blockchains are distributed ledgers designed primarily for managing and transferring patient health information in the healthcare industry.

If a CDO or an individual builds their own blockchain or uses a blockchain service provided by a blockchain platform provider, they may keep all their medical records on it or only a portion of them. Medical institutions may be able to securely store and exchange data by using the blockchain's immutability and decentralization. Remember that the privacy and security standards for blockchain-based healthcare payments differ significantly from those for blockchain-based healthcare payments in finance. The first option proposed is a blockchain-based payment system that accepts virtual currencies such as Bitcoin or Ethereum [8]. A distributed database is a technology that preserves EMR data, makes it available to users, and stores essential database data. Blockchain technology can benefit applications such as distributed databases and payment systems. To keep this study simple, it will solely look at how blockchain technology may help with privacy and security concerns in the healthcare business.

The issues of double spending and wallet security are just two of the privacy and security concerns raised by blockchain-based healthcare payment systems; the others are not addressed in this essay. Patients' private rights and the security of their computerised medical information are now two problems that must be addressed. Although the increased efficiency of electronic medical records can benefit both patients and clinicians, concerns about privacy and information security have

been raised. Is it unlawful for patients to review their own health records that they have created? Both the insurance provider and the treating doctor will have access to all the patient's medical records, regardless of who provides treatment for the patient. Who has access to a patient's medical records? Should different people have access to various parts of the patient's medical record? Who has the legal authority to make such decisions? In the digital age, where should a patient's medical records be housed to preserve utmost privacy? How many electronic medical records of patients would need to be stored in a central database that provides open access if numerous databases could be linked over a network? Is there a specialized data storage solution available that can provide the privacy and security that EMRs require? The "creator" of a medical record is the person or organization ultimately accountable for the data and instructional content of the record. The treating physician or laboratory experts frequently input a patient's medical history into a healthcare information system. The "manager" of such information is the person or organization in charge of monitoring secret information and always maintaining its security [9].

A healthcare system's administrators interact with both patients and employees. In a healthcare system, the generation, storage, and retrieval of medical records are subject to patient-declared privacy constraints; it is the administrator's obligation to maintain the system's security. When we say "owners," we mean any individual or organization who is legally allowed to hold an object. Frequently, the patients who should have legal ownership of the information in their medical records are not the intended recipients of that information. Nothing would change even if they had access to personal medical records because everything remained the same.

Both federal and state laws protect a patient's right to privacy, confidentiality, and authenticity of medical information, and these rules must be followed. Here are some examples of this privilege: On the other hand, once data is acquired and recorded in any manner, whether manually or digitally, the healthcare practitioner becomes the immediate proprietor of the information. This is because the healthcare provider also controls the data maintenance and storage infrastructure. The doctor or other healthcare provider ultimately holds legal custody of the patient's medical records and is responsible for ensuring their integrity. As a result, the healthcare practitioner is granted legal rights and duties under the conditions of the patient's medical record. Persons with access to a patient's medical record may be divided into two groups: those with the right to read the record and those with the right to generate it. Only the person who generated the medical records is authorized to make modifications to them [10].

Because they either treated the patient or performed the laboratory test, this person is accountable for the accuracy of the data in the patient's medical record. This individual must have either treated the patient or arranged for them to be tested at a laboratory. Regardless of the inaccuracy, the data that has already been entered into the patient's medical record is final and cannot be changed. Whatever the motives for entering the data, this is correct. Until a new diagnosis is established, the doctor will be unable to add the most current one to the patient's medical file. Patients can provide another person access to their medical records under the CDO's patient privacy policy. For example, access to the database's health-related information may only be granted to insurance companies to assist them in paying medical expenses.

A patient must first acquire written consent from a CDO before receiving medical care there. This documentation can be obtained from the medical facility where the patient will be receiving care. The patient's permission indicates that, in its capacity as data custodian, the CDO may disclose personally identifiable information to third parties. This is what will happen if the patient follows the doctor's recommendations. Patients can also sign a declaration authorizing the sharing of their medical information among physicians who are members of a medical union. As a result, patients can save money by foregoing unnecessary diagnostic treatments. As part of their medical care, the patient is offered the option to make this decision. Any changes to the patient's or family member's access rights to their medical records, as well as any new rights granted to others, must be communicated to the patient or family member.

The capacity of the CDO to organize the large volumes of medical data at his disposal will have a considerable influence on the resolution of the second challenge. Most hospitals throughout the world are now developing their own EHR. However, the vast majority of EHRs are developed and maintained either on-site at the site of use or remotely at a third-party data center. Other EHR systems, on the other hand, are developed and executed by the CDO organization itself, and they may be installed and administered anywhere in the world. The first solution, which may be viewed as a local storage mechanism, is simple to implement but limits data sharing with other EHR systems [11].

Recent advances in distributed ledger technology have fueled optimism for the creation of secure platforms for the interchange and storage of digital medical information. Because it combines distributed ledger technology with cryptographic techniques, blockchain technology can perform critical security duties such as validity verification, resistance to manipulation, and resistance to distributed denial of service (DDoS) assaults. For data transfer and storage to be considered safe, they must meet several standards. In general, Satoshi Nakamoto [12] is credited with inventing the blockchain concept, which was initially published in 2008. The first public implementation of the blockchain technology, dubbed "Satoshi Nakamoto," was publicly accessible in 2009. The decentralised digital money system known as Bitcoin was chosen as the preferred currency. We'll go through the coin's key security and privacy features, as well as the methods used to generate them. We'll also go over the safeguards in place on the Bitcoin blockchain to preserve user anonymity and data confidentiality.

After a node broadcasts a transaction to the whole Bitcoin network, miners "mine" it by merging it with other recently made transactions into a block and looking for a nonce that meets the required hash function. This is referred to as "mining." This is the outcome obtained when a Bitcoin node "broadcasts" a transaction to the whole Bitcoin network. This stage occurs after the node has already published the transaction. This approach is used when a node in a network must notify other nodes in the network about a transaction. The blocks are not regarded as authentic until all nodes successfully incorporate them into their own blockchains, which may take some time. Only after a block has been added can its hash be used to determine the hash of the preceding block; at which time it is recognized as genuine and authentic [13]. To proceed with accepting the block, the following steps must be taken: To prevent hostile nodes from undermining the process of obtaining consensus without the help of a centralized authority, this system must be able to guarantee that the state of the blockchain is always constant across all copies. Furthermore, this technique must ensure that the state of each copy of the blockchain is always consistent. These two prerequisites are mutually exclusive and cannot exist in isolation. A consensus approach is used to ensure that the great majority of network users offer their permission before any transaction produced between any two nodes on the network may be finalized. It is vital to add redundancy to the network's architecture so that it may continue to function regularly even if any of the nodes get damaged or destroyed. It is critical for the network's overall functionality that it be able to recover quickly and thoroughly from instances like these.

Gossip, sometimes known as the Epidemic Protocol [14], is a protocol that is often used in distributed database systems. This protocol is used to synchronise data held on specific nodes. This approach is also known as an "epidemic process," which is essentially another term for it. This is the primary goal of the plan that will be implemented in the future. In the long run, this method will provide results equivalent to those attained in the past. As part of the "Gossip" protocol, a certain node in the network will send information to a subset of the other nodes in the network. This procedure will be carried out over the whole network. Similarly, to how a virus spreads, the information finds its way to each and every node in the network on its own. After the operation is completed, the data is distributed throughout the network to each node for processing. Bitcoin transactions are verified using the Gossip protocol, which also ensures that messages are transmitted in a timely and uninterrupted way.

The approach enables the achievement of these two goals in an efficient and effective manner. It will be able to attain both goals at the same time with the aid of this technique. This remains true regardless of whether new blocks are being generated or if the network has accepted previously generated blocks. The hash chain cryptography technology is employed in the Bitcoin blockchain to ensure data integrity and prevent data manipulation. This solution employs two technologies with a proven track record of success: the hash pointer and the Merkle tree [15].

A hash pointer is a value that is first extracted from transaction data and then encrypted using a hashing technique. This number acts as the storage address for the data created because of the compression of transaction data. We can check for changes to the data since we are utilizing hash references. A blockchain enables all data blocks to connect with one another and share information with one another. The position of a Merkle tree's leaf node may be identified using a cryptographic hash of the data block. To identify the node, the cryptographic hash of each succeeding node, which is the same as the hash of all the nodes it has created, is employed. Only the leaf nodes of a Merkle tree are connected to the data block's hash value. Merkle trees, which are a generalization of hash chains, may effectively and efficiently analyze the information contained in very large data structures for correctness. The Merkle tree is depicted here as an example of a hashing algorithm. Merkle trees are used within the Bitcoin blockchain to help establish a reliable and immutable method of storing and preserving transaction history.

A Bitcoin transaction's validity is verified using a combination of two different security methods that work in tandem. The first thing that must be shown is evidence that the transaction occurred. Once a coin has been used in a transaction, it cannot be spent on its own, removing the potential of an attack in which the money is spent twice. As a result of this improvement, the chance of coins being stolen has been greatly reduced. A digital signature is the most reliable way of authenticating computer-related affairs. To secure the legality of every transaction, Bitcoin employs both a consensus mechanism and a publicly verifiable digital signature method known as the Elliptic Curve Digital Signature Algorithm (ECDSA). When consensus procedures and digital signatures are combined, each user on a blockchain may independently confirm the legality of every transaction logged on the ledger. Users that employ this method have a greater chance of promptly discovering transactions that violate the cryptocurrency's rules of service, such as spending the same coin more than once. Because of the "Simplified Payment Verification" (SPV) protocol, the time it takes to confirm a Bitcoin transaction is getting shorter and shorter. Rather than downloading and analyzing the whole blockchain, it will just keep the block headers from the chain that is presently the longest. As a result, there is no need to physically remove construction components [16]. This reduces the computational and storage load that the Bitcoin wallet client is expected to bear.

Pseudonymity is the practice of hiding one's identity on the internet by adopting a pen name or another fake persona in lieu of one's actual name. Pseudonyms are popular in online gaming communities. Another alternative to using a pseudonym is to operate under a different name, such as an assumed name or an alias. As a result of the widespread use of pseudonymity, users may now participate in debates that are, likely, anonymous. When a user joins the Bitcoin network, a hash of their Bitcoin public key is automatically generated in the form of a Bitcoin account address for them. Users have permission to send and receive bitcoins at this address. Using a pen name generated from the user's public key hash is one method of remaining anonymous when engaging with other users online. Even if individuals engage with the Bitcoin system while hiding their true identities behind aliases, their true identities may be found. Anonymity is maintained by hiding one's identity behind a public key.

As a result, it is generally safe to assume that a person's online identity may be determined from their public key if they want to publish it. Consider the digital signature we discussed earlier: To evaluate whether the signature is legitimate, the user compares it to the signer's public key. Because of this proof, the validity of the signature as an original work of art has been proven. When addressing something known as "public key infrastructure," it is critical to emphasize that a trustworthy third party oversees managing all the public keys that are in use. A public key infrastructure (PKI) system may verify a user's identification by returning a public key that can only have been produced by that person. A PKI will next verify the signer's identity after a signature has been confirmed. In this aspect, a PKI offers several benefits to its users. This implies that, in the context of PKI and certification authorities (CA), it is not possible to employ centralized techniques for user registration and key management, such as CAs and public key infrastructures, within Bitcoin's decentralized network [17]. To participate in the Bitcoin system, users must generate one-of-a-kind private and public keys that cannot be reproduced by anyone else. It is conceivable that the user is using a pseudonym when there is no CA to confirm the public key, since it cannot be linked to the user's genuine identity when there is no CA to verify the public key. When displayed in this manner, the user's personal information may be clearly differentiated from the public key. An opponent, according to the concept of "unlinkability," cannot deduce anything about the nature of any links between two or more system components based on his observations and prior knowledge of those entities. This is what it means when it claims that an adversary cannot draw any conclusions about the nature of any links between two or more system components. When combined with pseudonymity, unlinkability is a highly sought-after attribute of anonymity because it gives an extra degree of protection to the system's privacy. By utilizing a random technique, Bitcoin users may generate an endless number of random key pairs or addresses. This is equivalent to the ability to open several bank accounts.

It is critical to note that these key pairs are produced at random, have no relationship with one another, and have no link to the unique user's personal information. Furthermore, none of them bear any resemblance to one another [18]. Users can choose from a variety of pseudonyms while sending and receiving money, which contributes to at least partially unlinkable anonymity. Bitcoin's use of several pseudonyms to provide the impression that a single user's activity cannot be linked to a specific individual is dishonest and deceitful. Statistical approaches may be used to trace the transit of bitcoins and mine the addresses contained in transactions. If we take a closer look at this, a user's entire Bitcoin transaction history will become public information if her identity is connected to her Bitcoin addresses. This data will be made available to the public. To showcase the possible uses of blockchain technology, we will begin this section with a use scenario involving the sharing of EHR information. When questioned about his symptoms, Bob, one of the clinic's patients, stated that he suffered from stomach aches on a regular basis. Because she was worried about her patient's health, her primary care physician advised that she undergo a comprehensive physical examination at Hospital A. After a second opinion, he was

diagnosed with stomach cancer. It was proposed that he have his stomach removed at a cancer treatment centre. When Bob arrived at Hospital B, he was immediately put under the care of an attending physician. Because of his diabetes, which increases his risk of complications after surgery, Bob's attending physician must consult with a committee of physicians from several institutions before selecting what type of therapy to give him. Because one of these doctors is Bob's primary care physician, they are the most familiar with Bob's current health [19]. This will aid in the development of a more comprehensive strategy for surgical procedures and therapy. This is noteworthy given that Bob has a variety of medical concerns, including diabetes.

The consultation participants must be aware of Bob's whole medical history, not only the results of his tests and the data documented at hospital B. It is feasible to protect patients' privacy while speeding up operations by implementing a blockchain-based healthcare system that makes it easier for providers to successfully share patients' medical information with one another. Any medical records saved on the blockchain will be accessible and transparent to any system administrator [20]. To be more specific, using blockchain for electronic health record sharing leads to the following advantages: Bob's history, medical information, and any other pertinent papers are securely stored on the chain. This allows any consultation group member who requires them to have rapid access to them when they are needed. By storing HER access logs, prescriptions, and other treatment-related actions on the blockchain, patients and other authorised users will have access to their information whenever and wherever they choose. Furthermore, it is easy to find in the event of a medical emergency. The type of patient records preserved may change depending on the degree of the patient's illness, as indicated in Figure 1. Regardless, all patient records include the patient's name, the name of the attending physician, and the date the record was created. The attending physician in charge of the patient's care must digitally sign electronic medical records, or EMR but right now, only a small number of the doctors who oversee the record's content are required to sign it.

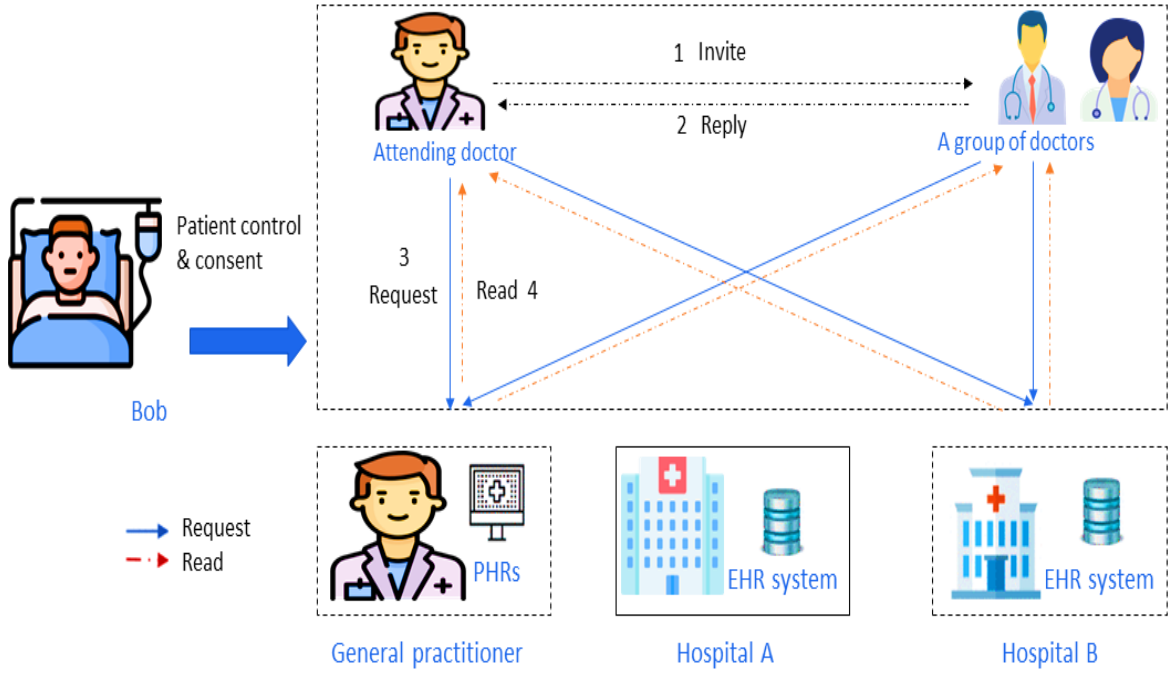


Figure 1. The use of Shared Electronic Health Records without a Blockchain.

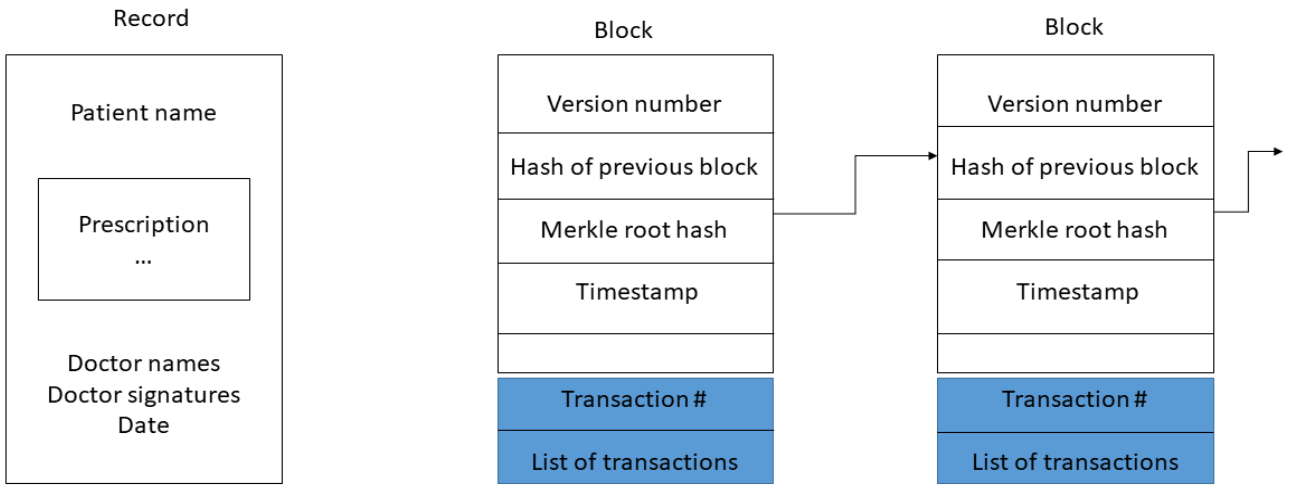


Figure 2. Internal Structures of Records and Blocks

A transaction is just an updated record that can be followed across the blockchain, finally, these entries will be grouped into groupings known as blocks [21]. Blocks are the physical manifestations of the digital ledger that comprise the blockchain. The format of transactions in the healthcare business, as shown in Figure 2, may be influenced by the structure of the blockchain used there. If the public and private keys for the transaction are generated at random, the user's anonymity will rise considerably.

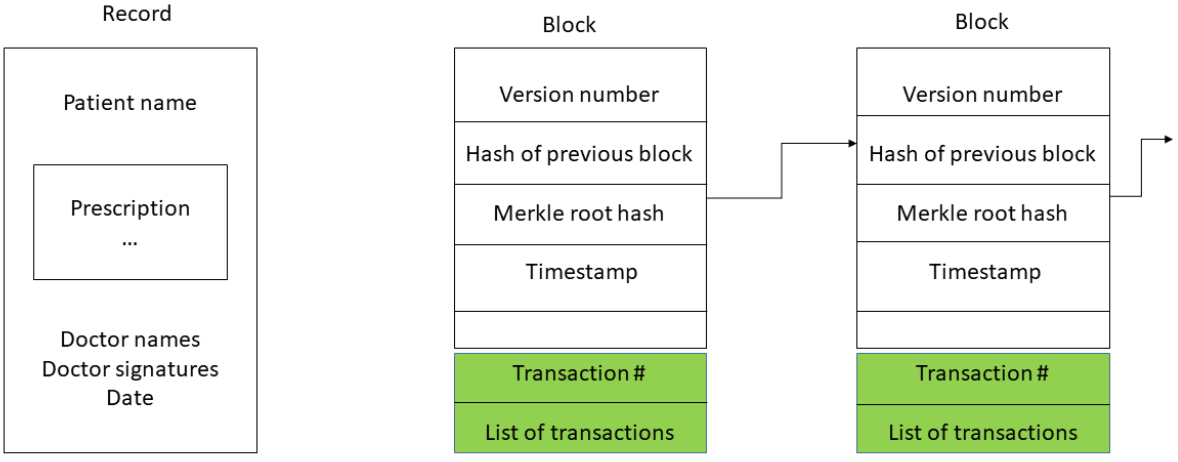


Figure 3. Three Separate Reference Architectural Designs' Transactional Frameworks

Deals are organized into larger groupings known as "blocks" with time, the bricks start to fall into place. Figure 3 shows three separate reference architectural designs' transactional frameworks. After confirming submitted transactions, miners consistently add them to blocks, which are then added to the chain's final node. Throughout this time, processing is taking place in the background. A block stores the hash of the block before it, as well as a collection of transactions. Each of these data items is retained in its entirety in a block. The basic structure of the block, like the internal data, will be determined by the consensus technique used.

In a blockchain-based healthcare system, we will assume that clinicians would produce new patient records in an EHR system managed by the hospital's CDO. When a patient agrees to allow their medical history to be shared with other medical institutions or healthcare providers, their electronic health record is converted into a transaction and sent over the network. This occurs when a patient grants consent for the dissemination of his or her medical records [22]. After mining is completed and miners have reached consensus, the transaction will be "automatically" put into a new block that will be "automatically" uploaded to the network. This is expected to happen once the blockchain has been fully established. Figure 4 depicts the volume of medical data delivered over blockchain. As a result, the blockchain may divide into three different networks. Healthcare is the only other area that has used blockchain technology so far. The blockchain infrastructure will be present in some form or another. In any scenario, the CDO may benefit from blockchain technology.

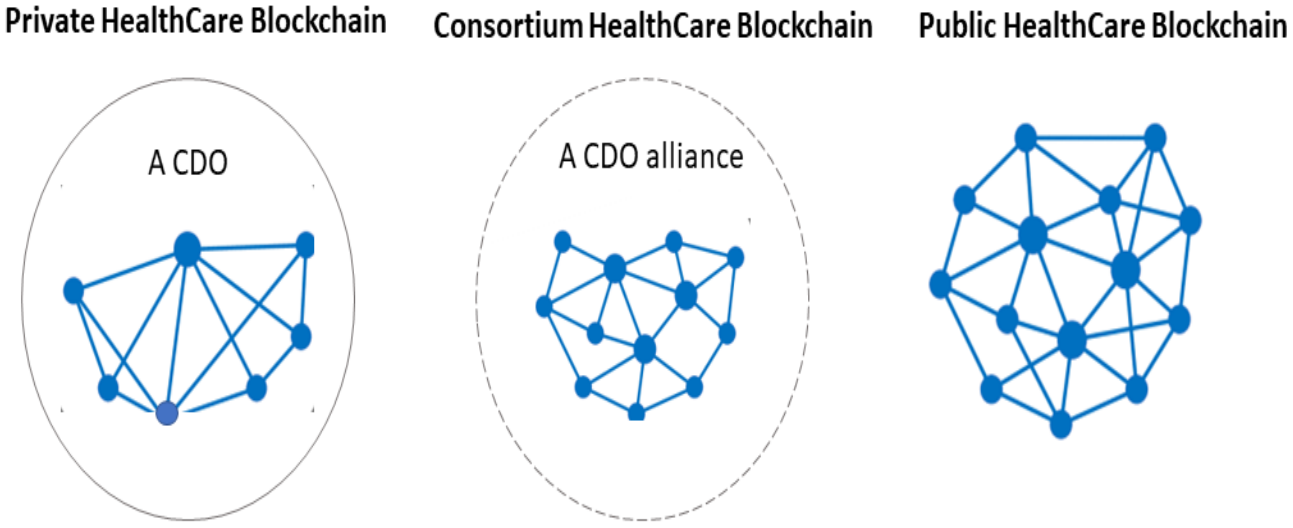


Figure 4. There Are Three Distinct Blockchains Being Used in the Healthcare Industry

Anyone has access to the distributed ledger's data as well as the distributed ledger itself. The core infrastructure of a blockchain is developed and maintained by a blockchain service provider that also owns the infrastructure. Passwords and other user authentication procedures are among the numerous components of a complete security and privacy architecture. Integrating multimodal security and privacy components into the medical blockchain network, which stores patients' confidential information, is a challenging and time-consuming operation. When blockchain technology is implemented in the healthcare business, user safety and privacy must be prioritized. All patient information, in our opinion, should be kept as private as possible. This includes taking all reasonable efforts to avoid cyberattacks, such as encrypting sensitive data, authenticating users, and securing apps, as well as staying current on security certifications and processes.

3. Proposed Approach

The data recorded on the healthcare blockchain is expected to provide a higher level of privacy than Bitcoin transaction records. People's unwillingness to discuss their health issues with others is increasing. This tendency is expected to continue. As a result, those in charge of creating and managing healthcare blockchains must place an even greater focus on protecting patients' privacy. The privacy and security needs for blockchain technology in the healthcare sector are summarised here briefly. When dealing with money, you must surely maintain consistency [23].

Each transaction is heavily dependent on the patient health data stored on the node and must be perfectly timed. It's possible that using the consensus technique employed by blockchain technology will ensure this. This is done to guarantee that the blockchain remains consistent. Keeping Financial Transaction Records: The Reality other parties cannot edit the medical data that is part of a transaction while it is being broadcasted, mined, or stored on the blockchain. Because blockchain technology employs a hash function that is immune to collisions, it makes it extremely difficult to undertake fraudulent

alterations to transaction histories. Integrity and authenticity of financial transactions before accepting medical records as part of a transaction, readers of medical records using healthcare blockchains must ensure that the medical records they are reading are true and unmodified [24]. A transaction on a blockchain, which has applications in the medical business, is used to do this. The transactions' and the system's accessibility because accessibility is a key element of the blockchain used in the healthcare industry, users may access transaction data whenever and wherever they need to. Those who use this method will not have to worry about their identities being disclosed. Users can request anonymity at any moment during the authentication procedure before giving any personal medical information. The user does not want the specifics of the medical data to be connected to his identity because any valid user can access the data on the blockchain. When even a single piece of a user's medical information is linked to the user's identity, a larger problem occurs. This exposes all the user's medical information, which might have disastrous consequences for the user's life and career. Authorized users are only permitted to view a patient's medical records within the lawful treatment times permitted by law. Consider the previously outlined scenario in which electronic health records must be transmitted. Bob's doctors will not be able to access his medical records during consultations or treatments unless he first grants them permission. The patient should have unlimited access to the access record and should be able to check at any time whether his or her personal health information is being accessed and utilized correctly. Identification and authentication methods for system users when implementing blockchain technology in the healthcare field, permissioned blockchains are the most widely employed. On this blockchain, a central authority node is responsible for confirming user IDs. Users do not want to jeopardise the security of the blockchain, which is why. No one wants to jeopardise the anonymity provided by the blockchain, which is the cause of this. For your convenience, we have produced a table that details the privacy and security requirements as well as the techniques that comply with them. We emphasize that certain requirements, such as consistency, tamper-resistance, and validity, are guaranteed by the intrinsic qualities of blockchain technology and explain why this is so. Implementing blockchain technology is one option for meeting some of the extra privacy and security concerns, such as availability and anonymity [25]. There are numerous approaches that may be used. However, by introducing new technological aspects, the blockchain may be improved. To meet the remaining security and privacy needs, more technical measures will be required. This is an extremely crucial factor to remember when it comes to maintaining your privacy.

On the one hand, patients in a blockchain-based healthcare system would like total transparency. This is the case because the accessor is a skilled medical professional. That is the question: Should we band together or not? Similarly, some people may not want others to have access to their confidential medical records [26-28]. For example, a researcher searching for links between heart disease and demographic variables would require access to all heart disease medical information to complete their analysis. According to the principle of restricted disclosure, it is against the regulations for researchers to get more information about people's ailments when preparing their medical records. In certain cases, patients desire that all their CDOs be linked together to provide a continuous history of their medical care. This request might come from hospitalized patients or those who visit a doctor in the privacy of their own homes. The simplicity with which relevant information may be found will be appreciated by both the medical personnel who are treating the patient and the patient themselves.

This raises an essential question: given that it would typically consist of individuals performing a range of tasks, a publicly accessible blockchain for healthcare would need to establish what sort of anonymity measures it would require. Due to the anonymity constraints inherent in blockchain technology, we highly advise users of healthcare blockchains to utilize a keyed-hash message authentication code. Within the constraints of this system, a user can establish several aliases, each of which can be accessed using a unique key. If a person wishes to share their health information with another user, they can give that other user permission to link to their medical data by providing permission to the first user. When it comes to integrating medical data, the more often a key is changed, the less likely it is that one piece of data will be related to another [29-30]. Using two separate pseudonyms would be more efficient. If that process was used instead, the result would be as follows: While working at hospital B, Bob makes the deliberate decision to abandon his previous identity and adopt a new one. Doctors at Hospital A will be able to examine just the patient records created there, but doctors at Hospital B will be unable to read any patient records created at Hospital A. Figure 5 depicts the first possible outcome of several different ones: a data chain for storage and exchange. Certain users may be granted access to the system after successfully completing the authentication procedure. Patients and physicians are two examples of these consumers.

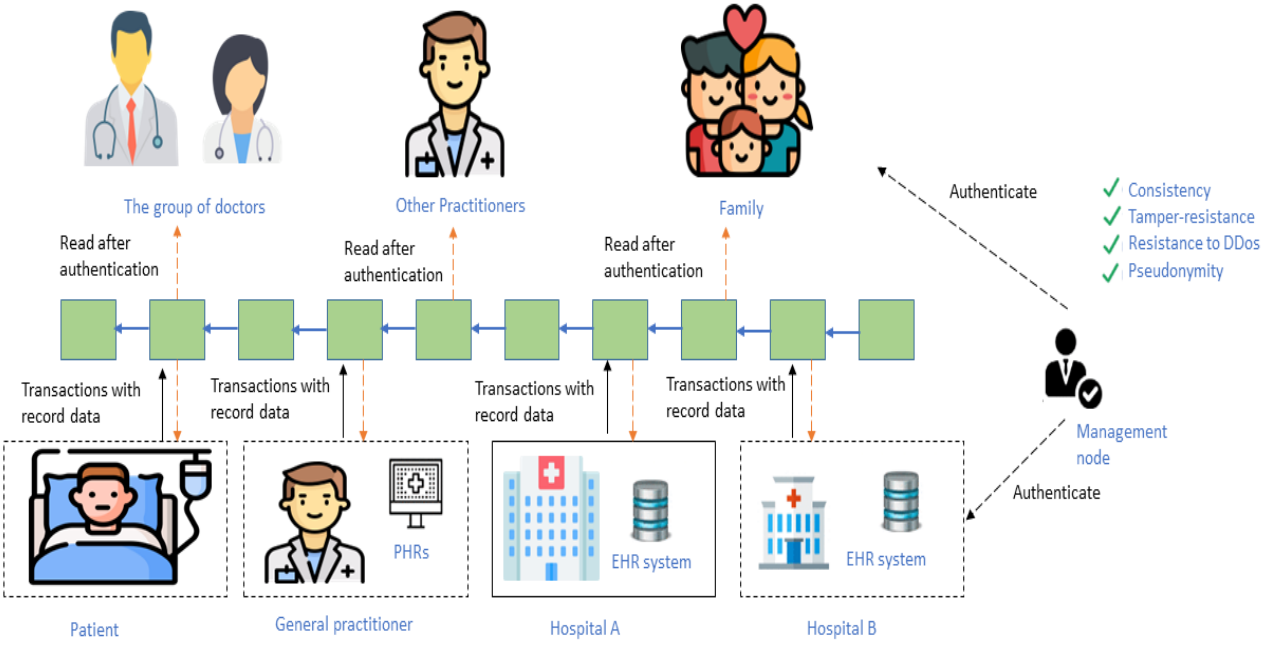


Figure 5. A Chain Based on Plaintext-on-Chain for Data Storage and Transport

Consider the following uses of an electronic health record: Hospitals A and B are both members of the same medical association. A blockchain-based solution might allow patients' data to be shared among partner healthcare organizations. After the management node has validated the data, it may be accessed by the team of physicians, Bob and his family, and anybody else who requires access to Bob's medical information. Figure 6 depicts the DSS chain's reference transaction architecture for our assessment. As a result, all Alliance inpatient and outpatient CDOs will be able to trace a patient's whole medical history sequentially. The hash of the result is signed using private keys by the doctors in control of the information in the record.

3.1 DSS Chain Characteristics

The present financial transaction is linked to all previous ones involving a certain patient. It establishes a continuous chronology of a patient's medical information across all participating CDOs, whether they are inpatients or outpatients. This not only allows doctors to keep track of their patients' difficulties, but it also allows patients and other users to access the files quickly and easily they require. If hostile individuals get access to the system, data will surely be compromised. During the authentication process, the system administrator will also discover critical information. To be more dependable and trustworthy, the healthcare blockchain requires extra privacy and security precautions such as symmetric encryption and anonymous authentication. Because of the underlying nature of the blockchain, these approaches are essential. Anonymous authentication is a method of validating a user's identity without revealing any personally identifiable information. These identity-based or group-based signature-based authentication techniques can be used to confirm roaming service customers. Their approaches can successfully ensure user anonymity and allow for the cancellation of previously granted access. We saw quick and anonymous wandering and the procedure for SIN authentication in reference number 15. Group signature is critical to their system since it not only allows users to be verified independently from their home servers, but it also provides strong user anonymity and maintains optimal security. This was submitted anonymously. Anonymous signers can maintain their privacy while keeping their identity hidden thanks to anonymous signature algorithms. It seems logical that the more people in a group, the more difficult it is for an opponent to determine who is signing. A manager oversees managing the members of the group inside the group signature algorithm. In the event of a disagreement, many steps must be performed, including adding or deleting group members and disclosing the signer's name. Therefore, the management node may function as the group manager, controlling the group's operations, and group signatures can be applied to consortium blockchain transactions.

Once again, attribute-driven signatures are used. Attribute-based signatures, or ABS for short, allow signers to employ any attribute predicate authorized by attribute authorities to authenticate messages. By switching from identity verification to characteristic verification, ABS prevents the signer's identity from being revealed during the signing process. In real-world scenarios, however, a single user may have numerous identifying characteristics, and various administrative organizations may issue certificates for each of these characteristics. One example is using a private key associated with the titles "doctor" and "researcher" to digitally sign a medical paper. A means of communication that may be traced while being private and secure Figure 6 depicts an example of a hypothetical alternate circumstance. In this potential blockchain use, the plaintext of patient medical information is encrypted and stored alongside the transactions. To encrypt the record, use the recipient's public key in conjunction with a safe asymmetric encryption algorithm. The transaction is then broadcast into the network, together with the previously merged ciphertext and sender and receiver public keys. Furthermore, healthcare consortium blockchains and public healthcare blockchains are better suited for this type of healthcare blockchain system than commercial healthcare blockchains. As a result, the blockchain's primary function in this circumstance is to serve as a route for the secure transmission of data

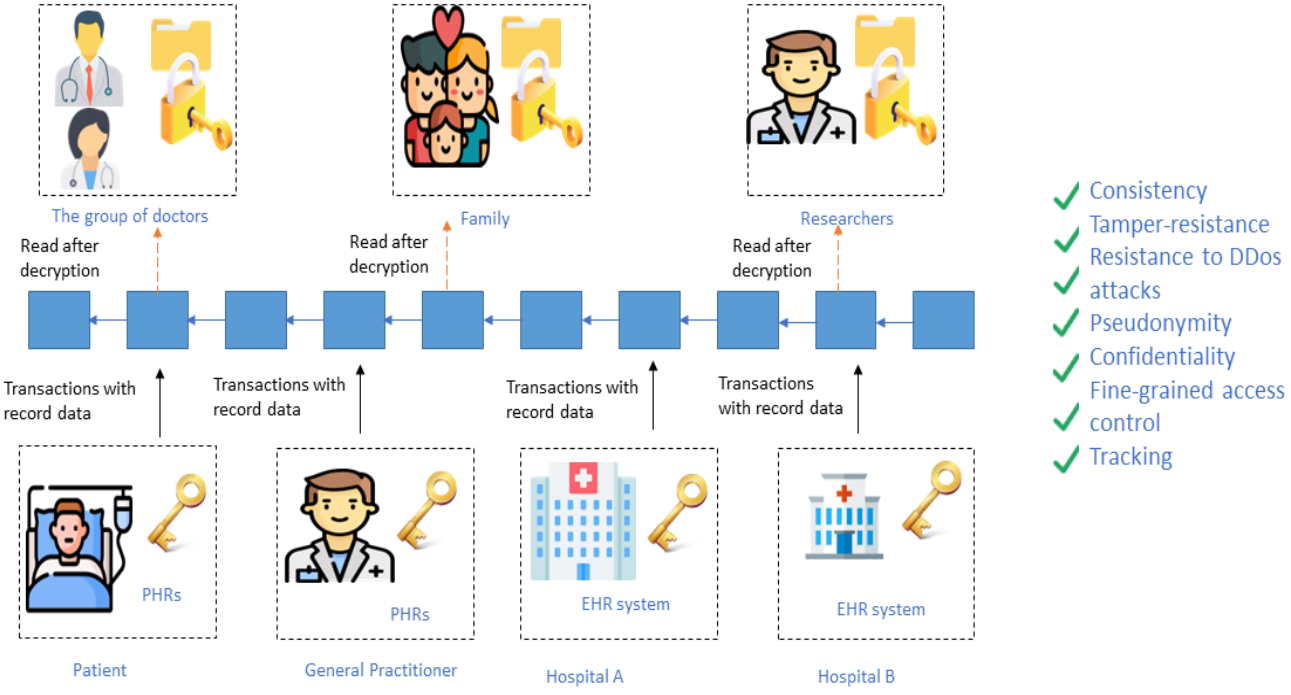


Figure 6. "Ciphertext-On-Chain." for Chain Transmission and Secure Chain Tracking

Consider the former issue that developed when an electronic health record was used. When Bob's team of physicians must analyze his medical history to decide whether or not to undergo surgery, Bob's primary care physician uses an asymmetric encryption technique to encrypt each record. Bob's team of physicians then broadcasts the resulting transactions over the network. This allows the medical professionals to confidently determine whether to operate on Bob. This type of protection will keep Bob's medical records safe from unauthorized access. The medical personnel, which includes physicians and nurses, is equipped with the instruments needed to understand each file. In this instance, to safeguard the patient's medical file, an attribute-based encryption approach might be implemented. As a result, the amount of data space required by the blockchain may be greatly decreased. When a receiver validates the validity of the signatures, they validate the whole chain of communications. Because each transaction usually involves several receivers, it is possible for a transfer-directed graph to emerge for each record. Figure 7, on the other hand, depicts a transmission-directed graph in motion. Users 4 and 5 receive R1 from User 1 after it has been encrypted and transmitted to Users 2 and 3 in separate encrypted transactions. As

a result, a record-level transmission-directed graph is formed, which can be used in a system to track patient information transfer.

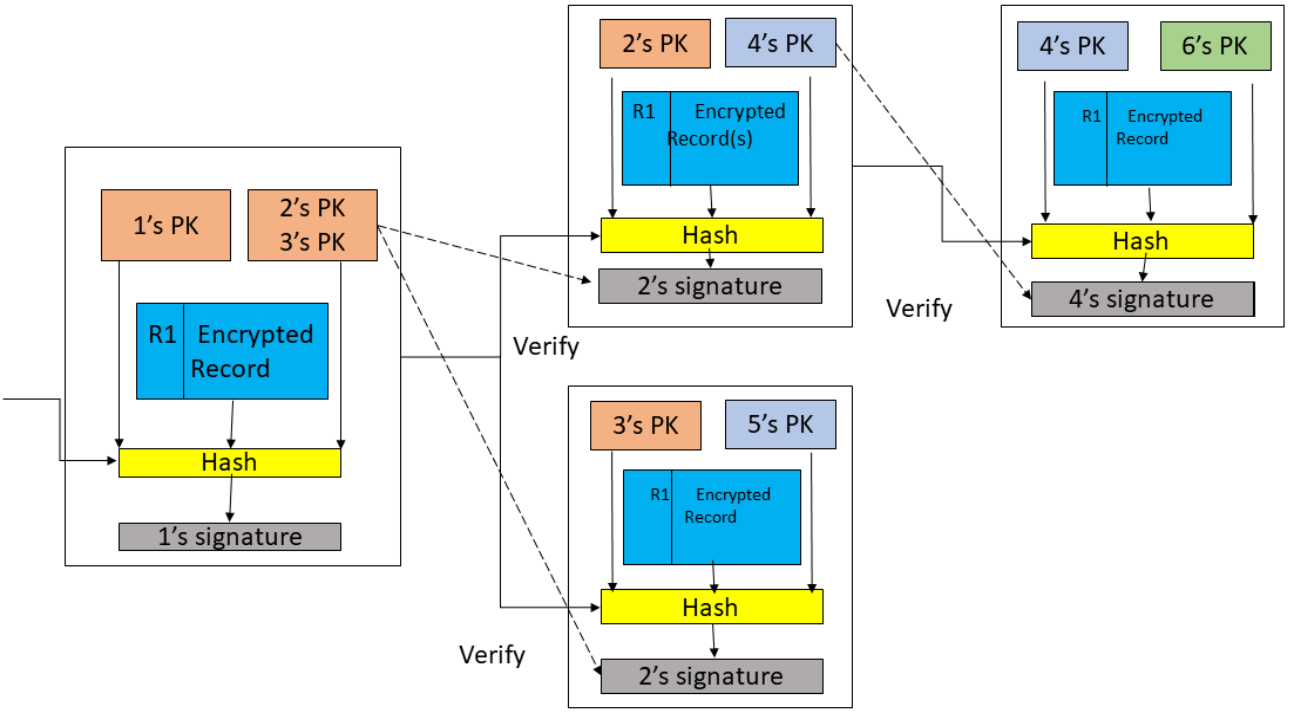


Figure 7. A Transmission-Focused Graph

The following is a sample list of some of the various perks provided at STT sites: Only individuals with access to the matching private keys are able to decode and examine the encrypted patient health information stored on the blockchain. Each transmission in the series is linked to the ones that came before it in an unbroken chain from beginning to end. To determine the sequence in which the records were transmitted, a directed graph can be employed. This advancement will make it easier for users to track how their personal health details are shared. The sender is under no obligation to take any step in order to provide the receiver read access (PRE). This approach may be used to decrypt ciphertexts encrypted with homomorphic encryption without affecting the underlying plaintexts. As a result, every time a record is moved to a new location, a new transaction is required. As a result, the amount of difficulty involved with adding information to the blockchain will increase. Furthermore, if a non-authorized user is provided access to a key that belongs to an authorized user, two or more collaborating individuals may launch a collusion assault. PRE and ABE, which are resistant to collusion efforts, are additional security and privacy safeguards required to assure the safety and confidentiality of a blockchain-based healthcare system. These safeguards must be implemented. These safeguards are critical for preserving the confidentiality of patients' medical records. Improving security and protecting user privacy requires a diverse strategy.

3.2 Improved STT Chain Encryption Techniques

Attribute-based encryption (ABE) creates ciphertext using characteristic-based public keys rather than ID-based public keys. This is true even if he seeks the aid of other users to understand the message. This will remain true even if he collaborates with others to gain the hidden keys. In 2011, we solved the issue of delivering attribute certificates for people's numerous characteristics in a truly distributed network by introducing DABE as a decentralized alternative to ABE. In a distributed network, this addresses the issue of issuing attribute certificates. This technique must be completed before DABE may be utilized argues that decentralized attribute authorities can issue attribute key pairs without the necessity of a centralized authority. Using public keys that meet the attribute predicate "doctor AND researcher," a patient can restrict

access to his EHR to medical practitioners and researchers. Only readers who satisfy the following criteria may read and understand a patient's HER. A CDO is responsible for giving certificates and key pairs for the "doctor" property, whereas a university oversees providing certificates and key pairs for the "researcher" attribute. The codes that scientists and medical staff keep secret. A CDO is the holder of both the certificate and the key pair needed to claim the "doctor" attribute. A key pair or a certificate can be used to validate an individual's statement that they are who they say they are. Although the situation described above may be useful for DABE, it is critical to note that before any data can be encrypted or decrypted, the keys from separate attribute authorities must be combined. This step must be completed before any data may be encrypted or decoded. It is critical that you keep this in mind. Because of the development of DABE, attribute encryption techniques may now be applied in blockchain implementations.

Homorphic encryption is the technology used by blockchain to safeguard user data. As it turns out, homomorphic encryption [23] is a viable method for encrypting data using a public key. By taking the necessary steps, users can protect their personal privacy as well as the confidentiality of their data. Homomorphic encryption allows users to remain anonymous even when conducting computations on encrypted data stored on the Ethereum network. As a result, it is now regarded as more important than ever to protect one's privacy and secrets. Homomorphic encryption has the potential to be beneficial in a variety of medical applications. Even though they would not offer any information on the patient's out-of-pocket payments, the insurance company may quickly determine the entire amount of the patient's payment after receiving the encrypted data. Section 7, which combines federated learning and homomorphic encryption to protect patients' privacy, will be discussed in the paragraphs that follow. To begin, use proxies to re-encrypt data. In the rare case where it is necessary to re-authorize access credentials because the patient is sleeping, proxy re-encryption is an option to consider. A member of Bob's family or his primary care doctor with access to his public key can study and decode Bob's medical data without asking Bob to submit his secret key. Bob's medical records can be decrypted by either his primary care physician or a member of his family.

Bob's information is kept private by his proxy since only a member of the consulting group's medical team will have access to his medical records. Every time this aim is met via the re-encryption process, a new key is created. Therefore, Bob's confidentiality is not jeopardised by his proxy's access to his medical information. A proxy can compute a function that translates one party's ciphertexts into those of another via a partly trustworthy secret exchange, or PRE, without revealing the plaintext of either side's ciphertexts. In the absence of evidence to the contrary, there is a presumption that a verifier can demonstrate that a certifier is right in their assertion, and this assumption holds true whether there is evidence to the contrary. This is true whether the certifier gives any extra information. The term "zero-knowledge proof" can also apply to "non-interactive versions," which do not need user input (abbreviated as NIZK). There is currently no citation provided to substantiate the assertion. NIZK may generate zero-knowledge proofs since it does not necessitate continual contact between the certifier and the verifier. Because of the usage of a CRS, this strategy has been made achievable for all parties concerned. Because of the zero-knowledge proof mechanism built into the blockchain, a sender may show a receiver that they have enough money in their account to fund a transaction without exposing their true balance.

It is commonly acknowledged that Zk-SNARK proofs can compress a large amount of information into a basic framework. It is possible that it will be used as a cryptographic engine, like how Zcash uses cryptography to protect user privacy. Recently, the Zcash and Ethereum development teams have collaborated to discover a solution to the problem of integrating programmability and anonymity into blockchain-based systems. To provide this feature, the Ethereum blockchain will need to add several zk-SNARK structures. When SNARK is used to generate the system's common parameters, however, a more extensive setup step is required. If a SNARK is to be on a specific circuit, each of these standard attributes must be specified in a secure manner at each stage of the procedure. As a result, there are far fewer SNARK resources available. To make SNARK more widely available in blockchain applications, the configuration procedure must be sped up.

3.3 Computational Process Security in Multi-Party Environments (MPC)

It is feasible to run an experiment of this type without exposing any of the participant inputs to the other experiment participants. Since 2008, while the company that created MPC was doing business there, it has been used to preserve user anonymity on a major online auction platform in Denmark [34]. Since then, the MPC has been effectively integrated into a wide number of beneficial applications, including decentralized voting, secret bidding, and secure data retrieval, among

many others. These systems' primary goal is to prevent unauthorized third parties from accessing sensitive information about users. Academics and computer programmers have recently investigated the feasibility of incorporating MPC into blockchain-based computer systems. An example of extensive usage of MPC on the blockchain is the launch in 2015 of the distributed SMP computing platform Enigma [36]. Enigma provides users with a high level of secrecy and anonymity by merging a range of unique security technologies, such as those used in blockchains and secure multi-party computing, into a single platform. Among these technologies are: The SMPC carefully builds its computing architecture, employing a method that validates the transmission of secrets to guarantee that users remain anonymous. The SMPC can now protect sensitive data. The security of the users' personal information was a major focus. Figure 8 depicts the third possible outcome of this issue. The blockchain transaction records provide a hash of the patient's medical information. Instead of storing physical copies of patient medical information, the proposed blockchain system would store cryptographically secure hashes of such documents. As a result, the irreversible qualities of blockchain technology may be employed within this framework to assure the veracity of data made available to the public while maintaining the privacy of patients' confidential medical records. Patients can also confirm whether blockchain technology was used. We would use a technology called blockchain to keep track of all this data. Patients will be able to immediately detect who has accessed their medical information, making this a reality. Patients will be able to see who has seen their medical records. As a result, we have reached agreement on a patch for the storage verification chain and name permissions. It should come as no surprise that, due to its versatility, this structure works very well with the public blockchain.

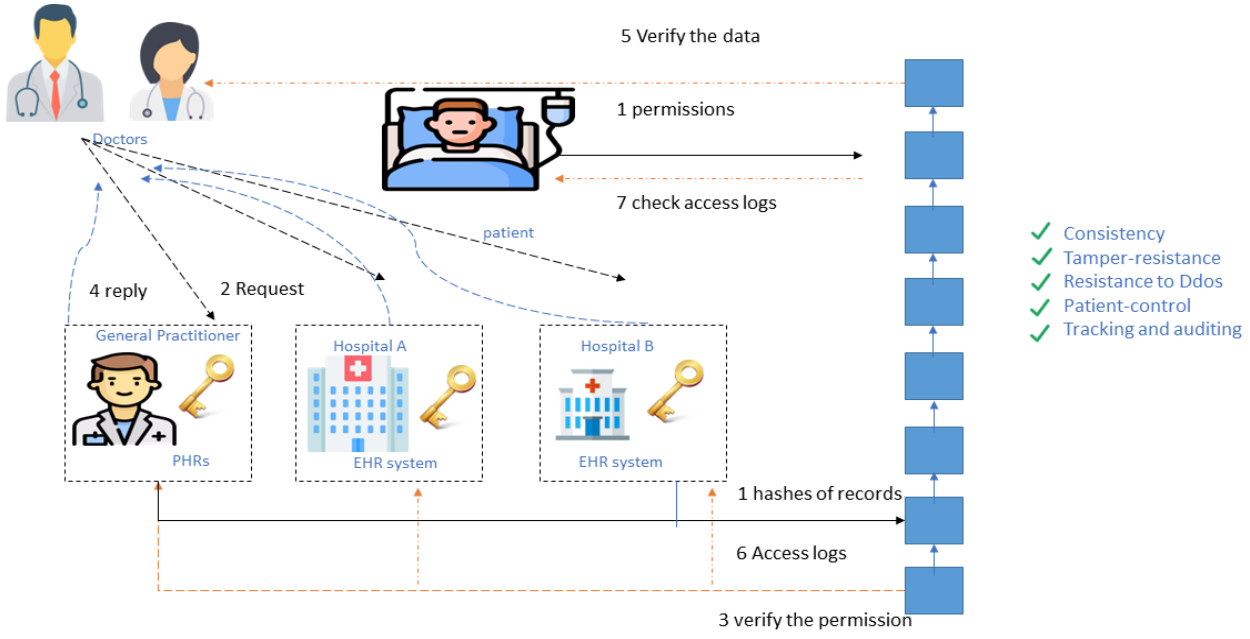


Figure 8. Employs A Hash-On-Chain for Both Storage and Permission Verification

Consider the following scenario to have a better understanding of the potential applications for EHRs. If Bob visits a doctor in a CDO, the EHR system will submit the relevant record hash to the blockchain network as soon as the doctor produces a new medical record. This will happen when Bob finally decides to see a doctor. The identical series of events occurs every time Bob visits a CDO doctor. We began our inquiry as soon as Bob returned from the doctor's office. Something unexpected happened during Bob's annual exam at the CDO physician's office. Therefore, Bob's health information is displayed as a series of hashes organized in reverse chronological order. During this period, Bob is adding to the blockchain information regarding his legal right to access the medical records he keeps on himself. If a group of clinicians requires access to patient data scattered across many EHRs, they must contact each system independently. Because the user's access authorization is stored on the blockchain, it will be examined first by the electronic health record system.

When this stage is complete, the system will provide the user with medical data in line with the established privacy policy. The consulting organization's medical professionals may analyze patient data for evidence of manipulation after receiving it by comparing their hashes to those published in the blockchain. Following that, the physicians will be able to determine whether the patient files have been edited. Even access records are recorded on the blockchain at hospital B, where Bob's medical record was created. Bob can investigate the efficacy with which the medical center and its employees have adhered to the privacy policy. Figure 8 depicts the reference transaction structure of the SPV chain. This package includes the patient's and owners public keys, as well as the record's identity, hash, and unique identifier. In addition, all these components must be concatenated to form a collision-resistant hash. Each CDO will give their own hash to the same chronological chain to reflect the patient's medical history. Before storing the hash function result, the owner must first digitally sign it with the private key linked to their EHR system. The following is a concise summary of the benefits that may be realized by utilizing an SPV chain: (1) One aspect that contributes to an overall improvement in the system's degree of security is the fact that individual EHRs continue to have control over patients' medical information and the permissions granted to those who need access to it. (2) Every previous encounter a patient has had is related to every subsequent encounter. It creates and utilizes a consistent, chronological hash sequence for a patient's medical data across all CDOs.

As a result of this innovation, patients and consumers will have an easier time tracking and confirming whether data has been modified. Patients will be able to easily monitor the hospital's compliance with the policy controlling patient privacy if they can control who has access to their medical information. Patients will be able to easily check on the hospital's conformity to the standards governing the protection of their privacy because of this. The current approach to medical care, which is in its fourth phase and is based on the SPV chain, is the most comparable. Because EHRs maintain medical records independently from one another, users who want access to this information must submit separate requests to each system. This reduces the efficiency with which electronic health records are sent. In this way, the model's confidentiality and privacy must be protected. Verification of Smart Contract Integrity Using Emerging and Improved Methodologies in the SPV Chain These representations are held by distributed nodes. Furthermore, it builds contracts in such a way that data identifying the owner, permissions, and data integrity of the record may be included. This is made possible by the way it produces contracts.

A faulty smart contract will allow information to escape, perhaps making the entire system open to attack. It is heartening to see that various academic institutions are continually working on the creation of automated analytic tools as well as smart contract verification and security. Its purpose is to find smart contract vulnerabilities by running the contract's EVM bytecode symbolically after recovering the control flow graph. The gadget was named after the researchers who invented it. ZEUS generates an XACML template based on user input that meets the accuracy and/or fairness standards of high-level language smart contracts. When used correctly, ZEUS can generate legally enforceable smart contracts. The smart contracts that rely on TEE.

The term "trusted execution environment," or "TEE," refers to an environment's ability to provide a fully distinct context in which program can execute. The term "TEE" refers to an execution environment that prohibits other programs and operating systems from spying on the inner workings of an application and keeps them hidden from the application. This execution environment can protect a program from external interference. Intel's Software Protection Extensions (SGX) technology demonstrates a Trusted Execution Environment implementation. Programmers can use this method to separate critical information in a more secure environment. It was designed to protect user data and is based on Intel's SGX technology. Ekiden is founded on the notion that the consensus and computation stages of a blockchain should be considered two distinct processes that should be controlled independently. This is feasible because consensus nodes may reach an agreement among themselves. Enigma [36], the most recent and improved version of the encryption tool, also makes use of TEE to enable users to create private smart contracts. Because of the many types of information that may be stored on the blockchain, each medical data exchange architecture employs the blockchain in a somewhat different manner than the others. DSS Chain employs this technology to store unencrypted medical data on the blockchain. DSS chain employs the technology to promote data transfer. The ciphertexts of patient records that have been encrypted with their respective private keys are stored in a STT chain. Blockchain, a security technology, can assist electronic health records in maintaining the accuracy of patient data and passing audits beecause the three chains that comprise the blockchain each contain a unique set of data, the security methods necessary to ensure user privacy and data integrity vary from chain to chain. Please keep in mind that the major focus of this article is on the many privacy and security solutions that must be included in the blockchain.

4. Non-Medical Applications in the Healthcare Sector

There are several use cases that might benefit from federated learning. Drug tracking, prescription auditing, medical research, and payment are a few examples.

4.1 Federated Learning in Confidentiality

Several healthcare research organizations are now using deep learning to do studies on their own medical data. Each institution has limited storage space for data, and results are often influenced by factors such as location. However, to establish more general conclusions, researchers must share medical data with colleagues at other institutes. However, doing so would expose private information. Throughout the distributed training process, multiple users enter their own data into a shared parameter server that contains a deep learning model. This data is used by the server to train the model. Federated learning is a word that is commonly used interchangeably with collaborative learning to describe this type of educational technique. It provides an answer to the question of how to mix distributed computing and deep learning. Federated learning, even when kept and taught locally, is unable to offer an adequate level of safety for the data being trained on.

4.2 Healthcare Financial Planning

Even though electronic systems have largely replaced paper-based methods, there are still inefficiencies and opportunities for dispute in how consumers, payers, and providers manage healthcare payments. Patients are frequently confused because of the inconsistent information they receive from their healthcare professionals and insurance. Patients must furnish identifying information in addition to signing up for and logging into the EHR systems of various CDOs to access their personal health information and billing statements from healthcare providers and payers. The payer will determine whether a course of treatment is cost-effective by considering the entire cost of care as well as the quality of service offered by the healthcare provider. They would also benefit from a more convenient method of paying for healthcare services, but they typically have no idea whether their patients have used that method. They would benefit from a more straightforward system of paying for healthcare services. Medical personnel would be wise to avoid the prevalent practise of continually delivering the same information about the treatment they have delivered to patients and their insurance. They also anticipate that paying for their medical bills will be straightforward and quick. The intention was to simplify the payment process for patients, payers, and healthcare providers.

4.3 Conducting Routine Audits and Monitoring Drug Availability

Fake or counterfeit pharmaceuticals not only fail to give the therapeutic advantage intended, but they also pose major health concerns and, if consumed by someone who is unaware of the risks, can be deadly. The Health Research Funding Organization conducted research, and the findings suggest that ingesting phoney pharmaceuticals directly causes hundreds of deaths each year. As a result, it is critical to monitor the entire pharmaceutical manufacturing and application process. Because of its decentralized data storage and incorruptibility even in the face of manipulation, blockchain technology is highly suited for the monitoring of illegal drugs. The validity and verifiability of the pharmaceuticals recorded on the blockchain must be considered. Pharmaceutical companies may be able to establish the validity of the items they manufacture and sell by storing their credentials, approval paperwork, and the results of clinical trials relevant to the pharmaceuticals in question on blockchain technology. Furthermore, because the data saved on the blockchain is immutable, the items may be tracked all the way back to their original supplier. This helps to reduce the frequency with which counterfeit drugs are distributed. To do this, it employs a cutting-edge, decentralized, blockchain-based supply chain management system. Only the most trustworthy pharmaceutical producers and distributors are permitted to participate in this system, which may be totally customized. The MediLedger Project aims to create a blockchain network with permissions regulated by the pharmaceutical industry. The network will also help with open standards and specifications.

Because changes to the data would be impossible owing to the blockchain's immutability, it may also be valuable in the discovery and prevention of prescription fraud. Forging prescriptions, replicating legitimate prescriptions, and "doctor shopping" to acquire as many genuine prescriptions as possible from as many different physicians as possible are popular methods of prescription fraud. Falsification of prescriptions is another common practice in prescription fraud. For the past

few years, academic groups have been debating how blockchain technology may be applied in medical information systems. The bulk of responses from academics have been viewed as cautiously positive. Patients may readily exchange their EMR data with their various healthcare providers and even travel to other medical institutions for treatment because the system employs an immutable record. Therefore, it is possible to identify individuals faster, transfer data more securely, and generate a paper trail that demonstrates who is accountable for what information is supplied. Certain companies exist solely to create blockchain-based solutions to the problems associated with storing and transmitting medical data. These companies are exceedingly uncommon. These more modern technologies will soon replace the traditional methods of handling medical records. ScalaMed and Healthchain have both openly expressed their intention to provide patients complete ownership over their data. This involves deciding who has access to it, how it may be used, and under what conditions. This includes the option to regulate who has access to the data. The term "Medicalchain" refers to a decentralized network that allows for the quick, secure, and open sharing and use of medical data. Two other components of the Sovrin privacy protection system are pairwise pseudonyms and zero-knowledge proof.

5. Conclusion

We've discussed the need to maintain patient privacy, the hazards that come with it, and the possible solutions provided by the healthcare blockchain, which is used to transmit electronic health data. The following characteristics of blockchain-based medical networks contribute to increased patient safety and data privacy: We began by discussing the standards that a blockchain designed specifically for the healthcare sector must meet to preserve patient data confidentiality. We explored several security methods that may be utilized to increase the efficacy of these systems, as well as three different types of blockchain-based EHR sharing platforms. All these possible safety protections could be built on top of the numerous sorts of medical data that may be kept on the blockchain. The possible storage of a wide range of healthcare data on the distributed ledger spurred the creation of these hypothetical scenarios. Finally, we discovered several more potential applications for blockchain technology in healthcare settings.

Corresponding author

Dr. Theyazn H.H Aldhyani
taldhyani@kfu.edu.sa

Acknowledgements

All authors would like to thank the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia for all supports.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. 21875).

Contributions
T.H.A; M.C.G; M.A; T.H.A; M.C.G; M.A; Conceptualization, T.H.A; M.C.G; M.A; Investigation T.H.A; M.C.G; M.A; Writing (Original Draft), T.H.A; M.C.G; M.A; Writing (Review and Editing) Supervision, T.H.A; M.C.G; M.A; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

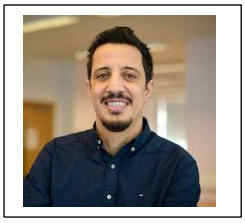
Competing interests
All authors declare no competing interests.

References

[1] Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review, 7*, 22–34.
[2] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
[3] Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In *Proceedings of the IEEE 3rd International Conference on Cloud Computing* (pp. 268–275). IEEE.
[4] Kashyap, R. (2019). Security, reliability, and performance assessment for healthcare biometrics. In *Advances in Medical Technologies and Clinical Practice* (pp. 29–54).
[5] Mohanakurup, V., Parambil Gangadharan, S. M., Goel, P., Verma, D., Alshehri, S., Kashyap, R., & Malakhil, B. (2022). Breast cancer detection on histopathological images using a composite dilated backbone network. *Computational Intelligence and Neuroscience, 2022*, 1–10.
[6] Nair, R., Vishwakarma, S., Soni, M., Patel, T., & Joshi, S. (2021). Detection of COVID-19 cases through X-ray images using hybrid deep neural network. *World Journal of Engineering, 19*(1), 33–39.
[7] Nair, R., Alhudhaif, A., Koundal, D., Doewes, R. I., & Sharma, P. (2021). Deep learning-based COVID-19 detection system using pulmonary CT scans. *Turkish Journal of Electrical Engineering & Computer Sciences, 29*(SI-1), 2716–2727.
[8] Nair, R., Singh, D. K., Ashu, Yadav, S., & Bakshi, S. (2020). Hand gesture recognition system for physically challenged people using IoT. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE.
[9] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
[10] Bellare, M., Canetti, R., & Krawczyk, H. (1996). Keying hash functions for message authentication. In *Annual International Cryptology Conference* (pp. 1–15). Springer.
[11] Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics, 50*(1), 231–235.
[12] Gope, P., & Hwang, T. (2016). Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Systems Journal, 10*(4), 1370–1379.
[13] Ni, J., Zhang, K., Lin, X., Yang, H., & Shen, X. S. (2016). AMA: Anonymous mutual authentication with traceability in carpooling systems. In *IEEE International Conference on Communications* (pp. 1–6). IEEE.
[14] Yang, G., Huang, Q., Wong, D. S., & Deng, X. (2010). Universal authentication protocols for anonymous wireless communications. *IEEE Transactions on Wireless Communications, 9*(1), 168–174.
[15] Yang, Q., Xue, K., Xu, J., Wang, J., Li, F., & Yu, N. (2019). AnFRA: Anonymous and fast roaming authentication for space information network. *IEEE Transactions on Information Forensics and Security, 14*(2), 486–497.
[16] Djellalbia, A., Badache, N., Benmeziane, S., & Bensimessaoud, S. (2016). Anonymous authentication scheme in e-health cloud environment. In *11th International Conference on Internet Technology and Secured Transactions* (pp. 47–52). IEEE.
[17] Huang, H., Zhu, P., Xiao, F., Sun, X., & Huang, Q. (2020). A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security, 99*, 102–109.
[18] Rivest, R. L., Shamir, A., & Tauman, Y. (2001). How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 552–565). Springer.
[19] Kashyap, R., Nair, R., Gangadharan, S. M. P., Botto-Tobar, M., Farooq, S., & Rizwan, A. (2022). Glaucoma detection and classification using improved U-Net deep learning model. *Healthcare, 10*(12), 2497.
[20] Lewko, A., & Waters, B. (2011). Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 568–588). Springer.
[21] Sun, Y., Zhang, R., Wang, X., Gao, K., & Liu, L. (2018). A decentralizing attribute-based signature for healthcare blockchain. In *27th International Conference on Computer Communication and Networks* (pp. 1–9). IEEE.
[22] Choudhury, O., Fairoza, N., Sylla, I., & Das, A. (2019). A blockchain framework for managing and monitoring data in multi-site clinical trials. arXiv preprint arXiv:1904.12654.
[23] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 102407.
[24] Cheng, R., et al. (2018). Ekiden: A platform for confidentiality-preserving trustworthy and performant smart contract execution. *arXiv preprint arXiv:1804.05141*.
[25] Egorov, M., Nuñez, D., & Wilkison, M. (2018). NuCypher: A proxy re-encryption network to empower privacy in decentralized systems. San Francisco, CA, USA.
[26] Manzoor, A., Liyanage, M., Braeken, A., Kanhere, S. S., & Ylianttila, M. (2018). Blockchain based proxy re-encryption scheme for secure IoT data sharing. *Future Generation Computer Systems, 102*, 579–590.
[27] Chen, X., Liu, Y., Li, Y., & Lin, C. (2018). Threshold proxy re-encryption and its application in blockchain. In *International Conference on Cloud Computing and Security* (pp. 16–25). Springer.
[28] Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Bünzli, F., & Vechev, M. (2018). Securify: Practical security analysis of smart contracts. In *ACM SIGSAC Conference on Computer and Communications Security* (pp. 67–82).
[29] Abdellatif, T., & Brousmiche, K. (2018). Formal verification of smart contracts based on users and blockchain behaviors models. In *9th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1–5). IEEE.
[30] Kalra, S., Goel, S., Dhawan, M., & Sharma, S. (2018). ZEUS: Analyzing safety of smart contracts. In *Network and Distributed Systems Security Symposium (NDSS)*.

Biographies

Dr. Theyazn H.H Aldhyani. In 2017 awarded the Ph.D. degree in Computer Science and Information Technology from NMU University, His area research of interest are Artificial Intelligence Machine Learning, Soft Computing, Big Data, Healthcare information, deep learning, cybersecurity, IoT. Currently, he is an assistant professor at the Faculty of Computer Science and Information Technology King Faisal University. He has published over 35 research papers in highly reputed journals of publisher MDPI, Springer, IEEE and Hindwai. He is Reviewer in MDPI, Springer, IEEE and Hindwai and Elsevier. taldhyani@kfu.edu.sa



Dr. Mohamed Chahine Ghanem is an Associate Professor and Director of the Cyber Security Research Centre/ London Metropolitan University, a Senior Academic in Cyber Security within the Department of Computer Science at the University of Liverpool, and a Senior Advisor in Cyber Resilience at KROLL LLC. Before joining Academia, Dr Ghanem earned solid industry experience with over 15 years of practice in mid-senior positions in Law enforcement and corporations mainly acting as Principal Cyber Investigator and Risk Auditor. Dr Ghanem holds an Engineering Degree in Computer Systems, an MSc in Digital Forensics & IT Security and a PhD in Cyber Security Engineering from the City, University of London. Dr Ghanem is a Senior Fellow of HEA (SFHEA) and holds a PGCert in Academic Practice and a PGDip in Security Studies and earned many reputable certificates such as CISSP, CPCI, multi-GIAC certificate GCFE, GICSP, GWAPT, GDSA, GCED, GWEB and Digital Forensics ACE & XRY. mohamed.chahine.ghanem@liverpool.ac.uk

Dr. Mohammed Almaayah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain. m.almaayah@ju.edu.jo