




Securing Medical Data Exchange: A Decentralized Approach Based on the e-IPGPChain Framework



Hamza Rafik^{1*}, Abdelaziz Ettaoufik², Abderrahim Maizate¹

¹ RITM- ESTC/CED - ENSEM, Hassan II University, Casablanca 20100, Morocco

² LTIM - FS BEN M'SIK, Hassan II University, Casablanca 20100, Morocco

Corresponding Author Email: hamza.rafik-etu@etu.univh2c.ma

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijss.140314>

ABSTRACT

Received: 22 February 2024

Revised: 9 May 2024

Accepted: 24 May 2024

Available online: 24 June 2024

Keywords:

edge computing, Hyperledger Fabric, IPFS, GPG-edDSA, internet of medical things, encryption and decryption digital signature

Delivering healthcare services closer to the end user faces a significant challenge in light of frequent cyberattacks that target personal data for disruption, financial gain, and damage purposes. Existing e-health monitoring solutions exhibit limitations related to performance, stability, and overall system security, which negatively impact medical service delivery and reveal technical difficulties related to privacy and availability. This paper introduces a novel approach that integrates various technologies intending to fully decentralize the sharing of medical data with minimum privacy risks while maintaining high-performance medical services. Our Solution e-IPGPChain, Leverages Hyperledger Fabric network-related RBAC policies, IPFS, and edge computing to build a robust system with a hybrid storage solution, ensuring optimal data availability. Furthermore, the proposed solution improves workflow security and privacy by employing a cryptographic ecosystem tool, GPG (GNU Privacy Guard), an open-source implementation of PGP (Pretty Good Privacy), featuring a strong and lightweight digital signature mechanism named edDSA besides, an encryption technology, to enhance the authenticity, integrity, and non-repudiation of exchanged medical data among different entities. The performance evaluation focuses on the most valuable metrics for the medical field such as latency, scalability, data processing, and system availability, which indicates a significant result. On the other hand, using the STRIDE framework identifies key points to ensure the security conformity from different angles for our solution against common cyberattacks. Evaluating common attacks against the solution demonstrates the level of privacy provided to secure medical data workflow.

1. INTRODUCTION

Exchange Data over multiple entities has increased recently in different sectors, due to the high digitalization expansion over various industries including Education, Financial Services, Commerce, and Healthcare sector. Health services have increased recently due to the expansion of viral and chronic diseases which raise medical requirements [1]. However, the Traditional e-health smart systems are revolutionizing the healthcare industry by providing medical services closer to end users based on multiple typical layers such as edge computing, Internet of Medical Things “IoMT” and Cloud computing technologies [1], which aim to manage medical records that are commonly known as Electronic Health Records “EHR”. The exponential increase of data over time puts an overload to the cloud networks for processing and storing data as well as difficult accessibility for various stakeholders, this results in serious performance, security, and privacy challenges due to its limited centralized built-in structure.

Indeed, the advancement skills of cyberattacks directly affect users’ personal medical data confidentiality. In fact, between 2009 and 2023, more than 5150 data breaches were

reported to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) [2] the occurred breaches resulted in an exposure of 382,262,109 healthcare records which represent 1.2x the population of the United States. According to Fortified Health Security’s report, the first half of 2023 indicated 295 breaches that impacted more than 36 million individuals [3], which led to increased data leakage, reputational and financial losses, and patient personal safety risks.

Based on the above occurrences, existing health monitoring systems become securely unsafe, lack privacy, and significantly degrade of quality of services [4] due to their network structure and insufficient security measures. This paved the way to adopt a decentralized approach for data storing and sharing services across multiple entities [5], such as Blockchain technology and distributed peer-to-peer (p2p) storage networks. Up to this point, the conventional systems revealed serious challenges in terms of confidentiality, Privacy, Availability, and Integrity related to sharing and storing personal medical data (EHR). Communicating data over the network uncovered the system’s component to several threats that can intensify into serious risks, such as the recent ransomware attacks [6]. Also, medical data grows intensively

thanks to the IoMT devices, which offload the current system and reveal significant performance, availability, and security challenges detailed in the following main points:

Secure sharing workflow: the basic structure of healthcare monitoring systems exposes serious security risks due to the variety of deployed components. Additionally, limited access control policies and a lack of encryption techniques can make this environment susceptible to advanced cyberattacks, which can potentially affect users' safety.

High availability: Health monitoring is an essential part of preventive care nowadays, particularly in case of emergency activities where the importance of the ability to access data for authorized entities at any time and from any place, while this is not properly satisfied on current approaches.

Data Integrity: Although existing healthcare monitoring systems have great features, they do not provide an efficient way to store, share, and verify health data ownership in a globally unified manner [7].

Bandwidth and Storage efficiency: The exponential increase of collected data places a heavy burden on the network resources, which affects the latency and storing capabilities to access medical data for actual structures.

Consistent data source: Ignoring signing data techniques leads to significant problems related to data tampering, Forgery, and Repudiation, which results in untrusted data exchange flow.

Deployment of emergent technologies helps to accomplish the objective of this paper to establish a fully secure decentralized e-health monitoring system, designed to address the common limitations listed above, the proposed solution, e-IPGPChain, integrates different technologies to overcome the existent solutions in terms of performance, security, and privacy measures across different stages. However, the use of the GPG-based Edwards-curve Digital Signature Algorithm "edDSA" employs keys shared features across the network to enable end-to-end encryption and digitally sign encrypted data, for effective confidentiality, integrity, and non-repudiation of collected data [8, 9], this technique enhances the trustworthiness of the data source, improves resource efficiency, and contributes to securing the overall data-sharing model.

Meanwhile, sharing data across multi-authorized participants involved the deployment of a private blockchain network leveraging the Hyperledger Fabric project based on RBAC (Role Based Access Control) policies, leveraging a logical workflow process ensured by specific developed Chaincode that contain a set of procedures to standardize sharing data over the blockchain network to the corresponding requester as listed from the work [10], in addition to using a private channel mechanism for extra access protection in a full collaborative medical environment. Therefore, the trend of preserving high data availability for the healthcare sector is important during monitoring phases, due to the critical medical information in case of emergencies also to provide a consistent data accessibility experience. Hence, the integration of IPFS along with the edge computing technology in our proposed approach provides an extra hybrid storing feature for medical data realizing the availability requirement as well as operating seamlessly with other components such as GPG-edDSA technique and Blockchain network for efficient and secure workflow as indicated and analyzed through a series of test cases focused on main e-health features. Furthermore, the STRIDE threat model was exploited to comprehensively evaluate the overall system from security and privacy

perspectives which lead to identifying the security risks and their corresponding implemented mitigations.

In the remaining parts of this paper, Section 2 outlines the related works characterized by some limitations from existing contributions, while Section 3 unveils fundamental system notions to comprehend the overall proposed structure. Section 4 describes the deployment of the proposed e-IPGPChain. Section 5 discusses the evaluation outcomes in comparison to the current solutions and provides a comprehensive security analysis. This paper will highlight the main contribution and purposes in the last section while providing future perspectives for further contributions.

2. RELATED WORKS

Many studies recently leveraged Blockchain technology with a variety of emergent mechanisms to address most of the security challenges exposed by regular e-health monitoring systems. Blockchain represents an immense promise to revolutionize the healthcare sector by offering a solid and relevant structure based on transparency, immutability, and efficiency to manage sensitive medical data. Utilizing this structure contributes to the e-health ecosystem in their security and privacy perspectives while guarding an efficient performance delivery. However, despite these features, existing contributions remain insufficient due to the significant development of the healthcare industry, evolved cyber-attack techniques, and the exponential growth of data volume. These aspects indicate the need for further exploration in blockchain, incorporating advanced solutions.

2.1 E-health system based on private blockchain

This part of the section focuses on the Private or Permissioned Blockchain structure which is mainly a permission-accessibility network to private data, as an example of a solution: The Hyperledger Fabric [11]. The listed contributions have been evaluated according to the information security measures, in addition to some relevant aspects such as access control policy, Data non-repudiation, Emergency data accessibility, Latency, scalability, and the interoperability of the overall system.

Mani et al. [12] introduced PCHDM framework stands for Patient-Centric IPFS-Based Storage of Health Records, which is a patient-centric model that allows patients to fully control their data and share across a private blockchain-based IPFS structure securely with healthcare providers, nevertheless, this solution shows some limitations in terms of data integrity, scalability of the systems as well as non-repudiation. In the study of Margheri et al. [13], the authors proposed a relevant platform for managing EHR by using defined smart contracts on the Hyperledger Fabric network to enable tracking, this solution exposed difficulties in terms of data availability, and ensuring full data confidentiality. Rajput et al. [14] utilized a permissioned blockchain in their contribution that incorporates Access control policy, and auditing mechanisms aimed to facilitate access to medical records in emergency scenarios for authorized entities. This solution is affected by privacy concerns stemming from the need to share audit log information with all network members.

Moreover, Abdelgalil and Mejri [15] introduced a framework named Healthblock, which provides a secure and collaborative sharing model of medical data by leveraging the

technologies of blockchain, IPFS, and decentralized identity mechanisms to ensure patients have full control over their medical data and improve the users' security aspect. The suggested model exposed many challenges in terms of integrity, complexity scalability, and data confidentiality.

2.2 E-health system based on public blockchain

The Public blockchain network where there is no permission required to join the network [15] is commonly used for diverse sectors such as cryptocurrencies, Finance, Business, Education, Industry [11], due to its transparency and immutability. Therefore, this structure was adopted for delivering important services including healthcare monitoring systems.

Egala et al. [16] proposed a decentralized model named CoviBlock based on an Ethereum Blockchain, IPFS, and edge computing to address the limitations of centralized healthcare monitoring systems in terms of performance and security approaches. Besides the important cases targeted by this model,

is still limited in terms of data integrity, Privacy, and system Scalability.

For the paper Alsayegh et al. [17] presented an authorized medical data-access system based on blockchain and asymmetric encryption mechanism to ensure the secure exchange of EHR over the network. This proposed system is susceptible to SPOF (Single point of failure), data repudiation, and the transparency characteristics of the implemented blockchain network which is vulnerable to various accessibility threats.

In the study of Kumar et al. [18], the authors described an off-chain storage solution to manage medical data based on distributed solutions by leveraging the blockchain features to store data indexes that refer to the original data stored in the IPFS network which can guarantee secure and highly available data transactions among members. Besides the advantages of this framework, still exposed to several limitations including an access control policy and efficient encryption and confidentiality mechanisms.

Table 1. Related works summary and limitation overview

Ref.	Published Year	Contribution	Blockchain Technology	IPFS	Storage Optimization	Encryption	Integrity	Access Control	Challenges
[18]	2020	An off-chain structure based on Blockchain and IPFS to handle Medical records	Ethereum	✓	✗	✗	-	✗	- Access control - Storage efficiency - Extras deployment costs
[16]	2022	A novel model CoviBlock deploys the recent decentralized technologies to address the challenges of the existing health monitoring system	Ethereum	✓	✗	✓	✗	✓	- Extras deployment costs - Data Privacy - Storage efficiency - System scalability
[17]	2022	A blockchain-based data-sharing system resolves privacy limitations by using an asymmetric searchable encryption system and access control mechanism	Ethereum	✗	✗	✓	✗	✓	- Extras deployment costs - Single Point of failure - System Scalability - Storage efficiency - Data Integrity
[12]	2021	A patient-centric model (PCHDM) enables manage data in a decentralized context	Hyperledger Fabric	✓	✗	-	✗	✓	- Data Integrity - System scalability
[19]	2022	A framework designed to handle EHR using blockchain and IPFS with Multi-layered security measures	Ethereum	✓	✗	✓	✗	✓	- Data Integrity - Storage efficiency - Extras deployment costs
[13]	2020	Introduced a healthcare data provenance system for managing data using smart contract capability	Hyperledger Fabric	✗	✗	✗	✗	✓	- Data high availability - Storage capability and efficiency - Data security and privacy
[14]	2021	A tamper-resistant framework based on blockchain for data healthcare management	Hyperledger Fabric	✗	✗	✗	✗	✓	- System scalability - Data Security and Privacy - Storage capability and efficiency
[15]	2023	Healthblock is a combination of decentralized technologies to preserve the secure sharing of medical data	Hyperledger Fabric	✓	✗	✓	✗	✓	- Data Integrity - Storage efficiency - System scalability

Therefore, the work of Jayabalan and Jeyanthi [19], represented a framework that combines both technologies blockchain and IPFS intending to manage EHR by enabling multi-layers of security including multi-factor authentication, symmetric and asymmetric encryption to secure health data. This solution still needs more improvement in terms of the data preprocessing stage and data storage capability.

Sharing medical data is a crucial task nowadays due to the nature of the data used and the importance of the health landscape to improve medical delivery. However, most existing solutions remain limited in terms of security concerns, such as encryption and digital signature, as well as records accessibility. Additionally, the performance aspect faces challenges, particularly in preserving high availability resources while maintaining low latency and scalability. For a comprehensive overview, Table 1 outlines different related works leveraging the benefit of using emergent technologies including Permissioned “Private Blockchain” or Permissionless “Public Blockchain” [20], IPFS, and encryption techniques in comparison to our proposed model which defines a new approach that incorporates emergent technologies to build a lightweight solution to provide medical services with high performance efficiency while preserving a maximum security measure to protect personal user’s data over the network.

3. ARCHITECTURE OVERVIEW

In this section, we will discuss the main technologies and approaches that have been employed in our proposed system to ensure a secure, performant, and private collaborating environment to share large amounts of medical data with external stakeholders, while still retaining full control over access and ensuring the total integrity of the exchanged data amongst all network stages.

3.1 Hyperledger Fabric (permissioned blockchain)

Hyperledger Fabric is a Private type of Blockchain technology, in 2015, the Linux Foundation initiated this framework which frequently has been used in various areas like finance, healthcare, supply chain, and manufacturing to build a standardized blockchain framework for business workflow [21]. This Permissioned network is based on a modular structure that offers exceptional identity management and access control features, in addition to providing a secure architecture based on a channel mechanism, making it appropriate for our framework e-IPGChain to empower the secure sharing network of medical data across various authorized participants.

The Hyperledger Fabric technology is characterized by the following key features:

- *Distributed Digital Ledger*: maintains a shared, tamper-resistant ledger across multiple nodes [21].
- *Smart Contract*: also known as Chaincode for Hyperledger Fabric technology, defined to model the business logic that governs the behavior of the network.
- *Permissioned Network*: The ability to enable authorized members to access and control transactions over the network.
- *Private Channels Technique*: Provides an approach for nodes to collaborate privately and isolate traffic from non-authorized nodes, thereby offering transaction

confidentiality.

- *Consensus Algorithm*: Ensure the validity of transactions over the network, Hyperledger technology uses several consensus mechanisms such as practical Byzantine Fault Tolerance (PBFT) and more.
- *Membership Service Provider (MSP)*: Responsible for designing permissions, roles, and attributes for different network members that have been enabled from the Certificate Authority (CA) node.
- *Modular Architecture*: Allows the efficiency of personalization and integration with the existing systems and infrastructures.

Moreover, the Role-based Access Control (RBAC) related Chaincode scripting technique empowers network accessibility. It becomes more efficient by defining members’ roles and their assigned responsibilities and permissions [22] this is conducted to normalize the functional logic of grant access and perform certain operations in the Blockchain network. By integrating into the network, each member of the framework executes several phases, starting with establishing connectivity access. Therefore, the user submits a transaction proposal to the endorsing peers. Next, the endorsing peers simulate the transaction and return the endorsement results to the user, who then collects these endorsements and sends the transaction to the ordering service for building into a block, which is then broadcasted to all peers to be stored in their attached decentralized ledgers [5].

3.2 Peer-to-peer file management system (IPFS)

Distributed Storage is an advanced technology that provides a novel approach to enhancing digital storage capability and facilitating management and accessibility for individuals and businesses. For instance, IPFS [23] is an emergent technology that enables users to securely and efficiently store and share data without the need for central management entities. Thereby, it is characterized by its distributed structure based on peer-to-peer connectivity and content addressing mechanism, to identify the stored data and files on the overall network using a unique Content Identifier (CID) [24]. In addition, the IPFS structure is based on four main mechanisms for managing content known as Distributed Hash Table (DHT), Merkle DAG, Bitswap Protocol, and Self-Certifying File Systems (SFS) to store and retrieve files effectively, hence, ensuring data availability and increasing the redundancy, throughput, performance, and security [25].

Managing sensitive data over the IPFS includes using immutability, hashing, and content-addressing techniques to improve the storage capability of our solution alongside edge computing resources that complement the process. Data storage on an off-chain technology requires each user to be attached to the IPFS network, while the overall workflow started by splitting data into several fragments on multiple network peers to achieve the distributed approach, each with 256Kb maximum size, stored in an object format, that will be assembled into a Merkle DAG structure, a tree format topology, where the access to data is governed by a root hash ID that will be shared by the data owner for further phases [26]. This technology is intended to overcome the conventional client-server architecture by offering a more reliable, efficient, and secure method of preserving data along with advanced technologies to ensure a high continuity of exchanging critical data as employed for our proposed e-health system.

3.3 Encryption, decryption, and digital signature processes leveraging edge computing technology

In order to ensure data confidentiality and protect private information from unauthorized access and manipulation, encryption comes over to encipher data from its readable state using relevant algorithms. Therefore, the digital signature is a technique that uses mathematical algorithms to guarantee the Authentication, Integrity, and Non-repudiation of a series of data by attaching a distinctive signature to identify the source of data to contribute to enhancing the trustworthiness of data delivery [27]. The integration of the signature mechanism required the use of a lightweight tool combining both encryption and digital signature features.

Therefore, Pretty Good Privacy (PGP) [28] is an applicable tool that serves for encryption, decryption, compression, and digital signature of files and messages. It was created by Phil Zimmermann in 1991 and provides data confidentiality, integrity, and authentication by combining multi-cryptography techniques. GnuPG (GNU Privacy Guard or GPG) [29] is an open-source solution for PGP characterized by the same sequence logic of generation of the pair keys (Public/Private) assigned for each user which is adopted for the main cryptography operations of the proposed system. The public key is shared securely with corresponding members on the

network, while the private one is kept secret. Each user employs its user-specific key directories, which represent a separate password-protected directory within the edge device's filesystem to store each user's GPG keys. This ensures that private keys remain isolated and protected from access by unauthorized entities.

Edge computing is considered a closer resource gateway to the end user [1], which offers low latency, storage, and computing resources. This technology is exploited to enable the cryptographic tool GPG for conducting data processing operations, based on various supported cryptographic mechanisms and algorithms as listed in the Table 2. Accordingly, the adoption of the edDSA algorithm [30], particularly the ed25519 implementation scheme which uses SHA-512 (SHA-2 family of hash function), and Curve25519 make it suitable for our framework implementation due to its strong security and faster ability to provide further protection against tampering and forgery threats. The combination GPG-edDSA uses the cryptosystem mechanism based on ed25519, and AES schemes, for encryption, decryption, digital signature, and compression processes. Generated key pairs are engaged for ensuring the preprocessing of data by using the sender's private key and the corresponding receiver's public key. This guarantees accurate data verification and secure decryption.

Table 2. GPG supported encryptions and signature algorithms [29]

GPG Components	Algorithms	Application
Public key Algorithms (Asymmetric)	RSA	Encrypt-Sign
	ELG (ELGAMAL)	Encrypt-Only
	DSA (Digital Signature Algorithm)	Sign-Only
	ECDH (Elliptic Curve Diffie-Hellman)	Encrypt Only (Key Exchange)
	ECDSA (Elliptic Curve Digital Signature Algorithm)	Sign-Only
	EDDSA (Edwards-curve Digital Signature Algorithm)	Sign-Only
	IDEA (International Data Encryption Algorithm)	Encrypt-Only
	3DES (Triple Data Encryption Standard)	Encrypt-Only
	CAST5 (CAST-128)	Encrypt-Only
	BLOWFISH	Encrypt-Only
Symmetric-key or Cipher Algorithms	AES (Advanced Encryption Standard)	Encrypt-Only
	AES192	
	AES256	Encrypt-Only
	TWOFISH	
	CAMELLIA	Encrypt-Only
	Hash Algorithms	SHA1 (Secure Hash Algorithm 1)
SHA256, SHA384, SHA512, SHA224		
MD5 (Message Digest Algorithm 5)		Hash-Only
RIPMD160		Hash-Only
Compression Algorithms	Uncompressed	Data-Compression
	ZIP	Data-Compression
	ZLIB	Data-Compression
	BZIP2	Data-Compression

4. THE PROPOSED SYSTEM MODEL

In this section, we introduce our framework model proposed to address the main challenges uncovered by the conventional e-health systems related to Confidentiality, Availability, Performance, and Integrity of the overall system. The main system is formed by three key components: the user layer that combines IoMT and edge computing, the Hyperledger Fabric-blockchain structure, and the IPFS a distributed storage network. Our structure is divided into three levels:

- EHR Collection and Preparation level: Designed to collect, encrypt, compress, and digitally sign data for further operations.

- Storage level: Intended to save medical data based on a novel hybrid storing model combining local and distributed resources.
- Collaborative sharing level: Providing a secure and private exchange environment based on a Private-Access Control blockchain network.

4.1 e-IPGPChain: The decentralized structure overview

The e-IPGPChain is based on a decentralized structure, that is adopted for the future of secure transactions over the network and overcoming the dependency on centralized management entities, where data become a subject of

cyberattacks and Single Point of Failure “SPOF” related system elements [19]. The proposed system is designed to manage medical data by incorporating various decentralized technologies as illustrated by Figure 1, including the Permissioned Blockchain, and Hyperledger Fabric, while the IPFS deployed based on a peer-to-peer approach along with edge computing technology to provide an integrated solution

for storing data within different strategies local and distributed, moreover, the edge computing serve to prepare medical data by using a faster, secure, and more reliable cryptographical ecosystem “GPG-edDSA”. Therefore, this technology provides secure accessibility to patients through a VPN to personal directories based on an authentication mechanism to safely isolate the patient environment.

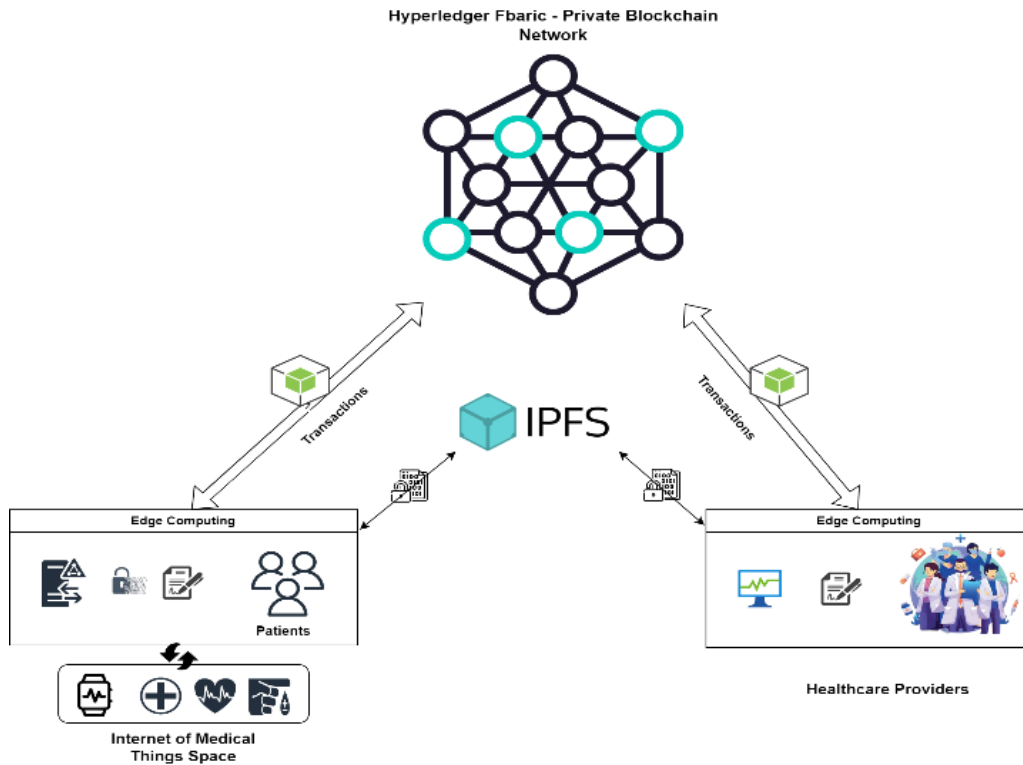


Figure 1. Overview design of the proposed decentralized e-health system "e-IPGPChain"

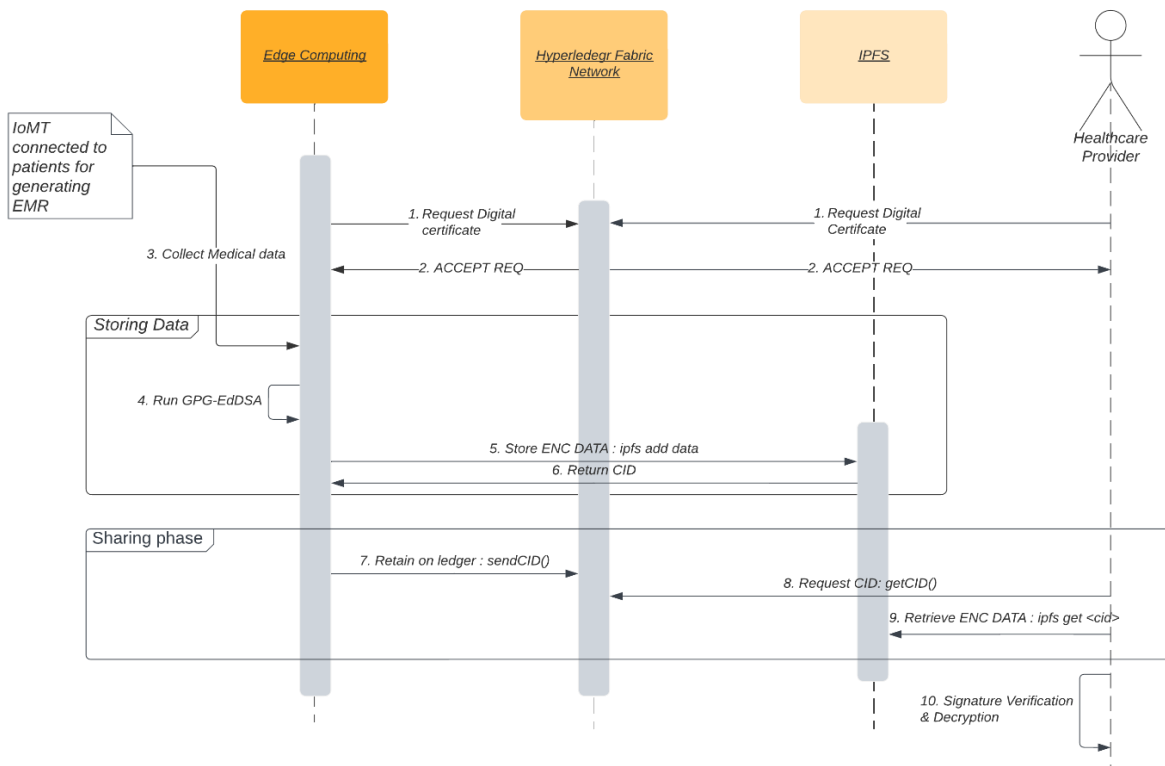


Figure 2. Sequence diagram of exchanging medical data workflow using e-IPGPChain model

e-IPGPChain, is a flexible and lightweight solution, where EHR is safely shared and stored after being collected through the IoMT network. The pre-processing phase incorporates edge computing and cryptographic techniques: Compression, Encryption, then Digital Signature. Furthermore, keeping high available data is achieved by the IPFS, where data is sent to be stored on a distributed network of peers, and returned a unique identifier (CID). The generated CID is transmitted within the Hyperledger Fabric network using Chaincode and Fabric Software Development kits “SDK”, where CID accessibility is based on different contributor assigned roles following RBAC policies. The overall system procedures are described by the sequence diagram from the Figure 2, outlines the main functional steps of the e-IPGPChain from the initial prerequisites to integrate and manage medical data, arrives to determine the accessibility of shared data through authorized healthcare providers. This Health collaborative architecture demonstrates the achievement of the highest security, reliability, and privacy levels through testing different experimentations, as elaborated upon in further chapters.

4.1.1 System’s members defined roles

The system includes the participation of different members in the collaboration process of healthcare services within a fully trusted environment. Four main roles are defined for the system’s key users, including:

- *Patients*: Normal users with “admin” privileges to fully control Medical Data (EHR), this role is assigned for patients to successfully submit transactions and manage data.
- *Doctors*: Users belong to the healthcare providers community, where they’re assigned a “doctor” role that is characterized by the ability to gather medical data through the Blockchain network and IPFS.
- *Nurses*: Users belong to the healthcare providers community, with reduced permissions. This category of users is assigned an “agent” role inside the network.
- *Emergency Members*: First aid healthcare providers, this type of user is committed to having emergency access in critical cases, they are assigned “alertmed” as a role, allowing faster and special accessibility to medical data through authorized tools such as VPN/IPSec access.

4.1.2 Notations

In the following parts of this work, we make use of various notations listed in the Table 3 related to the framework e-IPGPChain deployment workflow.

Table 3. List of notations

Notations	Descriptions
Md	Medical data
D	Normal Data
P	Preprocessed Medical data
En ()	Encryption Function
Dy ()	Decryption Function
K_enc	Symmetric Key encryption
PubKx ()	Public Key for user “x”
PrvKx ()	Private Key for user “x”
Sign(D)	Data Signature Process
Verf(D)	Data Verification Process
C	Ciphered Data
Hs ()	Hash Function
P, D, N, EM	Patient, Doctor, Nurse, Emergency Members
<pzone>	Patient zone channel

4.2 EHR pre-processing related edge computing

Medical data contains valuable information including vital signs related to different health conditions: Heart Rate, Blood Pressure, Oxygen saturation, and others [1]. The Internet of Medical Things delivers an unsecured data stream containing sensitive information. However, the integration of edge computing brings cloud technology features to the end-user layer through managing, preparing, and even delivering medical services in real-time. Computing resources play a crucial role in reinforcing collected data by applying cryptographic operations, according to the deployed GPG-edDSA scheme which is divided into three essential steps as described in further sections of this chapter.

4.2.1 Compression

GPG-edDSA algorithm as mentioned in the above section III.3 above, is characterized by its compression attributes that help to reduce data size and gain advantages to reduce Bandwidth utilization, and storage capacity and optimize the encryption and signature tasks. Along with the growing IoMT market [31], proportionally the average size of data increases exponentially which reveals the benefits of using compression capability. Most of the techniques deployed and supported are ZIP, ZLIB, and BZIP2, each one based on a specific algorithm depending on several factors and used for a particular requirement.

4.2.2 Encryption

The compressed medical data are effectively encrypted using the GPG-edDSA mechanism. However, the encryption process is achieved by using AES/GCM (Advanced Encryption Standard) the default symmetric encryption technique that involves two main features: the key generation and the encryption process.

The generation of keys is based on a cryptographical secure random number generator to guarantee the key’s unpredictability, according to this Eq. (1):

$$K_{enc}(AES256) = SHA256(R) [0:256] \quad (1)$$

The first 128 bits serve as an encryption key while the last 128 bits serve as the authentication key. AES is categorized into different lengths: 128, 192, or 256 bits which determines the strength of the encryption mechanism [32].

Generally, AES uses a block cipher to encrypt data in blocks, while the additional mode GCM (Galois/Counter Mode) helps to enhance the security by using a Message Authentication Code (MAC):

Cipher the target data, by using the combination key and data, as illustrated by the Eq. (2):

$$C(D) = E(K_{enc}[AES256], D) \quad (2)$$

Determinate the authentication Tag that will be compared in the decryption phase, the Tag noted “T” and calculated using this Eq. (3):

$$T = Hs(K_{enc}[AES256], C(D)) \quad (3)$$

The deployment of GPG-edDSA facilitates the Encryption/Decryption processes through a hybrid cryptographic system that combines the symmetric key with a public key that will be securely shared with corresponding

members of the network. Encrypt data using this approach, exploit the recipient's public key which is designed to enable decryption only by the holder of the corresponding private key, the process is described by these Eqs. (4), (5):

$$\text{Encryption Stage: } P = En(PubK_x, Md) \quad (4)$$

$$\text{Decryption Stage: } Md = Dy(PrvK_x, P) \quad (5)$$

4.2.3 Digital signature

As previously mentioned, the used cryptographic system is based on the generation of the pair keys for each framework user, as a sample for: Patient ($PrvK_{Patient}$, $PubK_{Patient}$), Doctor ($PrvK_{Doctor}$, $PubK_{Doctor}$), etc.

Therefore, GPG-based edDSA uses the ed25519 elliptic curve algorithm for the key generation, while the signature and verification processes involve multiple steps:

Generation of 256-bit pair keys:

Private Key generation is crucial based on leveraging the random number generator for obtaining a random secret scalar, the whole process is protected to guarantee the strength of the private key.

Public Key: For G defined as a point on the Edwards Curve 25519:

$$PubK_x = PrvK_x * G \quad (6)$$

Calculation of the hash value of the Medicalgene data, using this Eq. (7):

$$h = Hs(Md) \quad (7)$$

The signature process is executed and provides the following outputs:

$$Sign(Md) = eddsa(PrvK_{sender}, h) \Rightarrow (r, s) \quad (8)$$

where, "r" is the signature's first coordinate and "s" is the second coordinate.

The verification process described in (9) involves using the sender's public key to validate the integrity of data before any decryption process. This operation requires two main steps: firstly, calculating the hash of encrypted data using the Eq. (7), if it matches the correct hash, then proceed to the verification stage:

$$Valid/NotValid = Verif(PubK_{sender}, h, [r, s]) \quad (9)$$

4.3 Storage approach related to the e-IPGPChain scheme

Through the e-IPGPChain framework, the risk of a Single Point of Failure (SPOF) is significantly reduced, by providing a resilient hybrid storage design formed by the existing resources: Local and distributed. The edge computing technology serves as a local storing node, ensuring faster data accessibility. On the other hand, the effective feature employed in our framework, IPFS technology, exploits its distributed structure to provide data with a high availability aspect while preserving the confidentiality and the persistence of data. Unlike Edge storage resources, IPFS manages to store data in multiple nodes in the form of several chunks of 256 KB [24] and then generate a hash identifier named CID to address the target file on the whole distributed network to enable data accessibility [33]. This mechanism is detailed in the previous

sections. However, the generated ID will be securely shared with authorized stakeholders over the network.

After collecting and pre-processing Electronic Health Records (EHR), the Edge devices store the encrypted data leveraging local resources, while simultaneously sharing a copy of the data on the IPFS for collaborative purposes. Furthermore, sending and retrieving data from the IPFS network incorporates a special deployment that encompasses a series of functional requests to interact with the network components including the edge computing devices and the Hyperledger Fabric network. This process involves two main approaches:

- *Storing and Sharing:* At this stage, the framework initiates the activity by encryption and signature, then sends encrypted EHR to the IPFS network, while the returned CID will be shared over the Blockchain network for subsequent procedures. The entire process as depicted in the Algorithm 1, requires the existence of an essential set of components.

Algorithm 1: Compression, Encryption, Signature and Verification Procedures – Patient Side

Input: *raw_data* (*Md*) as string, *Public_key_recipient* an array of string, *Private_key_sender* an array of string

Output: *encrypted data* (*CiphD*) as string, *CID* as string array, *Boolean* (*False*, *True*)

- 1 *Import required Public_key_recipient from PGPEXCH_chaincode*
 - 2 *Create IPFS client instance*
 - 3 *Check Permissions and roles*
 - 4 **For each** *Md* in *medical_folder* **then**
 - 5 *Read the collected data as raw data* (*Md*)
 - 6 **If** *Md* # *Encrypted* **then Perform the GPG-edDSA procedure:**
 - 7 *Apply compression algorithm to Md: RD* (*Md*) <- *zip.compress*(*Md*)
 - 8 *Encrypt compressed data C* <- *En* (*RD*(*Md*), *Public_key*)
 - 9 *Sign data P* <- *sign* (*C*, *Private_key*)
 - 10 *Store data locally* *add.local*(*P*)
 - 11 *Add encrypted data to IPFS: ipfs.add*(*P*)
 - 12 **Return** *CID*
 - 13 **Else**, *return False*
 - 14 **End if**
 - 15 **Else** *Deny access, return False*
 - 16 **End For**
 - 17 **End Procedure**
-

- *Retrieving Data:* According to the requester's role as discussed in section IV-1-a, and the strict security access policies, the ability to access data as described in the Algorithm 2 is successfully passed through using the CID stored in the Blockchain network. The downloaded data from the IPFS network will be converted to readable status following the mandatory decryption and verification procedures.

Algorithm 2: Decompression, Decryption, Signature Verification Procedures – Healthcare Provider Side

Input: *CID* as a string, *Public_key_sender* an array of string, *Private_key_recipient* an array of string

Output: *Boolean* (*False*, *True*), *Decrypted_data* as an array of string


```

1  Import required Public_key_sender from
   PGPexch_chaincode
2  Create IPFS client instance
3  Check Permissions and roles
4  For (role == "Doctor") && (permission == "Granted")
   then
5    Check ShareCID_chaincode then get CID
6    Retrieve Data from IPFS with P<-ipfs.get("CID")
7    Start verification procedure: Verify (P,
   Public_key_sender) using GPG-edDSA
8    If (Verify(P) == valid) then
9      Decrypt Data RD(Md)<- (P, Private_key_recipient)
10     Decompress Data Md<-unzip.RD(Md)
11     Store Data locally add.local(Md)
12     Else, return False
13     End if
14 Else Deny access, return false
15 End For
16 End Procedure

```

Therefore, certain procedures listed in the algorithms above involve the use of Fabric SDK a relevant tool from the Hyperledger development kit, which requires essential security configurations to facilitate the interaction within the Blockchain network, while it can perform activities related to IPFS (send and retrieve) through predefined packages, in addition, it can offer a fundamental API for submitting to the ledgers and query elements [34].

4.4 Sharing approach related e-IPGPChain framework

The primary function of the healthcare monitoring system is to affirm a secure share link involving different network members while preserving data security, privacy, and high availability. The adoption of the Hyperledger Fabric Network accomplishes the objective of our framework by creating a private network aimed at secure transactions among entities. This ecosystem is adopted into our framework e-IPGPChain to ensure a data exchange approach incorporating multiple services and components such as the Fabric CA stands for Certificate Authority nodes, the endorsement policies likewise the PFBT (Practical Byzantine Fault Tolerance), and a relevant business logic workflow based on the RBAC policies developed using a Chaincode, as described from the algorithms below, also, the employment of private channel that represents an isolation environment including only the authorized members [5].

Following the network initiation, the CA nodes and MSP (Membership Service Providers) modules are responsible for issuing and managing the digital certificates for all members [21] to enable confidential communication. However, each member will be assigned a defined role for significant missions. The designed model to share information across the network adopted in e-IPGPChain is subject to the operational logic workflow as depicted on the subsequent Chaincodes:

- *Chaincode-related Public Key sharing:* Outlines the main process for sharing public keys with corresponding collaborators for encryption and digital signature purposes. The Algorithm 3 illustrates the procedures that start by checking the users' permissions and then proceed the chain according to the requested function to store or retrieve the public key within the network. The Fabric SDK is employed to call the appropriate functions related to the user's request.

Algorithm 3: Saving and Retrieving Public Key Algorithm over the Hyperledger Fabric Network

```

Input: Function_name to be called, args array of strings
Output: Boolean (Success, Failure)
1  For each user 'P', 'D', 'N', 'EM' Having access to the
   channel <pzone >
2  Check Permissions and roles
3  If function_name == StorePublicKey then
4  If args length is not 2, then return False
5  Else, store the value args[1] in the ledger with key
   args[0]
6  End if
7  If function_name == getPublicKey then
8  If ((args length is not 1) || (the retrieved value is
   empty)) then return False
9  Else, Retrieve the value associated with the key
   args[0] from the ledger
10 End if
11 Else Deny access, then output == "Failure"
12 End For
13 End Procedure

```

- *Chaincode-related CID exchanging process:* The adopted collaborative model through this Chaincode aims to provide the ability to submit and retrieve Content Identifiers (CID) based on RBAC policies, which reveals a high-level private sharing model as seen from the Algorithm 4 below. Therefore, the features affirmed within the Chaincode are called through developed Fabric SDK applications.

Algorithm 4: Chaincode-Related Sharing CID of Medical Data Based on Role Based Access Control Policy

```

Input: Function_name to be called, user_role an attribute,
CID array of strings
Output: Boolean (Success, Failure), CID array of strings
1  For each user 'P', 'D', 'N', 'EM' Having permission to
   access to the channel <pzone >
2  Check Permissions and roles
3  If (function_name == StoreCID) && (user_role ==
   "admin") then
4  store the CID in the ledger Else return False
5  End If
6  If (function_name == getCID) && (user_role ==
   "Doctor") then
7  Retrieve CID from the ledger, Else return False
8  End If
9  Else Deny access, then output == "Failure"
10 End For
11 End Procedure

```

5. TECHNICAL DEMONSTRATION AND SYSTEM EVALUATION

This part of the paper represents our technical prototype that describes the proposed decentralized model e-IPGPChain, which practically discloses the procedures described in the sequence diagram above. This implantation demonstrates the integration of the proposed technologies that work in a collaborative environment to deliver high-quality and secure medical services. However, evaluating the e-IPGPChain model at the end of this section indicates the compelling advantages of adopting such a solution, from both

performance and security aspects, while maintaining an open research perspective for further development.

5.1 Deployment strategy and configuration

The practical deployment of the proposed e-IPGPChain model relies on a combination of two Virtual machines, a physical computer, and different toolkits, as illustrated in Table 4 below. The Blockchain network was formed of one organization, four peers, and a unique Certificate Authority (CA) node leveraging the private features of the Hyperledger Fabric solution. The choice of this configuration is based on the tradeoff between Latency, Security, and Cost efficiency. Furthermore, the overall network makes use of software development and deployment tools including Docker, SDK tools, and others, contributing to building a robust blockchain network that embeds the attributes of Chaincodes, Channels, consensus algorithms, and Membership Service Providers, the entire network process is assisted by one VM to play the link role between the solution members.

The distributed storage is handled by IPFS on two designed machines to perform the sending and retrieving activities. Moreover, the network is characterized by: Patients, and Healthcare providers, using both physical and virtual machines, respectively. Therefore, preparing collected data requires the use of several toolkits, including Fabric SDK, IPFS client command lines, and the GPG-edDSA cryptographic tool. Each Patient profile integrates the edge devices using a unique session authentication mechanism characterized by a login and password, to enable the patient-personal directory where the corresponding private key and encrypted medical data are stored. However, The Fabric SDK [34] plays an essential role in creating end applications for executing authorized transactions over the blockchain network by leveraging some defined libraries such as the case for our framework, NodeJS. As a result, the final picture of the deployment strategy resides in making separate machines, A Physical one represents the Patient edge while a virtual machine depicts the healthcare provider edge zone, both machines integrate the Hyperledger Fabric network performed as a separate Virtual machine that ensures a secure link for sharing the CID of medical data in a protected collaborative environment.

Table 4. Technical deployment characteristics

Component	Setup Overview
Virtual Machines (VM)	6 CPU, 20GB RAM, 500 GB
Physical Machine	HP ZBook, Intel Xeon W-11955M, 8 CPU, 24 RAM
Docker	v. 23.0.1
Fabric Release	v. 2.3.0
Fabric SDK	v. 2.2
IPFS-Client	v. 0.21.0 (Kubo)
Deployed Languages	Go v go1.21.1 Linux/amd64, Node v14.21.3
GPG-edDSA	v. 2.2.19

5.2 E-IPGPChain comprehensive use cases

The proposed model relies on several scenarios to reveal the designed access control and cryptographic attributes to establish a resilient and safe sharing environment of medical records, considering security and accessibility approaches:

- Scenario 1:** Demonstrates role-based access control (RBAC), by showing a patient, with either a valid or invalid assigned role trying to submit a data identifier (CID) within the Blockchain Network. Starting with registering and assigning roles procedures. In case a patient without a validated role sends the CID on the network peers return as an invalid operation, referring to RBAC policy Failure permission. Conversely, if the Patient with the convenient admin role, the network successfully validates and transmits the transaction CID within the peer's ledgers, the process results are illustrated in Figure 3 and Figure 4.

```

wallet path: /root/mywork/Patient/shareCID/addUSER/wallet
2023-09-22T09:54:50.705Z - error: [Transaction]: Error: No valid responses from any peers. Errors:
peer-peer3.org:1.sante.gov.ua, status=500, message-caller does not have the 'admin' role: attribute 'role' equals 'user', not 'admin'
at newEndorsementError (/root/mywork/Patient/shareCID/app/node_modules/fabric-network/lib/transaction.js:74:12)
at getResponsePayload (/root/mywork/Patient/shareCID/app/node_modules/fabric-network/lib/transaction.js:41:23)
at Transaction.submit (/root/mywork/Patient/shareCID/app/node_modules/fabric-network/lib/transaction.js:255:28)
at processTicksAndRejections (internal/process/task_queues.js:95:5)
at async main (/root/mywork/Patient/shareCID/app/storeCID.js:61:9)
Failed to submit transaction: Error: No valid responses from any peers. Errors:
peer-peer3.org:1.sante.gov.ua, status=500, message-caller does not have the 'admin' role: attribute 'role' equals 'user', not 'admin'
  
```

Figure 3. Failed submission transactions – patient side

```

root@Patient-ED:~/mywork/Patient/ShareCID/app# node storeCID.js
wallet path: /root/mywork/Patient/ShareCID/addUSER/wallet
Transaction successfully submitted with CID: QmPzn57UFWesPQFJrh6LDAWA19sQDE1dgmU7bnHsWnqaZ
Transaction successfully submitted with CID: QmAvB4wMyhcJ9gj1qwmvV54BH3L3q79GJt851ukqdyUj
Transaction successfully submitted with CID: QmY1Ux6x68HT4r7LPwekTwZvac2X2LDppqvFAA997ZhsFq
Transaction successfully submitted with CID: QmVComj9wH2wHHAcg7WcgBFR14iCYU8DqhMgV7BvyTGFq
Transaction successfully submitted with CID: QmUteZuADnGFcas7LYANYVGU1SroPuegLCqk1pHcDxmj5n
  
```

Figure 4. Successful processed transactions - patient side

- Scenario 2:** Illustrates the process for doctors retrieving data based on their permissions. Doctors have two permission types Granted or Denied, to retrieve the CID from the Blockchain network. For the granted decision, with the user's appropriate role, this enable him to retrieve data and proceed with the decryption steps seamlessly, while the access is rejected to retrieve data for unauthorized reasons from the network as depicted from the Figures 5 and 6 below.

```

root@Doctor-ED:~/mywork/Doctor/RetrievCID/app# node getCID.js
wallet path: /root/mywork/Doctor/RetrievCID/addUSER/wallet
Failed to submit transaction: Error: caller does not have the 'Doctor' role: attribute 'role' equals 'Agent', not 'Doctor'
  
```

Figure 5. Unauthorized access to data within the blockchain - doctor side

```

root@Doctor-ED:~/mywork/FABRIC/test# node getCID.js
Wallet path: /root/mywork/FABRIC/cli/wallet
Retrieved CIDs:
CID: QmPzn57UFWesPQFJrh6LDAWA19sQDE1dgmU7bnHsWnqaZ
CID: QmUteZuADnGFcas7LYANYVGU1SroPuegLCqk1pHcDxmj5n
CID: QmVComj9wH2wHHAcg7WcgBFR14iCYU8DqhMgV7BvyTGFq
CID: QmY1Ux6x68HT4r7LPwekTwZvac2X2LDppqvFAA997ZhsFq
CID: QmAvB4wMyhcJ9gj1qwmvV54BH3L3q79GJt851ukqdyUj
  
```

Figure 6. Allowed retrieve transaction of data's CID from the blockchain ledgers - doctor side

- Scenario 3:** Covers data signature verification, ensuring that only valid, authenticated data is processed. Data after being encrypted, signed, and uploaded to IPFS. The requester can successfully verify and confirm the source of data as seen from Figure 7 and then proceed with the decryption and decompression steps through an exchanged key-based encryption mechanism. Otherwise, the Not verified status causes untrusted data as depicted in Figure 8, hence a failed decryption as a result.

```
gpg: encrypted with 256-bit ECDH key, ID A3E875C4FB1FD735, created 2023-09-27
"Doctor <Doctor@sante.gov.ma>"
gpg: Signature made Thu 28 Sep 2023 07:40:16 PM UTC
gpg: using EDDSA key 2D327E3BD9AF585D585FF37E06FD96596237EB33
gpg: Good signature from "Patient <Patient@sante.gov.ma>" [ultimate]
```

Figure 7. Matched signature and successful decryption procedures

```
gpg: key 4C2386E4541E37A6: "omar < >" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
gpg: encrypted with 256-bit ECDH key, ID A3E875C4FB1FD735, created 2023-09-27
"Doctor <Doctor@sante.gov.ma>"
gpg: Signature made Thu 28 Sep 2023 07:40:16 PM UTC
gpg: using EDDSA key 2D327E3BD9AF585D585FF37E06FD96596237EB33
gpg: Can't check signature: No public key
Decryption failed.
```

Figure 8. Failed verification and decryption procedures

5.3 Performance-driven evaluation related to e-IPGPChain

We enabled an effective evaluation for e-IPGPChain to verify the performance ability of different deployed technologies from multiple perspectives including Latency, Scalability, Storage efficiency, and benchmarking data process. The Hyperledger Foundation community [35] recommend several projects for decentralized projects, where Hyperledger caliper is a part of it. This solution is used to measure the performance of various types of Blockchain network technologies using many pre-build configurations [36]. Consequently, related to our deployment strategy we used this benchmarking tool to evaluate the performance of the system based on numerous indicators such as Throughput TPS (Transaction per second), Transaction latency, and resource utilization. In our case, conducting the system evaluation requires various benchmarking configurations, as highlighted in the following points:

- **Latency:** Denotes the complete time elapsed by a transaction from initiation to response [37].
- **Implementation setup:** our analysis of the Latency of incorporating sending Transactions at various durations, starting with 60, 120, 180, 240, 300, 360, 420, 480, 540, and 600 seconds, which provide insight into the system response capability at high load during scenarios case.
- **Result Discussion:** Figure 9 below reveals important metrics results related to the latency analytics. During all defined periods, the maximum latency achieved by transactions workload seems optimal regardless of the increase in transactions over time for an e-health system to deliver medical services at acceptable levels.
- **Scalability:** Assess the system's capacity to effectively manage the intensive increase of data and users, particularly in the case of integrating IoMT technology while guaranteeing efficient service delivery [15].
- **Implementation setup:** we arranged the system to accommodate an increased number of transactions starting with 500 transactions, ending with 10000 Transactions submitted to the network at a linear rate starting with 15 Tps and finishing the process with 75 Tps. This use case incorporates the execution of three workers simultaneously. Therefore, another test scenario was performed to assess the system's ability on multiple structure implementations, using a regular number of transactions of 2000 at a fixed throughput of 50 Tps, to

experiment with the scalability of our framework in case of further extended deployment.

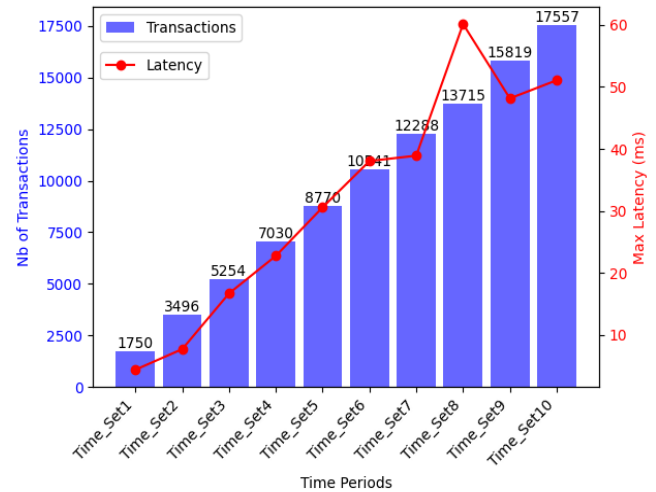


Figure 9. Latency evaluation with a related number of transactions over defined periods

- **Results discussion:** After conducting several benchmarking rounds, as previously detailed, the system still preserves optimal resource operation as indicated by the Figure 10 below at the increased workload. On the other side, sending the same quantity of transactions to different implemented structures reveals efficient output results, where the throughput preserves an admissible rate, that is realized in ten peer networks, 31.4 Transaction per second as shown from the Figure 11, while the average latency depicts reasonable results varying between 5.45 ms to 16.56 ms for a structure with 10 peers where the ideal response time for the health sector should be less than 200 ms to provide real-time medical services [38]. Consequently, the e-IPGPChain solution responds to the current and future growth of data volume which makes it a scalable structure for healthcare delivery services.

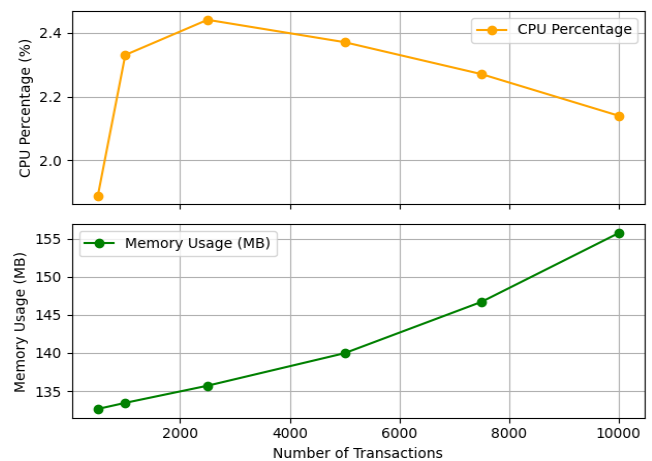


Figure 10. Blockchain efficiency with exponential increase of transaction numbers

- **Storage efficiency:** Maintain an optimal use of the system's storage resources, resulting in consistent and extended access to medical data.
- **Implementation setup and discussion:** Adopting the

Hybrid storage model incorporates edge computing and IPFS to help balance the storage resources, while including the GPG-related compression algorithms to reduce the size of collected data depending on various factors such as the type of data being compressed, the compression algorithm used, and the compression level specified [29].

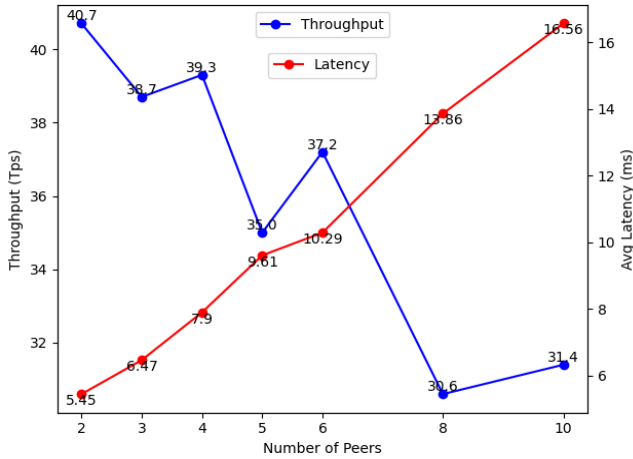


Figure 11. Exploring latency and throughput evaluation with varying numbers of blockchain network peers

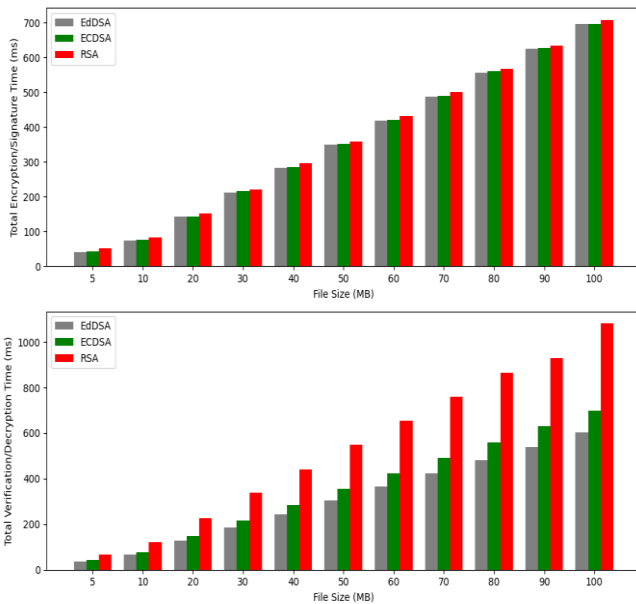


Figure 12. Medical data total time processing evaluations

- **Data Process Evaluation:** Managing related Data is the most important step to deliver secure healthcare services within optimal resource utilization, including encryption, digital signature, and verification.
- **Implementation setup:** The effectiveness of the cryptographic tool, GPG-edDSA is evident through a series of benchmarking tests targeting the total execution time of the Encryption and Signature procedures, in addition to the decryption and verification total process time. By leveraging performance evaluation tools to assess the processing time for different file sizes to conduct the cryptographic operations, the objective is to demonstrate the efficiency of the adopted solution algorithm.

- **Results discussion:** The results analysis from the figures below highlights the efficiency of the GPG-edDSA scheme over the widely used mechanisms including GPG-RSA and GPG-ECDSA by performing test cases using different file sizes. The time taken in data encryption and signature seems equitable with a small positive outperforming for GPG-edDSA, while for decryption and verification processes, the proposed tool proves how efficient and faster compared to others. The obtained results seen from Figure 12, contribute to the overall performance system and even enhance security and privacy with the latest advanced techniques.

5.4 Security assessment

5.4.1 Threat model-based STRIDE

Security Threat modeling is a technique to evaluate the system's security aspect and help to reinforce the overall components from multiple threats' impact. Among all the modeling options, the Open Web Application Security Project (OWASP) provides an open-source tool used to indicate possible threats and select related countermeasures following visual model illustration and based on standard threat frameworks including STRIDE, LINDDUN, CIA, as described in Table 5 [39] playing an important role in classifying the risks and applying the countermeasures.

Table 5. OWASP threat frameworks overview

Terminologies	Definitions
CIA	Confidentiality, Integrity, Availability
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges
LINDDUN	Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance

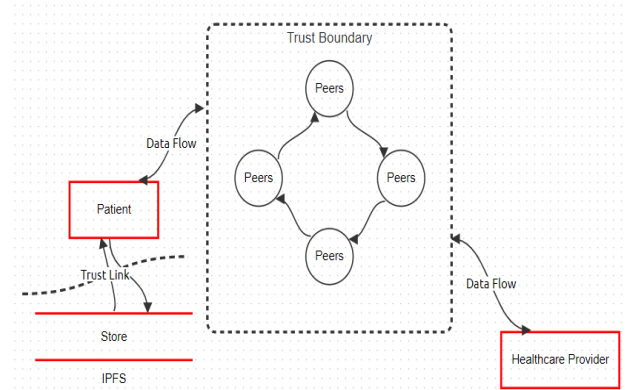


Figure 13. Threat model representation related to e-IPGPChain solution

To analyze our proposed solution, we employ the OWASP threat dragon tool. The process involves the contribution of multiple mechanisms encompassing the complete system's components. Figure 13 describe the threat model following the STRIDE framework, demonstrating how the basic network structure can face multiple threats that impact the normal process of the healthcare monitoring system. However, the proposed e-IPGPChain came over to mitigate the uncovered threats according to the STRIDE standard focused on

particular sections to address main security and privacy challenges related to medical data sharing workflow.

Following the deployment strategy, the threat model involves:

- **Actors:** Identifies the main system contributors as listed:
 - Patients: Assigned to produce and handle medical data, responsible for storing and manipulating personal data.
 - Healthcare Providers: Includes main health stakeholders authorized to access medical data, the scope of their roles defined based on the mission category they undertake.
- **Assets:**
 - Medical Data: Represented as a sensitive vital sign indicator measuring patient health conditions.
 - Patient Privacy: Identify the private attributes related to patients including personal information.
 - System, data availability: Determines the system resiliency and accessibility under all consequences.
 - Data Integrity: Preserving data unchanged along the sharing process with different stakeholders.
 - User Accessibility: Describes the process of accessing systems and services with security directive mechanisms.
- **Adversaries:**
 - Outside Threats: Represent health organizations, external users, and Individual cybercriminals. Inside Threats: These involve authorized users within the system who may have been compromised.
 - Malicious campaigns: External network Ver/Viruses, System Bugs, vulnerable system components.
- **Identifiable threats:** According to the security STRIDE framework, it is possible to identify the potential threats that may affect the system's efficiency and privacy as resumed in the Table 6 above. The identification of threats based on the current Cybercriminal effects.
- **Mitigation strategies:** the emergent technologies implemented in e-IPGPChain solution can effectively mitigate various security and privacy issues for sharing medical data process. The deployed techniques can reduce the threats occurring as seen from Table 6.

a. Cyber risk evaluations

The integration of various technologies and external stakeholders exposed the system architecture and personal data to critical potential Cyber-attacks and security threats. Building the system model based on threat modeling approaches helps to minimize the security risk to systems by identifying the weak points simulated within a particular technology. Nowadays, Medical data is increasingly targeted by several cyber-criminal organizations [40], in order to violate the trust and patient privacy, financial fraud, disrupting clinical services and social impacts. Our proposed framework work was evaluated based on these common potential attack vectors:

- **Man-in-the-middle attack:**

The attacker tries to find a way between the data owner and the authorized requester to manipulate content for tampering and fraud. Our proposed framework employs robust authentication and authorization mechanisms using paired cryptographic keys exchanged safely through blockchain network based RBAC policies to successfully ensure data encryption and digital signature.

As a sample of the basic transaction of sending data between Patient X and Healthcare Provider Y. In advance, X uses Y's public key to encrypt and digitally sign data eq (4). Y after receiving CID based on matched Role within the network, can retrieve data and uses X's Public key to verify data and decrypt based on eq (9), (5). As a result, the attacker is unable to share public keys referring to strongly defined access control even if it prevents data decryption due to an incorrect private key.

- **Distributed denial of service:**

Adversaries attempt to make interesting services difficult or unable to access, by dumping the target systems such as edge devices, IPFS, and Blockchain networks with excessive requests, disrupting the availability of healthcare monitoring systems.

The scalable structure, duplicated network peers, and redundancy storage capability of our proposed solution can reduce DDoS impacts and continue the accessibility to medical data in critical situations, as demonstrated in the performance evaluation section with stressed test cases, the system still delivers full functionality with the best latency rate.

Table 6. e-IPGPChain security evaluation-based STRIDE Threat model related corresponding mitigations

Identifiable Threats	STRIDE Categories	Mitigation Strategies
Threats related to impersonation or gaining unauthorized access by exploiting user credentials through Phishing Attacks and Man-in-the-Middle (MitM).	Spoofing	Strong authentication and authorization mechanism for access to edge computing and performing Actions within the Hyperledger Fabric network.
Outlines the unauthorized manipulation of medical data, causing potential harm produced through Data Breaches and Repay attacks.	Tampering	Using Encryption Techniques to reinforce the integrity and non-repudiation of data.
Focus on challenging the authenticity and the integrity of targeted data, this threat is related to non-repudiation attacks.	Repudiation	Adopting lightweight and highly secure digital signatures in addition to blockchain sharing workflow.
Threats contribute to exposing medical information through exploiting some adversarial attacks including, eavesdropping and data breaches.	Information Disclosure	Implement a strong encryption mechanism based on exchanging keys over a blockchain network.
Threats related to disrupting the system accessibility and making resources unavailable. Take advantage of Distributed Denial of Service (DDoS) attacks that affect the system workflow.	Denial of Service	Incorporating Hybrid Storage functionality targeting the high availability in addition to deploy adopt decentralized structure.
Threat exploiting the vulnerabilities to gain a high level of access to resources and even perform unauthorized operations through several attacks such as privilege escalation.	Elevation Escalation	The private keys and Blockchain profiles issuing process is totally secure and Private.

- *Replay attack:*

An attacker can intercept and replay messages, which can pretend to be a legitimate user to other parties. In our scheme, a unique ID mechanism is attached for each transaction which can prevent such attacks.

For example, when a patient wants to send a transaction, each data has a unique <cid> that is attached to an incremental id index, as these IDs can be ordered to prevent misrepresentation of the transaction order. The recipient can verify the CID and check the incremental ID to ensure the transaction order is correct. This prevents replay attacks, as the attacker cannot reuse old CIDs due to the sequential ID index.

- *Key management vulnerabilities:*

The cryptographic key management process can be targeted by attackers to attempt to collect sensitive user keys for unauthorized access to manage paired keys.

Our approach establishes personal directories with secret GnuPG folders, as an example for Patient X, *~/gnupg/private-keys-v1.d*, where keys are safely stored. Additionally, the public key generation and encryption processes are ensured by the concerned owner, who is required to provide a predefined passphrase for each action. As a result, access control solutions for edge and blockchain technologies make it difficult for malicious actors to gain access and tamper with the protected key directories.

6. CONCLUSIONS

The vast requirement for healthcare services involves the deployment of advanced technologies to fulfill the need for a data-sharing model secure and performant. The extensive use of IoMT devices to collect medical records and the big data analysis constraint reveal critical challenges to managing the huge volume of data and ensuring real-time accessibility.

Our approach, e-IPGPChain leverages Hyperledger Fabric and incorporates IPFS for distributed storage, in addition to edge computing resources for maintaining a performant data processing strategy. Moreover, medical data is highly protected by using a strong and flexible cryptosystem tool GPG-edDSA, ensuring encryption and digital signature procedures. Additionally, the hybrid storage feature guaranteed through Edge resources and IPFS technologies improves high data accessibility, availability, and global system reliability, as demonstrated by conducting multiple benchmarking test cases. From the security perspective, the STRIDE threat model defines the key elements that are used to reinforce our proposed solution, via employing different mechanisms on e-IPGPChain to perform secure data exchange. Exposing our scheme to various cyber-attacks reveals the strongly implemented techniques to address the limitations of existing solutions to protect data workflow.

This solution remains open for further improvement, particularly in reducing the complexity of the overall system, and aligning the solution's modules with key regulatory frameworks such as HIPAA, and GDPR. Currently, the encryption technique lacks relevant security measures to protect keys against potential risks like side-channel attacks and a lightweight solution to improve performance efficiency. The limited compatibility of the encryption and the digital signature algorithm used can potentially lead to interoperability issues, that impact the system stability, and disrupt healthcare delivery services.

REFERENCES

- [1] Rafik, H., Maizate, A., Ettaoufik, A. (2023). Data security mechanisms, approaches, and challenges for e-health smart systems. *International Journal of Online and Biomedical Engineering (iJOE)*, 19(2): 42-66. <https://doi.org/10.3991/ijoe.v19i02.37069>
- [2] Healthcare Data Breach Statistics. *HIPAA Journal*. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.
- [3] McKeon, J. (2023). Biggest healthcare data breaches reported this year, so far. *Health ITSecurity*. <https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far>.
- [4] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, V. (2021). BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain. *IEEE Internet of Things Journal*, 8(14): 11743-11757. <https://doi.org/10.1109/JIOT.2021.3058953>
- [5] Chen, C.L., Yang, J.X., Tsaur, W.J., Weng, W., Wu, C.M., Wei, X.J. (2022). Enterprise data sharing with privacy-preserved based on Hyperledger Fabric blockchain in IIOT's application. *Sensors*, 22(3): 1146. <https://doi.org/10.3390/s22031146>
- [6] Mohurle, S., Patil, M. (2017). A brief study of wannacyr threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5). <https://doi.org/10.26483/ijarcs.v8i5.4021>
- [7] Chentharra, S., Ahmed, K., Wang, H., Whittaker, F., Chen, Z.X. (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>
- [8] Koch, W. (2015). EdDSA for OpenPGP. draft-koch-eddsa-for-openpgp-03. <https://datatracker.ietf.org/doc/draft-koch-eddsa-for-openpgp-03>.
- [9] Yakubov, A., Shbair, W., State, R. (2018). BlockPGP: A blockchain-based framework for PGP key servers. In 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, pp. 316-322. <https://doi.org/10.1109/CANDARW.2018.00065>
- [10] Ri, O.C., Kim, Y.J., Jong, Y.J. (2022). Blockchain-based RBAC Model with Separation of Duties constraint in Cloud Environment. *arXiv*, 2203.00351. <https://doi.org/10.48550/ARXIV.2203.00351>
- [11] Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F.L., Yi, X., Yang, X.C., Amarasinghe, G., Chen, S.P. (2020). Public and private blockchain in construction business process and information integration. *Automation in Construction*, 118: 103276. <https://doi.org/10.1016/j.autcon.2020.103276>
- [12] Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., Khalaf, O.I. (2021). Hyperledger healthchain: Patient-centric IPFS-based storage of health records. *Electronics*, 10(23): 3003. <https://doi.org/10.3390/electronics10233003>
- [13] Margheri, A., Masi, M., Miladi, A., Sassone, V., Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, 141: 104197. <https://doi.org/10.1016/j.ijmedinf.2020.104197>
- [14] Rajput, A.R., Li, Q.M., Ahvanooy, M.T. (2021). A

- blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthcare*, 9(2): 206. <https://doi.org/10.3390/healthcare9020206>
- [15] Abdelgalil, L., Mejri, M. (2023). HealthBlock: A Framework for a collaborative sharing of electronic health records based on blockchain. *Future Internet*, 15(3): 87. <https://doi.org/10.3390/fi15030087>
- [16] Egala, B.S., Pradhan, A.K., Gupta, S., Sahoo, K.S., Bilal, M., Kwak, K.S. (2022). CoviBlock: A secure blockchain-based smart healthcare assisting system. *Sustainability*, 14(24): 16844. <https://doi.org/10.3390/su142416844>
- [17] Alsayegh, M., Moulahi, T., Alabdulatif, A., Lorenz, P. (2022). Towards secure searchable electronic health records using consortium blockchain. *Network*, 2(2): 239-256. <https://doi.org/10.3390/network2020016>
- [18] Kumar, R., Marchang, N., Tripathi, R. (2020). Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In 2020 International Conference on COMMunication Systems & NETWORKS (COMSNETS), Bengaluru, India, pp. 1-5. <https://doi.org/10.1109/COMSNETS48256.2020.9027313>
- [19] Jayabalan, J., Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, 164: 152-167. <https://doi.org/10.1016/j.jpdc.2022.03.009>
- [20] Ali, H., Ahmad, J., Jaroucheh, Z., Papadopoulos, P., Pitropakis, N., Lo, O., Abramson, W., Buchanan, W.J. (2022). Trusted threat intelligence sharing in practice and performance benchmarking through the Hyperledger Fabric platform. *Entropy*, 24(10): 1379. <https://doi.org/10.3390/e24101379>
- [21] Introduction - hyperledger-fabricdocs main documentation. <https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html>, accessed on Oct. 26, 2024.
- [22] Adlam, R., Haskins, B. (2019). A permissioned blockchain approach to the authorization process in electronic health records. In 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, pp. 1-8. <https://doi.org/10.1109/IMITEC45504.2019.9015927>
- [23] What is IPFS? | IPFS Docs. <https://docs.ipfs.tech/concepts/what-is-ipfs/#defining-ipfs>, accessed on Dec. 22, 2023.
- [24] Chen, J.N., Zhang, C., Yan, Y., Liu, Y. (2022). FileWallet: A file management system based on IPFS and Hyperledger Fabric. *Computer Modeling in Engineering & Sciences*, 130(2): 949-966. <https://doi.org/10.32604/cmescs.2022.017516>
- [25] Benet, J. (2014). IPFS - content addressed, versioned, P2P file system. *ArXiv*, 1407.3561. <http://arxiv.org/abs/1407.3561>
- [26] Kaur, M., Gupta, S., Kumar, D., Raboaca, M.S., Goyal, S.B., Verma, C. (2023). IPFS: An off-chain storage solution for blockchain. In Proceedings of International Conference on Recent Innovations in Computing, Springer, Singapore, pp. 513-525. https://doi.org/10.1007/978-981-19-9876-8_39
- [27] Merkle, R.C. (1990). A certified digital signature. In: Brassard, G. (eds) *Advances in Cryptology — CRYPTO'89 Proceedings*. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, New York, NY, pp. 218-238. https://doi.org/10.1007/0-387-34805-0_21
- [28] Garfinkel, S. (1995). PGP: Pretty Good Privacy. O'Reilly Media, Inc.
- [29] Syed, D., Al-Ghushami, A.H., Zainab, A., Abdulhamid, S.M., Al-Kuwari, M.S.D.A. (2023). Information security using GNU privacy guard. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). <https://doi.org/10.1109/ccwc57344.2023.10099196>
- [30] Josefsson, S., Liusvaara, I. (2017). Edwards-curve digital signature algorithm (EdDSA). Internet Engineering Task Force, Request for Comments RFC 8032. <https://doi.org/10.17487/RFC8032>
- [31] What Is the Internet of Medical Things (IoMT)? | Definition from TechTarget. IoT Agenda. <https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things>, accessed on Sep. 5, 2023.
- [32] Advanced Encryption Standard. (2023). Wikipédia. https://fr.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=207176364, accessed on Oct. 5, 2023.
- [33] Content Identifiers (CIDs) | IPFS Docs. <https://docs.ipfs.tech/concepts/content-addressing/>, accessed on Jan. 15, 2024.
- [34] Hyperledger Fabric SDK for Node.js. <https://hyperledger.github.io/fabric-sdk-node/>, accessed on Oct. 15, 2023.
- [35] Projects | Hyperledger. <https://www.hyperledger.org/projects>, accessed on Oct. 26, 2023.
- [36] Sukhwani, H., Wang, N., Trivedi, K.S., Rindos, A. (2018). Performance modeling of Hyperledger Fabric (permissioned blockchain network). In 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, pp. 1-8. <https://doi.org/10.1109/NCA.2018.8548070>
- [37] Al-Sumaidae, G., Alkhudary, R., Zilic, Z., Swidan, A. (2023). Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. *Information Processing & Management*, 60(2): 103160. <https://doi.org/10.1016/j.ipm.2022.103160>
- [38] Qureshi, H.N., Manalastas, M., Ijaz, A., Imran, A., Liu, Y.K., Kalaa, M.O.A. (2022). Communication requirements in 5G-enabled healthcare applications: Review and considerations. *Healthcare*, 10(2): 293. <https://doi.org/10.3390/healthcare10020293>
- [39] OWASP Threat Dragon | OWASP Foundation. <https://owasp.org/www-project-threat-dragon/>, accessed on Oct. 26, 2023.
- [40] Alder, S. (2024). January 2024 healthcare data breach report. *HIPAA Journal*. <https://www.hipaajournal.com/january-2024-healthcare-data-breach-report/>, accessed on Jan. 20, 2024.