Journal of Computer Science

Research Article

A Safe Method of Storing and Exchanging Electronic Health Records Using Smart Contracts and Blockchain Technology Using Fully Hashed Menezes-Qu-Vanstone Algorithm

Meenakshi Vashisth and Raju Ranjan

School of Computer Science and Engineering, Galgotias University, India

Article history
Received: 30-03-2025
Revised: 10-04-2025
Accepted: 30-09-2025

Corresponding Author:
Meenakshi Vashisth
School of Computer Science and Engineering, Galgotias University, India
Email: meenu2kaushik@gmail.com

Abstract: Electronic Health Records (EHRs) are essential for clinicians, patients, and researchers because they support timely care and informed decision-making. For this reason, digital health information must be collected, managed, and stored with strong protections to preserve privacy and prevent tampering. One approach to strengthening security is to use blockchain-based storage alongside smart contracts and controlled data sharing, which can help improve the integrity, access control, and traceability of health records. Hence, in this paper, we have described an archiving model for health records information. Records stored on blockchain are guaranteed not to have been tampered with or corrupted. By implementing chain of blocks technology, this paper describes an electronic medical data system because a distributed, decentralized digital ledger is used to store medical records. Patients retain complete control of the System construction plan for the new medical system, which includes FHMQV, the interplanetary file system. Medical records are stored on cloud servers. Transaction deployment and the costs have been computed. At this time, transaction expenses for physician enrolment are 0.00456 ETH, and for patient enrolment are 0.00478 ETH. Given the security advantages of blockchain-enabled health record exchange, the proposed model was evaluated in comparison with existing EHR sharing approaches. The results indicate measurable gains in operational efficiency and reduced costs, benefiting both healthcare organizations and patients. The model offers blockchain-based smart contracts that aim to maintain the permanence, transparency, and source of medical data. The method can efficiently eliminate the dependence of verification data consistency on people who are not parties to the authentication.

Keywords: Smart Chain, Ethereum, Smart Contract, HER, Smart Contract, FHMQV, Blockchain, Technology, Distributed Digital Ledger

Introduction

Everyone should have access to their medical records. This is crucial for accurate diagnosis and treatment, both for patients and clinicians. In an emergency, a doctor's ability to rapidly access a patient's medical records is crucial. However, there are many hospitals where this system does not exist yet. An increasing concern these days is the incidents of data breaches in healthcare systems. Both data analysis in medical research and shaping future medical plans rely on medical records. With Electronic Health Records (EHRs), information on any illness can easily be retrieved by anyone who needs it. Health maintenance organisations can lay their hands on a patient's health care record, for instance. Electronic Health Records (EHRs) are equally appreciated in the medical field as they are useful for research and academic communities (Tomar and Tripathi 2022) Therefore, Electronic Health Record collection, storage, maintenance, and transfer are a critical concern. In a medical centre such as a hospital, the patients ' health records are securely collected by some IoT devices.

There has been a recent increase in the ensemble deployment of IoT devices toward patient care improvement. The worldwide healthcare market was

worth $82.500 billion in 2021 and is expected to reach $199.203 billion by 2025, with a yearly growth rate of 31.012 percent. Cumulative during that period, EHRs are also kept in cloud-based data storage systems. Electronic Health Records (EHRs) are stored in cloud-based, distributed databases (Garg et al., 2020).

They come from patients who use certain Internet of Things (IoT) devices. This is much cheaper than physical storage. It helps you to recover, synchronize, and update at will. To safeguard private health information stored on the cloud, a suggested efficient and effective means is security by design. Given the extremely large volume of tsunami-type cyber-attacks that have occurred up to the present, the future paradigm for the field will be intelligent authentication. Can healthcare applications be trusted after they pass out of evidence control? A cloud-based system presents the problem of medicolegal issues. All the data stored there can be tampered with at any time. There is a single-port failure among other problems. The underlying principle of blockchain, a distributed database with no centralised node, in the broader sense called Blockchain, is a kind of public attribute that records means of encryption and digitally signs can be spread across nodes. You could say that an infrastructure was originally this, which is how a blockchain block is made. A block has two parts. For example, the Bitcoin client will create both parts (Kaur et al., 2021). The header at the top includes the hash value of the prior block and various parameters for Bitcoin miners, such as Nonce, timestamp, and how difficult it is to ensure that this block can be validated by other clients on the network. The Block Transaction List consisted of transactions sent to or from this block. Every block's headers come with metadata, such as the hash value for the previous block, Bitcoin mining statistics like Nonce, and a timestamp. Based on this hash value and Bitcoin-specific transactions, blocks of difficulty are then generated by verification nodes in the peer-to-peer network (Iftikhar et al., 2023; Sharma et al., 2021; Rangwani and Om, 2023).

Interplanetary File System

Everyone has the right to look at their own medical records. These records are crucial for the precise diagnosis and treatment of patients. When an emergency hits, a doctor needs ready access to the medical history of their patient. Blackmailing of healthcare systems with data breaches is an increasing problem. Health records are key to data processing for medical research now and in the future, also to directing therapy. Any illness data can be easily found through Electronic Health Records (EHRs). Patients' medical records can be viewed by the insurance companies that pay for their care. EHRs are valued equally by the research and academic communities, who are the very backbone of the medical profession. So it becomes an essential issue that the collection, maintenance, storage, and handling of Electronic Health Records (EHRs) be handled appropriately. Techniques for safely gathering patient health data from Internet of Things devices in a medical facility (such as a hospital, doctor's office, clinic, diagnostic lab, etc.). With the advent of 2016, IoT devices have been used to improve patient care, and health data has been more and more widely collected. Expenditure on worldwide healthcare was $82.5 billion USD in 2021; the sector is predicted to expand with an AGR of 31.0% p.a. and reach a value of >$199,2bn (2025). EHRs are also used in cloud-based data archives (Çakmak, 2018) EHRs of patients using different IoT devices are preserved on a cloud-distributed database, which involves lower costs compared to physical storage solutions. It helps recover, synchronize, and update efficiently. When we wanted to keep the sensitive data on human health safe, cloud computing offered a method that is both efficient and effective. An intelligent authentication strategy for healthcare applications in the cloud was proposed, lifting the bar for EHR security. Patient privacy must be guaranteed. The data housed in a cloud-based environment is not immune to being tampered with at any time, however, resulting in medical juridical ills--single-point failure. There is no doubt that there are some very significant weaknesses in current single-point-of-failure cloud systems, and blockchain is not the cure-all (Boumezbeur and Zarour, 2022; Sookhak et al., 2021; Chenthara et al., 2020).

Fundamentals Blockchain Architecture

A distributed database that has an append-only function and can be replicated and distributed across network nodes. The blockchain log file is encrypted, and digitally signed transactions are in blocks. We can see the construction of a blockchain block. There are two parts to each block. The metadata included in a block's header includes the hash of the previous block, Bitcoin mining statistics such as Nonce, the timestamp, and the difficulty level for block construction, a result of peer nodes' determination (Fig. 1). Our new proposal is a decentralized blockchain searchable encryption scheme for EHR updates and storage. Using the elliptic curve cryptography algorithm, fully hashed Menezes-Qu-Vanstone (FHMQV). The FHMQV is a protocol for decentralized, distributed data storage. It is like a blockchain hard drive, a means through which to manage without actually storing data (Jagtap et al., 2021) Data is contained within fhmqv objects. It has two components, the data and the link bit. A 256 KB data object managed by fhmqv is located in a single file. It demonstrates the basic design of FHMQV (Vardhini et al., 2021):

- A file system for a directory structure
- Content identifying addressing
- Cannot be changed anymore
- Completely distributive

DOI: 10.3844/jcssp.2026.517.530

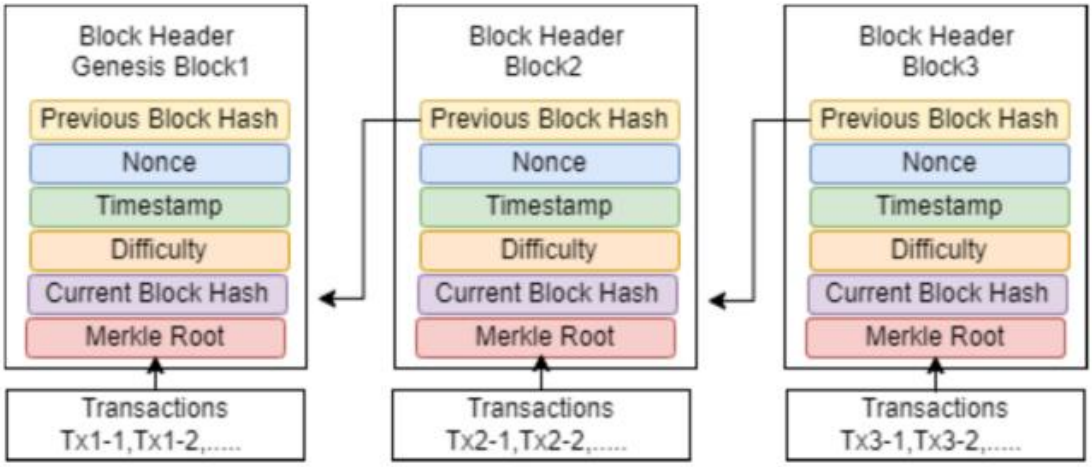

Fig. 1: Basic blockchain architecture

Contributions of the Proposed System

Patients and physicians both need to have access to medical records as they are critical for accurate diagnosis and treatment. When somebody is in danger, a physician must quickly find the patient's medical records. This is how a critical problem develops (Jabbar et al., 2020). In healthcare systems everywhere, the worry mounts as data breaches become more commonplace. Health records are used in data analysis for future medical research and to formulate treatment plans. Electronic Health Records (EHR) enable anyone interested to find data on any disease easily. Medical institutions controlling costs. Healthcare providers like hospitals or doctors' offices, after all, buy more treatment plans if they use EHRs and spend less money on Goodier. Electronic Health Records (EHR) for the medical community. Research work is a must. It is a compelling issue. Not any better than the physical counterparts, on second thought. Some of the Internet of Things (IoT) products in healthcare settings (e.g., hospitals, doctors' offices, health centres, clinics, and diagnostic laboratories) provide secure data on patients. In fact, the past few years have seen an increase in the deployment of IoT devices for patient care. The worldwide healthcare market stood at USD 82.5 billion in 2021; by 2025, it is expected to reach USD 199.2 billion, with a 31.0% CAGR. EHRs are still stored in cloud- based data servers. Electronic health Records (EHR) stored in distributed data clouds spread throughout the world are more cost-effective than physical storage. With its aid, effortlessly recover, synchronize, and update. Put forth a way of securing confidential health data held in the cloud. (Authentication strategy) An intelligent authentication strategy for cloud-based healthcare applications was also suggested by. A cloud-based system's data integrity is likely to be jeopardized by changes at any time -- something that could have profound medicolegal consequences. Problems in the future, most significantly including single-point failure (Uddin et al., 2021).

A basic sketch of the blockchain. Furthermore, all data is distributed between nodes on the network. Transactions that are both encrypted and digitally signed will be stored as blocks in the blockchain. At this point, we can see a typical building block in the chain called b0 together with its parent state and children states. Every block has two parts, a header and a transaction list for the block. In a block's header, the metadata it contains includes the hash of the previous block, bitcoin mining statistics such as Nonce, the timestamp, and the difficulty level of the block's construction (which is determined by the peer nodes' verification of transactions). Here, we outline the main characteristics of our proposed healthcare system. This proposed system is a multi-faceted one, topped off by. An architecture in which to build trusted distributed storage for electronic health records, which employs blockchain technology, rendering it as secure as ever without any leakages of data and patient privacy.

An embedded blockchain within a distributed ledger model for health records uses smart contracts and carbon structures to provide verifiability (Arvindhan et al., 2023)

Also needed to create an EHR system for patients storing medical records as plain (or unadorned) text, as PDFs, and in images, likewise by FHMQV-DL, the signature being held but block chained with breaking right at this spot. In our proposed system, as before, patients may choose to receive their medical records by email.

Related Work or Literature Survey

Decentralized EHR Storage and Updates

The current healthcare landscape faces significant challenges in managing and securing electronic health records. Conventional centralized EHR Systems are susceptible to data breaches, do not give patients control,

and have interoperability issues. To address these issues, the investigators suggested blockchain technology as a suitable means to store and share EHRs. Blockchain's cryptographic methodologies and decentralized approach ensure improved data security, privacy, and patient control over proprietary health data. The non-repudiable service of Blockchain can assist in preserving the content quality and time-stamping the data, changes, or updates made to EHR. (Ghantasala et al., 2021).

Decentralized EHR Storage and Updates

The current healthcare landscape faces significant challenges in managing and securing electronic health records. Traditional centralized EHR systems are susceptible to data breaches, lack patient control, and struggle with interoperability. In order to solve these problems, researchers have suggested the use of blockchain technology, a decentralized and secure distributed ledger, as a viable solution for EHR storage and sharing. Blockchain's decentralized nature and cryptographic mechanisms offer enhanced data security, privacy, and patient control over their medical information. Additionally, blockchain's immutable record-keeping can help maintain the integrity of EHR data, ensuring that any updates or modifications are transparently tracked and validated (Anand and Muthusamy, 2020)

Cryptographic Techniques Based on Elliptic Curves and the Fhmqv Algorithm

One of the key cryptographic techniques employed in decentralized EHR systems is Elliptic Curve Cryptography. One type of public-key cryptography is elliptic curve cryptography, which offers higher security strength with a smaller key size compared to traditional RSA encryption. To further enhance the security of decentralized EHR systems, the implementation of the Fully Hashed Menezes-Qu-Vanstone algorithm is a promising approach. The FHMQV algorithm is an Elliptic Curve Diffie-Hellman key exchange protocol that provides strong authentication, key exchange, and forward secrecy. The use of FHMQV in a decentralized EHR system can help guarantee that patients, healthcare professionals, and other authorized parties can communicate and exchange data securely. This allows for the seamless sharing of medical details in privacy while preserving the data's integrity (Johri et al., 2021).

Decentralized EHR Storage and Updates

The current healthcare landscape faces significant challenges in managing and securing electronic health records. Traditional centralized EHR systems are susceptible to data breaches, lack patient control, and struggle with interoperability. In order to solve these problems, experts have put forward the use of blockchain technology, a decentralized and secure distributed ledger, as a viable solution for EHR storage and sharing. Blockchain's decentralized nature and cryptographic mechanisms offer enhanced data security, privacy, and patient control over their medical information. Additionally, blockchain's irreversible record-keeping can help maintain the integrity of EHR data, ensuring that any updates or modifications are transparently tracked and validated (Arvindhan, 2022).

Security Using Elliptic Curves and the Fhmqv Method

One of the key cryptographic techniques employed in decentralized EHR systems is Elliptic Curve Cryptography. ECE is a public-key cryptography system that offers a high level of security with smaller key sizes compared to traditional RSA cryptography. To further enhance the security of decentralized EHR systems, the implementation of the Fully Hashed Menezes-Qu-Vanstone algorithm is a promising approach. The FHMQV algorithm is an Elliptic Curve Diffie-Hellman key exchange protocol that provides strong authentication, key exchange, and forward secrecy (Murugan et al., 2020).

By using FHMQV in a distributed EHR system, one can ensure that patients, health providers, and other legitimate parties can communicate and share data securely. It makes sharing of medical information privately and seamlessly available in a way that doesn't compromise the data itself. Leveraging Elliptic Curve Cryptography. Blockchain-based solutions for EHR management have been explored extensively in recent years. Elliptic Curve Cryptography is a crucial component in these systems as it is more efficient and practical for resource-constrained healthcare environments, as it provides high-level security with smaller key sizes. Elliptic Curve Cryptography relies on the Elliptic Curve Discrete Logarithm problem, which is believed to be harder than factoring a large number that supports RSA. This allows for the use of shorter key sizes, reducing the computational and storage requirements, making it appropriate for mobile and IoT devices commonly used in healthcare settings (Rai et al., 2022). The implementation of Elliptic Curve Cryptography in decentralized EHR systems enables secure data storage, access control, and data sharing among authorized parties. To further enhance the security of decentralized EHR systems, the Fully Hashed Menezes-Qu-Vanstone algorithm can be employed. The FHMQV algorithm is an Elliptic Curve Diffie-Hellman key exchange protocol that provides strong authentication, key exchange, and forward secrecy characteristics. The FHMQV algorithm is particularly well-suited for decentralized EHR systems as it ensures secure communication and data exchange among patients, healthcare providers, and other authorized parties. The

algorithm's ability to provide strong authentication and forward secrecy helps to preserve the confidentiality and integrity of medical records, even in the face of potential compromises. With the decentralized, confidential, and immutable nature of blockchain technology, it has shown promise as a solution for issues related to traditional EHR systems. Researchers have proposed integrating Elliptic Curve Cryptography and the Fully Hashed Menezes-Qu-Vanstone algorithm to enhance the security and privacy of decentralized EHR management. Elliptic Curve Cryptography provides a high degree of security with smaller key sizes, making it more effective and useful for people with limited resources, more efficient and practical for resource-constrained healthcare environments (Mondal et al., 2022). The FHMQV algorithm, an Elliptic Curve Diffie-Hellman key exchange protocol, provides strong authentication, key exchange, and forward secrecy characteristics, further strengthening the security of decentralized EHR systems. By leveraging these cryptographic solutions, decentralized EHR systems can ensure secure data storage, access control, and exchange of data among authorized parties, and personalizing the patient profile without compromising the privacy or medical integrity. In this paper, a comprehensive classification of multiple applications involving blockchain technology is presented (Wu et al., 2022). The scope of these scenarios will cover, healthcare management, voting systems, governance, education, public sector initiatives, supply chain management, Internet-of-Things (IOT) applications, business/industrial uses, privacy data, and information management solutions. Latency, scalability, sustainability, and quantum robustness have been mentioned as blockchain technology's drawbacks. The future direction of blockchain technology applications and the research deficit were identified. However, the paper poses challenges to practical implementation (Quasim et al., 2020). Reviewed major known studies on blockchain technology in electronic health. This study shows that blockchain technology logistics developments are increasing in the health domain for multiple applications, exchanging decentralized health data to improve disease diagnosis and/or healthcare provision among different parties (e.g., diagnostics centres). e.g., diagnosis centres. The review further confirms that a blockchain platform can provide for a medical data storage security regime, data management, and privacy; however, the paper offers no comments on implementation (Babu et al., 2023).

Methods

The Fully Hashed Menezes-Qu-Vanstone (FHMQV) algorithm functions as a key agreement protocol that utilizes Elliptic Curve Cryptography (ECC). The system is structured to facilitate a secure key exchange between two entities, while maintaining resilience against a range of attacks, including those that target vulnerabilities in previous protocols Fig. 2.

All health service centres must submit applications by mail or facsimile (fax) to the registration office chosen by Peking University. If the submission is accepted, the number of approved health service centres in China will be recorded for both acceptance and rejection. Once registered successfully, each health centre will be assigned a unique ID for future reference. Doctors will be registered according to regulations at a designated health centre and will have a unique registration ID. Patients will be registered by means of appointment with only a sanctioned health centre or a licensed medical staff (Al-Omrani and Humayun, 2023).

Each participant maintains two key pairs:

Long-term keys: $(a, A = g^a) $ and $(b, B = g^b) $ (1)

Ephemeral keys: $(x, X = g^x) $ and $(y, Y = g^y) $ (2)

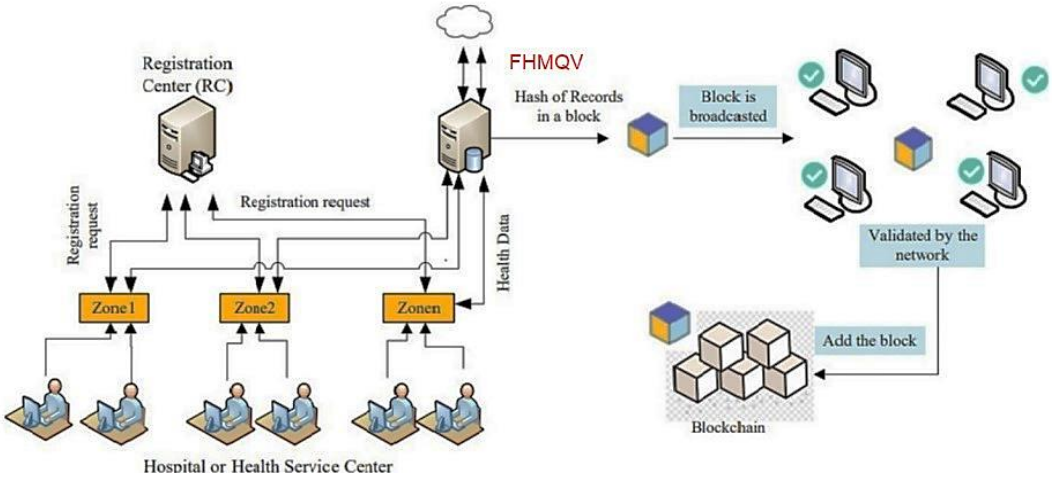

Fig. 2: Architecture of FHMQV with health service centre

ALGORITHM FHMQV_ Key Agreement

```
INPUT:
   - Elliptic curve E over finite field Fq
   - Base point G on curve E with prime order n
   - Hash functions H1, H2 (cryptographically secure)
   - Participant identities: Alice_ID, Bob_ID
OUTPUT:
   - Shared secret key K for secure blockchain communication
PHASE 1: SYSTEM SETUP AND PARAMETER GENERATION
PROCEDURE SystemSetup()
BEGIN
   // Initialize elliptic curve domain parameters
   SELECT elliptic_curve E: y² = x³ + ax + b (mod p)
   SELECT base_point G = (Gx, Gy) on curve E
   SELECT prime_order n of point G
   SELECT cofactor h = |E(Fq)| / n
   // Initialize cryptographic hash functions
   INITIALIZE H1: {0,1}* → Zn  // For scalar conversion
   INITIALIZE H2: {0,1}* → {0,1}^k  // For key derivation (k = key length)
      SET security_level = 256  // bits for post-quantum security
   SET error_threshold = 0.02  // Based on research p-value
      RETURN (E, G, n, H1, H2, security_level)
END
PHASE 2: KEY PAIR GENERATION FOR PARTICIPANTS
PROCEDURE GenerateKeyPair(participant_ID)
BEGIN
   REPEAT
      private_key_long ← RANDOM_INTEGER(1, n-1)
   UNTIL private_key_long ≠ 0
      public_key_long ← private_key_long * G  // Elliptic curve point multiplication
      REPEAT
      private_key_ephemeral ← RANDOM_INTEGER(1, n-1)
   UNTIL private_key_ephemeral ≠ 0
      public_key_ephemeral ← private_key_ephemeral * G
     Store keys securely (blockchain node storage)
   key_pair ← {
      long_term: (private_key_long, public_key_long),
      ephemeral:                    (private_key_ephemeral, public_key_ephemeral),
      participant_ID: participant_ID,
      timestamp: CURRENT_TIME(),
      quantum_resistant: TRUE
   }
      RETURN key_pair
END
```

Medical facilities are responsible for capturing, analysing, and uploading medical data to the blockchain for storage. Data capture is achieved through IoT gateways utilizing Raspberry Pi devices. Patient health information can be stored in different formats, such as text, PDF, or image files. When dealing with large data sizes or PDF/image files, the system uses the Inter Planetary File System (IPFS) for storage, which produces a hash value with a set length. (Li et al., 2022) A smart contract has been created and implemented to support the system's operations. Once the smart contract is deployed, a Graphical User Interface (GUI) application is automatically generated, providing users access to various functions. Data input is done through the GUI, which transfers the information up the model architecture's hierarchy for storage on the blockchain.

Access Records

Accessing records is facilitated by transactions encoded within smart contracts on the blockchain. The hash value for offline storage records is obtained from the blockchain, enabling easy access to the complete record set. If necessary, Health records that have been retrieved can be transmitted to a registered email address using the graphical user interface application.

Smart Contracts Implementation

A language called Solidity is employed in smart contracts, which are programs that use blockchain technology. Once previously determined conditions are met, they are carried out automatically. These methods are widely employed to improve smart contract execution performance (Chandini and Basarkod, 2023). The system is made up of three main components, Doctor, Patient, and Health Centre. Thus, there are three sources available for initiating transactions. The three high-level components in the architecture of the smart contract model are referred to as the patient, doctor, and health institution. Each smart contract securely manages registration, retrieval, and update of entity-specific data. The health centre contract, for instance, generates unique IDs, validates registration requests with a registered registration centre, and keeps track of crucial information such as the name of the hospital/date/phone number, etc. In the same spirit, the doctor contract handles updates to the doctor's profile and registration, but secures that only legitimate parties can modify records. Stringent access control is implemented through patient contracts, ensuring that only patients or registered physicians may view or modify the private medical data. This modular design aims to promote the safe and reliable management of healthcare operations in the encrypted blockchain network.

The algorithm provides the structure of all records for doctors, along with their corresponding functions.

Key Generation

Deployed over an elliptic curve, each party generates a private key and corresponding public key:

- Let PP be a point on the elliptic curve, and dad Aand dB dB be the private keys of parties A and B, respectively. Their public keys are QA = d APQA = dA P and QB = d BPQB = dB P

Hash Function

A cryptographic hash function, HH, is used to create commitments that prevent the immediate exposure of sensitive information, such as private keys, public keys, or

other associated data. However, while this technique helps obscure the data itself, it does not guarantee anonymity. For example, the use of persistent identifiers, like names or PGP IDs, can still reveal information about a participant's identity.

Key Exchange

- The parties exchange their public keys QAQA and QBQB
- Each party computes a shared secret using their private key and the other party's public key, along with the hash of the public keys

Shared Secret Calculation

- Party A computes the shared secret as: SA = H (QB, d A) SA = H (QB, dA)
- Party B computes the shared secret as: SB = H (QA, dB) SB = H (QA, dB)
- Both parties derive the same shared secret due to the properties of the hash function and elliptic curve operations (Amir Latif et al., 2022)

Session Key

- The shared secret can then be used to derive a session key for symmetric encryption

Security Features

- Resistance to Man-in-the-Middle Attacks: The use of hashing and the properties of elliptic curves help prevent unauthorized parties from intercepting or altering the key exchange
- Forward Secrecy: If a private key is threatened in the future, past session keys remain secure due to the ephemeral nature of the keys used in the exchange

Implementation Considerations

- Choice of Elliptic Curve: The security of the FHMQV protocol heavily relies on the choice of the elliptic curve and the parameters used
- Hash Function: A secure hash function (e.g., SHA-256) should be used to ensure the integrity and confidentiality of the exchanged keys (Hashim et al., 2022)

Consider $G(F_p)$ be a prime field, $a, b \in G(F_p)$ and are constants. An elliptic curve $E_p(a, b)$ over $G(F_p)$ is defined as the set of points $(x, y) \in G(F_p)$ where the following Equation is satisfied:

$$E(F_p): y^2 = x^3 + ax + b \quad (1)$$

ECDSA Signature Generation

The signing of the message is performed according to the following:

Step 1: Select a random integer k from$[1, n-1]$
Step 2: Compute $kG = (x, y)$; and compute $r = x(\mathrm{mod} n)$. If $r = 0$, go back to Step 1
Step 3: Compute $e = h(m)$, where h is the secure hash algorithm
Step 4: Compute $s = k^{-1}(e + rd)(\mathrm{mod} n)$. If $s = 0$, go back to Step 1 and reselect k

Then A's signature on message M is the pair (r, s), and A sends it to verifier B.

ECDSA Signature Verification

After B receives A's signature for message M, it performs the following steps with the public key $Q = dG$ for verification:

Step 1: Verify that r and s are integers in the interval $[1, n-1]$; if not, the signature is invalid
Step 2: Compute $e = h(m)$, where h is the same hash function
Step 3: Compute $u = ew(\mathrm{mod} n), v = rw(\mathrm{mod} n)$
Step 4: Compute $(x', y') = uG + vQ$; and Compute $r' = x'(\mathrm{mod} n)$
Step 5: If $r = r'$, the signature is valid, it is invalid

ALGORITHM 1 SMART CONTRACT FOR DOCTOR

Input: Doctors detail information

Output: Registered doctors Id

```
struct doctor info   struct Doctor Info (string doctorLicenseId;string doctor Name; string doctorAddress;string doctorSpecialization;string doctor Phone; string[] hospitalId)
                     Reg_doctor(variables to add data)

                     if ( $m$ sg.sender $==$ reg_center $)$ then
                     Store doctor details in the block,
                     return the hospital Id.

                     Else
                     I terminate the session.
                     End
                     retrieve_doctors_details (doctors_Id)
                     if doctor_ Id exists then
                     retrieve doctors' details and return
                     Else
                     I terminate the session.
                      End
                     Update doctors details(doctors_Id, variables to update data)
                     if (msg.sender $==$ doctors_id ) then
                              Update data and return success.
                     Else
                              return fail
                     End
Else                 unauthorized access, terminate session

end
```

ALGORITHM 2 SMART CONTRACT FOR HEALTH CENTRE.

Input: *Detailed information about a health centre*

Output: *Registered health centre Id*

struct Hospital Info (string hospitalId; string hospital Name; string contact Number; string hospital Address; string hospital Spec)
reg_Health_Center (variables to add data)

if (m sg. sender $==$ reg_center $) $ then
Store health centre details in the block return hospital Id

Else
I terminate the session.
End
retrieve_hospital_details(hospitalId)
If hospital Id exists, then.
retrieve hospital details and return
Else
I terminate the session.
End
update_hospital_details (hospitalId, variables to update data)
if (msg. sender $==$ health_center) then
Update data and return success.
Else
return fail
End
Else
unauthorized access, terminate session

end

The FHMQV system then takes that and produces a unique hash for the file uploaded by the user. The file's content within this network is stored. One result of the Pinata FHMQV process is that the back-end application sends this. When the hash obtained from the medical report is retrieved by the system (the manner is key), the application then interacts with a smart contract that has already been set up in Ethereum. The smart contract is a record manager in effect, between the patient's ID and the FHMQV hash, it keeps this data. If authorized parties present a medical report to the smart contract in question on the blockchain by calling appropriate operations, such documents are described and committed within its blockchain-based storage system (Ali et al., 2025). The FHMQV hash related to the patient's ID can be obtained.

Seeing that the FHMQV hash is ready, authorized person or persons can easily conjure up a link to the medical report within the FHMQV network. The patient can enjoy his health information other than reading it through email. In a word, by sending a POST request to the backend endpoint and using JSON format of data transfer, medical Information is transmitted to patients who have valid email addresses.

Because blockchains aren't built to efficiently manage vast data files, an Inter Planetary File System (IPFS) is necessary for storing huge Electronic Health Record (EHR) files in healthcare systems that leverage blockchain technology. It is more efficient to upload encrypted portions of the EHR file to IPFS and then distribute them throughout a decentralised network than to upload the whole file to the blockchain. Content Identifiers (CIDs) are cryptographic hashes that are assigned to each file and act as its permanent IPFS address. Afterwards, the CID is not saved in the file itself but on the blockchain, usually via a smart contract. Making any modifications to the file would cause an entirely distinct hash, immediately signalling unauthorised modification; the blockchain functions as a time-stamped index, making it impossible to tamper with the data. Through smart contract-enabled access management, the system gives users precise control over who can access their electronic health records. Only authorized individuals, such as particular medical professionals or specialists, can see or decrypt a patient's medical data thanks to the ability for patients to dynamically grant, revoke, or delegate permissions. Cryptographic key management systems, such as the usage of post-quantum secure key agreements (e.g., FHMQV) and ephemeral keys, which offer forward secrecy and guard against unwanted interception, enforce access rights. Because every access event is permanently recorded, patients can keep checking who has accessed their data and when on the blockchain, improving privacy protection and transparency.

The healthcare provider gets the CID from the blockchain, then retrieves the file from IPFS and uses the correct key to decode it. Management of sensitive medical data is made efficient, private, and dependable with this strategy, which combines IPFS's scalability and durability with blockchain's confidentiality and accountability.

The Transaction Rate Implementation, Execution, Testing, and Confirmation

The smart contracts that have been developed are deployed and executed using Remix IDE, which is an online integrated development environment. Fees are required for the deployment of smart contracts and the execution of transactions. Ether from Ganache accounts has been utilized as transaction fees, as illustrated in Fig. 3. Three different accounts in Ganache is used to pay for Ethereum may have transaction fees charged in each smart contract transactions fee related to the three, at the same time using an exchange rate in US dollars term shown on x and y axes non barycentric coordinates Here's the details and costs of an intelligent contract being put into operation shown in Fig. 4 by Ganache. Registration of health centres is completed at

DOI: 10.3844/jcssp.2026.517.530

the registration centre, which issues each registered health centre with a unique ID. The function reg_HealthCenter () first makes sure that the request is coming from the registration centre. When verified, a hospital ID will be created and output. The process of the deployment and interaction for hospital contracts has been described in Algorithm 1, which you provide in your paper. The function retrieve_hospital_details () receives a registered hospital ID as input and outputs the corresponding hospital information. The update_hospital_details () function is used to add new information linked to the hospital.

The reg_ doctor () function is designed to capture and store the doctor's information within the blockchain. Upon execution, this function returns a unique identifier for the registered doctor, which will be utilized in subsequent processes. The function update_ doctor_details () allows for the addition of new information regarding a registered doctor, which will subsequently be recorded in the blockchain.

By choosing appropriate communication protocols, including MQTT, CoAP, or HTTP, to link local devices to the gateway and then to cloud platforms or backend servers, you can connect a Raspberry Pi IoT gateway to your general system architecture. Install the required drivers and middleware, then connect sensors and actuators to the Raspberry Pi via GPIO, USB, or serial interfaces. Table 1 After configuring the gateway software to control device connectivity and data processing, safely send data to cloud services, including AWS, Azure, or Google Cloud, employing suitable authentication and encryption techniques. Set up monitoring tools for device and data flow management and guarantee strong security with firewalls and consistent upgrades. Supporting real-time analytics, monitoring, and remote control inside your company or cloud architecture, this connection allows seamless, safe, scalable data transfer from edge devices through the Raspberry Pi gateway to your larger IoT system.

The payment log was generated by the smart contract doctor. The representation of the intelligent contract for the patient is detailed in Algorithm 2. Prior to accessing our application, it is necessary for a patient to complete the registration process. Registration of a patient is permitted exclusively through an authorized physician or healthcare facility. The reg_patient () function is designed to store the health record of a patient within the blockchain and subsequently return an exclusive patient identifier. Access to patient records via the function retrieve_patient_details () is restricted to registered doctors and registered patients only. Only a registered doctor is authorized to make modifications to patient health records through the function update_patient_details ().

The process flow of reg_HealthCenter (), reg_Doctor (), and reg_Patient () procedures is as shown in Figure 5. Successful completion of the health centre enrollment process requires executing the reg_HealthCenter () function. When the hospital is registered, the computer program provides basic information, including hospital ID, hospital name, contact telephone, location, and class. At the time of registration for patients, the program takes in details such as patient ID, name, age, address, phone number, gender, disease, and medical history. Registration for doctors goes via use of the reg_Doctor () function, which sets the doctor's ID and various kinds of contact information, address, area of expertise, and the hospital's ID associated with it.

Table 2 compares the performance of Grover's Algorithm and classical FHMQV, demonstrating that Grover's Algorithm achieves a lower error rate, greater stability, and a quadratic speedup, while the advantage in quantum resistance depends on the specific implementation context.

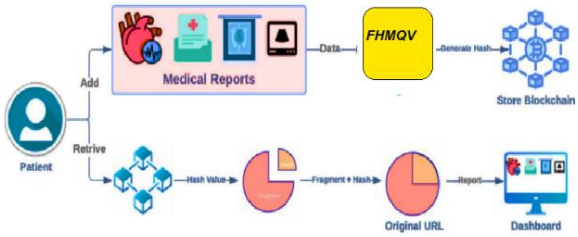

Fig. 3: Health data storing and retrieving through the FHMQV Algorithm

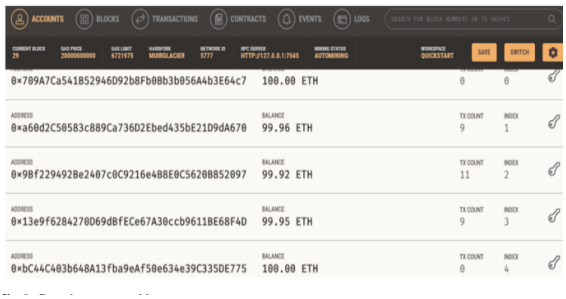

Fig. 4: ETH address with the count balance sheet

Table 1: Algorithm Performance Comparison

Metric	Grover's Algorithm	FHMQV Classical	Advantage
Error Rate	51.97%	55.66%	Grover's (Lower)
Standard Deviation	0.99158	1.65425	Grover's (More Stable)
Processing Speed	O(√N)	O(N)	Grover's (Quadratic Speedup)
Quantum Resistance	Quantum Native	Post-Quantum	Context Dependent

Table 2: ETA Cost used corresponding transaction

Operation	Gas Used	ETH Cost	USD Cost (ETH = $3,000)
Patient Registration	50,000	0.00478	$14.34
EHR Hash Upload	70,000	0.0067	$20.10
Access Authorization	45,000	0.004	$12.00

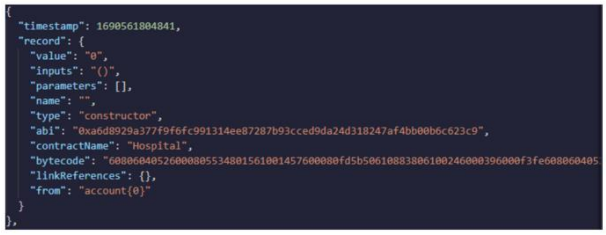

Fig. 5: Timestamp record for registration in the hospital record

Let's suppose 1 ETH equals $3,000. Below are the gas consumption and corresponding transaction fees in USD, with pictures that are intended for insertion directly into a blockchain-based EHR system. In other words, it implies, without saying so explicitly, that whichever activity costs a person in petrol (such as patient registration, EHR hash upload, or the granting of access rights) depends on how much ETH they should get in return. Take patient registration as an example, at 50,000 gas units, this exactly equals $14.34 (or 0.00478 ETH). By contrast, pouring the EHR hash upload is more laborious. It takes 70,000 gas and costs about $20.10 (or 0.0067 ETH). The lighter-duty access authorization process costs 0.004 ETH, which is $12.00. This cost-structuring transforms the scope and economic efficiency of smart contract interaction in electronic health record system development _ an outcome badly needed!

The doctor registration function records details like doctor ID, doctor name, address, specialization, and hospital ID. An example is provided in a transaction log for this function. When the smart contract executes the patient registration function, patient information, including patient ID, name, age, gender, address, telephone number, and medical data, is input, while the timestamp automatically captures the execution time. An instance refers to processing this patient registration transaction, Fig. 6.

Fig. 6: Timestamp record for the registered patient record

Results

Here, we have covered the outcomes of running the smart contracts. Fig. 7 demonstrates the interaction between smart contracts; it indicates the status of the currently performed contract along with the specifics of each transaction, as well as the transaction ID. The following parameters are assessed during contract interaction. The number of a transaction is shown by its nonce. It is the policy to process transactions in the order in which their nonce values are stored. How complicated the smart contracts are will determine the maximum gas amount needed to accomplish the transaction. Requirements for a health center's gas registration include 155166 gwei, 197442 gwei for a doctor, and 219395 gwei for a patient. More is being stored by us, in addition to medical history and patient data, instead of a healthcare provider's or hospital's records. Therefore, a patient record becomes more complicated and necessitates a higher gas limit.

For the registration of 20 health centres, the total transaction cost is 0.0412457 ETH. The average transaction cost is calculated as 0.002062 ETH (0.0412457 / 20). This methodology has been used to determine the data payload size for vaccine centre registration, vaccine administrator registration, patient registration, and all associated transaction overheads in Ethereum. All function parameters and their respective data types are considered in calculating the data payload size. For example, the data payload for the function reg_HealthCenter () is determined as follows. The parameters consist of uint300, string, uint300, string, and string, totalling 200 characters. There are 5 parameters, every 32 bytes in length, resulting in a calculation of 7*42 = 294 Bytes. This calculation indicates the data payload and associated transaction cost of each function, considering the deployment costs of hospital, doctor, and patient contracts. The analysis shows that as the intended data payload size increases, transaction execution costs also rise Fig. 8.

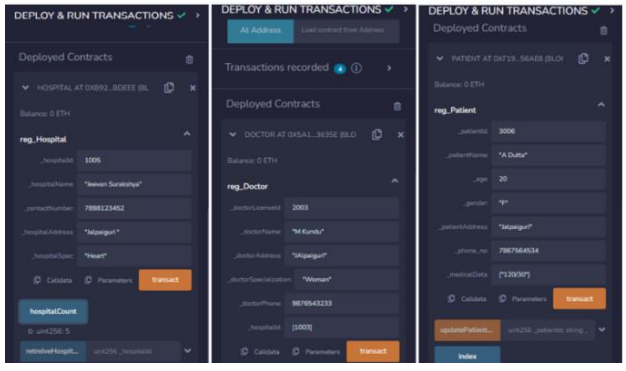

Fig. 7: Deployment parameter function for patient, doctor, and hospital

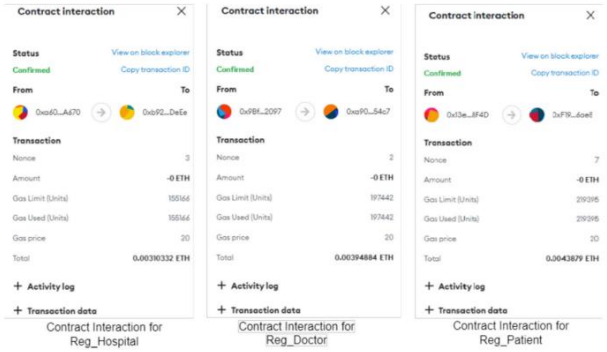

Fig. 8: Contract interaction status of Registered hospital doctor and patient

The data payload size and average transaction costs for registering doctors and patients have been evaluated. Despite this, the transaction cost for the registration functions within our system remains lower than conventional methods.

A cryptographic hash function called SHA-256 ensures data integrity and immutability by producing fixed-length unique hash values for every transaction or file. Hashing is a one-way technique that prevents the original data from being recovered from the hash, in contrast to encryption. Symmetric or asymmetric encryption algorithms (such as AES or elliptic curve cryptography) are used to safeguard the privacy of sensitive medical data. While their associated hashes are kept on-chain, encrypted medical files are kept off-chain, such as on IPFS. This hybrid strategy guarantees the confidentiality, tamper-proofing, and effective management of health data. Each transaction will generate a 256-bit hash value, which will be stored in the blockchain as a Merkle tree. Reversing data from a hash value is virtually impossible. Fig. 9.

Under the circumstances that the price for gasoline is maintained at 30 Gwei, the following table shows how much gasoline is used for critical, every-second stochastic processes in an EHR system based on blockchain. Using the formula, ETH Cost = (Gas Used Gas Price) 1,000,000,000, the computational cost of each operation has been translated into Ether (ETH) spending. Table 3 states that the cost is represented in gas units. With gas consumption of 70,000 units (0.0021 ETH), EHR Hash Upload is the most computationally intense activity, while Access Revocation uses the least with 40,000 units (0.0012 ETH). This breakdown can be used by developers and system architects to optimize smart contract interactions and estimate on-chain transaction costs Fig. 10.

The proposed electronic health record system ensures the satisfaction of data integrity properties and offers data immutability. Health records are processed utilizing a cryptographic hash function. For a specific transaction, a consistent hash value will be produced, and no two distinct transactions will yield the same hash value.

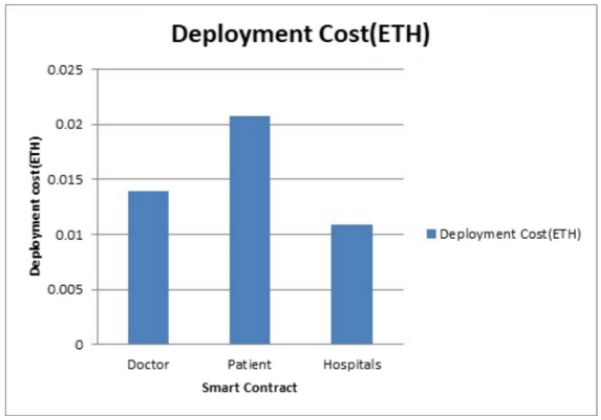

Fig. 9: Deployment cost of ETH with smart contract

Table 3: Transaction cost analysis using gas vs. the cost price

Operation	Gas Used	Gas Price (Gwei)	ETH Cost (Gas Used × Gas Price ÷ 1,000,000,000)
Patient Registration	50,000	30	0.0015
EHR Hash Upload	70,000	30	0.0021
Access Authorization	45,000	30	0.00135
Record Update	60,000	30	0.0018
Access Revocation	40,000	30	0.0012

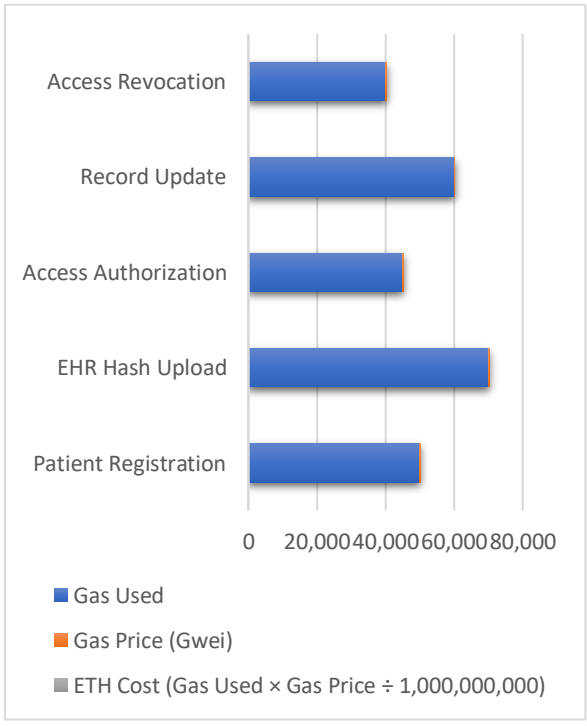

Fig. 10: Comparison of gas used Vs the ETH cost

Conclusion

Patients' health information is big business, and needs to be kept in a secure but immovable way. The paper provides a methodology for storage and maintenance using blockchain technology and smart contracts that can address the deficiencies in current methods. Smart contracts rely on Remix IDE and are supported by a connection with a MetaMask wallet that allows users to carry out transactions. The Ethereum in-memory local blockchain network created in Remix IDE integrates Ganache as well as a network using an Ether wallet. Usually, the patient and the doctor appear at the doctor's office together to get registered. They calculate that the system has lower costs than the current medical health record systems. Data about health is visible for authenticated users only. This is because data Transmission will appear as half-unreadable ciphering information (TC). Data stored in the blockchain cannot be changed. It is set as an irrevocable book that simply cannot deceive. Blockchain technology's scalability problem is solved by using cloud storage to store large medical data, including doctor prescriptions and patient reports based on FHMQV, within the framework of the blockchain. The proposed electronic health record system may use a private blockchain network such as Hyperledger Fabric for added security. Besides, the integration of biometric recognition services can ensure that patients and doctors are authorized to access electronic health records. There are still some restrictions, even if the proposed electronic health record system built on blockchain improves data security, privacy, and scalability. Real-time applications may be limited by public blockchains' transaction speed and latency. While storage scalability is addressed by the hybrid use of IPFS, access speeds and network dependability are dependent on external infrastructure. Additionally, FHMQV addresses quantum resistance; nonetheless, new quantum attacks require constant cryptographic updates. Future research will examine Layer 2 scaling options, improved privacy-preserving strategies like zero-knowledge proofs, and the incorporation of biometric-based multi-factor authentication.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Authors Contribution

The authors contributed equally to this study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Ali, A., Husain, M., & Hans, P. (2025). Federated Learning-Enhanced Blockchain Framework for privacy-preserving intrusion detection in industrial IoT. *ArXiv*, 1–18. https://doi.org/10.48550/arXiv.2505.15376

Al-Omrani, E. N., & Humayun, M. (2023). Securing Electronic Health Records (EHR) from Tampering Using Blockchain. *2020 International Conference on Smart Technologies in Computing, 761,* 397–410. https://doi.org/10.1007/978-3-031-40579-2_38

Amir Latif, R. M., Hussain, K., Jhanjhi, N. Z., Nayyar, A., & Rizwan, O. (2022). A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia Tools and Applications*, *81*(19), 26609–26632. https://doi.org/10.1007/s11042-020-10087-1

Anand, A., & Muthusamy, A. (2020). Data Security and Privacy-Preserving in Cloud Computing Paradigm. *Cloud Computing Applications and Techniques for E-Commerce*, 99–133. https://doi.org/10.4018/978-1-7998-1294-4.ch006

Arvindhan, M. (2022). Effective motivational factors and comprehensive study of information security and policy challenges. *Chapter in Cybersecurity Issues, Challenges, and Solutions in the Business World*, 531–545. . https://doi.org/10.1016/b978-0-323-90240-3.00029-1

Arvindhan, M., Upadhyay, S., Malik, A., Chakraborty, S., & Gupta, K. (2023). Comparing Techniques for Digital Handwritten Detection Using CNN and SVM Model. *Proceedings of Data Analytics and Management*, *788*, 431–444. https://doi.org/10.1007/978-981-99-6553-3_33

Babu, E. S., Yadav, B. V. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, *26*(4), 2217–2244. https://doi.org/10.1007/s10586-022-03652-w

Boumezbeur, I., & Zarour, K. (2022). Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. *Acta Informatica Pragensia*, *11*(1), 105–122. https://doi.org/10.18267/j.aip.176

Çakmak, A. (2018). *Web güvenliğinde SSL/TLS kriptografik protokolü: açıklıklar, saldırılar ve güvenlik önlemleri*.

Chandini, A. G., & Basarkod, P. I. (2023). Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *Journal of Ambient Intelligence and Humanized Computing*, *14*(4), 4221–4235. https://doi.org/10.1007/s12652-023-04526-8

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, *15*(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J. J. P. C., & Guizani, M. (2020). Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. *IEEE Transactions on Industrial Informatics*, *16*(5), 3548–3557. https://doi.org/10.1109/tii.2019.2944880

Ghantasala, G. S. P., Reddy, A., & Arvindhan, M. (2021). Amalgamation of Blockchain, IoT, and Big Data by Using Distributed Hyperledger Framework. *Lecture Notes in Networks and Systems*, 33–55. https://doi.org/10.1201/9781003081180-3

Hashim, F., Shuaib, K., & Sallabi, F. (2022). Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography*, *6*(3), 47. https://doi.org/10.3390/cryptography6030047

Iftikhar, A., Qureshi, K. N., Shiraz, M., & Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101788. https://doi.org/10.1016/j.jksuci.2023.101788

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 43–50. https://doi.org/10.1109/iciot48696.2020.9089570

Jagtap, S. T., Thakar, C. M., El imrani, O., Phasinam, K., Garg, S., & Ventayen, R. J. M. (2021). A Framework for Secure Healthcare System Using Blockchain and Smart Contracts. *Proceeding of the Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 922–926. https://doi.org/10.1109/icesc51422.2021.9532644

Johri, P., Arvindhan, M., & Daniel, A. (2021). Enabling Technologies: A Transforming Action on Healthcare with IoT a Possible Revolutionizing. *Artificial Intelligence for a Sustainable Industry 4.0*, 265–279. https://doi.org/10.1007/978-3-030-77070-9_16

Kaur, K., Kaddoum, G., & Zeadally, S. (2021). Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 5178–5189. https://doi.org/10.1109/tits.2021.3068092

Li, H., Yang, X., Wang, H., Wei, W., & Xue, W. (2022). A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. *Journal of Healthcare Engineering*, *2022*, 1–11. https://doi.org/10.1155/2022/2058497

Mondal, S., Shafi, Md., Gupta, S., & Gupta, S. K. (2022). Blockchain based secure architecture for electronic healthcare record management. *GMSARN International Journal*, *16*(4), 413–426.

Murugan, A., Chechare, T., Muruganantham, B., & Kumar, S. G. (2020). Healthcare information exchange using blockchain technology. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(1), 421. https://doi.org/10.11591/ijece.v10i1.pp421-426

Quasim, M. T., Radwan, A. A. E., Alshmrani, G. M. M., & Meraj, M. (2020). A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry. *Proceeding of the International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, 605–609. https://doi.org/10.1109/icstcee49637.2020.9277193

Rai, B. K. (2022). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, 80–102. https://doi.org/10.1007/s10742-022-00279-7

Rangwani, D., & Om, H. (2023). Chaotic map based multi-factor authentication protocol for underwater environment monitoring. *Multimedia Tools and Applications*, *83*(9), 26871–26900. https://doi.org/10.1007/s11042-023-16608-y

Sharma, V. P., Sharma, P. C., Kumar, S., Yadav, N. S., Sharma, S., & Choudhary, D. (2021). *Deep Learning-based Solution for Sustainable Agriculture*. https://doi.org/10.52305/ENYH6923

Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, *178*, 102950. https://doi.org/10.1016/j.jnca.2020.102950

Tomar, A., & Tripathi, S. (2022). Blockchain-assisted authentication and key agreement scheme for fog-based smart grid. *Cluster Computing*, *25*(1), 451–468. https://doi.org/10.1007/s10586-021-03420-2

Uddin, M., S. Memon, M., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. *Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records*, *68*(2), 2377–2397. https://doi.org/10.32604/cmc.2021.015354

Vardhini, B, Dass, S. N., R, S., & Chinnaiyan, R. (2021). A Blockchain based Electronic Medical Health Records Framework using Smart Contracts. *Proceeding of the International Conference on Computer Communication and Informatics (ICCCI)*, 1–4. https://doi.org/10.1109/iccci50826.2021.9402689

Wu, G., Wang, S., Ning, Z., & Zhu, B. (2022). Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1917–1927. https://doi.org/10.1109/jbhi.2021.3123643