IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 June 2022, accepted 8 September 2022, date of publication 12 September 2022, date of current version 12 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3206046

RESEARCH ARTICLE

Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks

SABRI BARBARIA[1], MARCO CASASSA MONT[2], (Senior Member, IEEE), ESSAM GHADAFI[3], HALIMA MAHJOUBI MACHRAOUI[1], AND HANENE BOUSSI RAHMOUNI[1,4]

[1]Laboratory of Biophysics and Medical Technologies, Higher Institute of Medical Technologies of Tunis (ISTMT), University of Tunis El Manar, Tunis 1068, Tunisia
[2]BMT, U.K. Cyber Security Management Consulting, Teddington TW11 0AP, U.K.
[3]School of Computing, Newcastle University, NE1 7RU Newcastle, U.K.
[4]Computer Science Research Centre, University of the West of England, BS16 1QY Bristol, U.K.

Corresponding author: Sabri Barbaria (sabri.barbaria@istmt.utm.tn)

ABSTRACT Nowadays, due to the evolution of information technologies and their adoption in the healthcare domain, new risks to medical data protection and patient privacy are increasingly present. It is therefore important to implement approaches that can prevent rapidly emerging cyber-attacks. Essentially, the adoption of cyber security measures in healthcare should be oriented towards a better assurance of patient rights and consent management. Blockchain is one of the most advanced technologies that can deal with many types of cyber threats ensuring the integrity, availability, and privacy of the data. It adds elements of trust and traceability to the data exchange processes deployed within Hospital information systems and beyond. In this paper, we study the usability of blockchain in the healthcare domain and we develop a data exchange approach based on the Hyperledger Blockchain model. The focus here will be mainly on privacy concerns and the integration of patient consent in the data-sharing operational controls.

INDEX TERMS Blockchain, hyperledger fabric, privacy, healthcare data management, healthcare IT.

I. INTRODUCTION

Nowadays, cybersecurity and privacy are some of the most important topics due to the big evolution of technologies and the number of technology users. The health information domain is one of the most important sectors that have a very crucial impact on our life, it manages our sensitive health data. For that, many technology standards have been proposed to protect this data when shared within hospital environments and beyond. In addition, due to the increased interest in the quality and quantity of the data that is the core of the healthcare IT systems many new threats to privacy and data availability have been occurring. In particular, the increased number of reported data breaches is nowadays considered a critical issue. This includes incidents related to compromising sensitive information about patients' medical histories [1]. Consequently, much research work and hospital engineering activities are making hospital network security a primary IT concern [2]. Hospital information systems (HISs) make it possible for physicians and other healthcare professionals to share essential information. This has facilitated the collaboration of healthcare professionals and multidisciplinary clinical networking to operate dynamically and better meet patients' needs. It is also worth noting that in addition to a patient's records, medical providers' networks can contain valuable financial information. This has particularly been the case since billing and payment systems have become a factual modular component of HIS [3]. The interconnected nature of HISs and the shortcoming of existing solutions to create fine-grained and holistic security and data protection measures increase the chance of hackers getting access to the data that has been collected under patients' names for years. Sharing patient information is integral to providing the best possible treatment to patients, but that same sharing also makes networks extremely valuable targets. This can affect the evolution of IT adoption in the healthcare domain and could disturb the current sustainability model [4]. A seamless move to evolving to an architectural trend such as Healthcare

The associate editor coordinating the review of this manuscript and approving it for publication was Mingjun Dai.

4.0 will not be as achievable as in other industrial or financial domains. Hence, new solutions need to be implemented to cover the current approach and add new layers to ensure the integrity and availability of the data.

A. BENEFITS OF THE BLOCKCHAIN TECHNOLOGY

Blockchain is one of the promising technologies that can ensure privacy, integrity and data protection in many applications including eHealth and health information systems it is beneficial due to its decentralized, immutable, transparent and secure nature. These features are most suitable to deal with the complex and decentralised mode of patient information exchange and storage. In fact, if properly implemented, blockchain-based medical records systems might be significantly more accurate, secure, and accessible than the one-size-fits-all approach used in today's electronic health records. It also allows patients to have more control over their data. The adoption of these technologies has been shown to reduce the chances of electronic medical records malfunctioning. It offers greater access flexibility without jeopardizing patient privacy, which is especially important when storing big amounts of data. This is conceivable because a blockchain is, at its core, a cryptographically enforced ledger that ensures the integrity of the data stored on it. When used to secure medical data, blockchain can store data in a way that is open to all users on the network, entirely unchangeable, and tamper-proof. Doctors, nurses, and other stakeholders would be able to control the flow of information from a single, trusted platform with electronic health records. Everyone would have access to the same information, and any changes would be accessible to the entire network very instantly. This means that medical users can be confident that the information they obtain about a patient is both accurate and up to date. The benefits of blockchain technology are frequently discussed for a large variety of medical use cases and applications applicable to the context of Health4.0. particularly there is widespread agreement that its role could transform drug development and supply chain management, clinical trial management, remote healthcare delivery to patients, and much more while allowing multidisciplinary teams to work on the same medical case simultaneously from a distance.

Using advanced cryptographic algorithms and ledger/block-based access controls, blockchain could make patients more in control and provide them with a higher level of privacy. Indeed, these technologies enable more efficient patient deidentification and reidentification methods. This is achieved by keeping identifiable and anonymized data about the same patients in separate blocks and assigning each one different access and permissions. Furthermore, we could improve provenance and patient consent management by utilizing blockchain-based smart contracts. It is therefore possible to enforce temporal and spatial limitations for data access in a seamless manner. For example, consent could be given by the patient for a limited duration.

B. THE BLOCKCHAIN TECHNOLOGY AND HEALTHCARE REGULATION

It was first developed by Satoshi Nakamoto in 2008 through his Bitcoin cryptocurrency technology [5]. Since that many works were produced focusing on blockchain technology, especially in the healthcare domain. For example, in [6] the authors have examined the data protection on multiple distributed ledger technologies like blockchain and have shown how to apply existing regulations like the General Data Protection Regulation (GDPR). They concluded that blockchain if adequately designed in a way that is compliant with GDPR, can share a common objective: giving a data subject more control over their healthcare data. Thereby using blockchain can narrow the gap between text law and technical policies by implementing automated actions (smart contracts) derived from contractual conditions and actual legal contracts. Trusted automation brought by smart contracts, combined with the finality of transactions in the blockchain, is likely what makes blockchain the most powerful (and also potentially disruptive) innovation of recent times, opening the door to more efficient, more automated services and new business models, especially in the healthcare context. In [7] they suggested a framework to share healthcare data using blockchain technology and IHE profiles. In [8] the authors use a blockchain-based approach to support data accountability and provenance tracking. The approach relies on the use of publicly auditable contracts deployed in a blockchain that increases the transparency concerning the access and usage of data to confirm GDPR compliance. In [9] they provide an overview of the potential for blockchain technology in the healthcare systems to overcome the challenges related to data security, privacy, sharing and storage in the domain and present many use cases. Nevertheless, blockchain can be used in many use cases in the healthcare domain like protecting the integrity of clinical trial results. In fact, blockchain could be used to ensure that data is collected and exchanged, when necessary while respecting patient privacy or proprietary information. Immutable records applied to clinical trials, protocols and results that can result in time stamps among others could solve the problems of results changing, data snooping and selective reporting. This could effectively reduce the incidence of fraud and errors in clinical trial records. In addition, blockchain can bring transparency to clinical trials. Indeed, it could be used by pharmaceutical industry applications to authenticate and track clinical trial results. Tracking results is also required from the patient side, particularly for those who would benefit from positive results or who might be worried about post-trial complications. Nevertheless, from a legal point of view, the right of access is a right to know. It might be required simply as the expression of one's curiosity. It is a right recognised by the individual whose data is being processed by various legal instruments, including the GDPR in article 15 [10]. This access to personal health data could be done via the blockchain. The blockchain could enable patients to control their data and manage access to it. Each patient could thus set up his or her medical profile in such a

way as to authorize access (total or partial) to the people of his or her choice (attending physician, family, etc.).

C. THE BLOCKCHAIN TECHNOLOGY CHALLENGES IN HEALTHCARE

The blockchain gives a reliable solution for particular healthcare function challenges specifically, confidentiality, integrity, and accessibility. However, this technology comes with its own set of challenges that should be addressed, like:

- Security: In [11] and [12] the authors address the security issues and challenges of blockchain technologies. Mainly the blockchain protection vulnerabilities are frequently connected to issues through the traditional consensus system utilized for verifying and confirming transactions. Consensus system techniques are incapable of preventing these security threats in the shared blockchain mechanism. In [13] the authors study the security challenges and opportunities for smart contracts in IoT mentioning the critical necessity for smart contract security and the necessity of smart contract regulation to improve the quality and security of the smart contract.
- Privacy: In [14] the authors highlighted the security and privacy issues of the blockchain technologies, the main challenge is patient consent, Present secure transmission structural designs of EHR disregard users or patients' privacy, like the replacing method useful every information without the authorization of owners or noise in the data requester review. The key challenge of keeping the confidentiality of patient information is by offering a structure that utilizes cryptographic systems to information confidentiality and reliability on a blockchain.
- Latency and throughput restrictions in the case of transaction latency, a blockchain gets time to process transactions.
- Interoperability and Standardisation: In [15] proposed application-level interoperability for blockchain networks mentions that interoperability is one of the crucial challenges preventing widespread adoption of blockchain applications. Several technical challenges must be addressed to healthcare data transferred information to the blockchain tools. The alive healthcare ledger (database) is not shared that cannot be combined or grow on a large scale.
- Social Challenges: Blockchain technology is still evolving, and therefore faces social challenges, like a cultural shift, besides the aforementioned technical challenges. Accepting and adopting a technology that is completely different from traditional work methods never comes easy. Although the medical industry is slowly moving towards digitization, there's still a long way to go for it to completely move on to this technology, especially ones like blockchain—which has yet not been validated in clinical aspects [16].
- Right to "Delete": Many data privacy laws protect patients and allow the right to remove data, which is a difficult accomplishment in blockchains because data may live on millions of computers around the world, may have no governing central authority, and may have been designed to be immutable. Data pseudonymization can alleviate some of the regulatory constraints connected with deletion. A piece of data can only identify a consumer when paired with additional data under pseudonymization, however, it remains to be seen if blockchain art provenance systems can fulfil the pseudonymization criteria [17].

D. PAPER STRUCTURE

In this paper, we propose an approach for health data sharing using blockchain to tackle problems of data integrity and protection. The rest of the paper is structured as follows. In sections 2 and 3 we present the state of art and technology choices with a comparative study with our contribution. In section 4 we introduce the system design and the modelling approach. In section 5 we present a security analysis. We dedicate section 6 to results and discussion. Section 7 presents our system performance. Finally, Section 8 concludes the paper by summarizing the objectives reached and open challenges.

II. BACKGROUND AND RELATED WORK

A. HEALTHCARE IT

Health information technology (HIT) is the application of information processing involving both computer hardware and software that deal with the storage, retrieval, sharing, and use of health care information, health data, and knowledge for communication and decision-making [18], [19]. It is one of the important domains that directly affect our life by improving the effectiveness and increasing the efficiency of the health facilities. In [20] The authors examine the digital transformation in healthcare and conclude that research is needed on the transformation of business models and its related implications for the management of different stakeholders' profiles and created values, including patients, providers and insurers.

B. HEALTHCARE DATA MODELS

A data model is a structure used to store information about a subject. Data comes in as a part of the workflow that providers are using. Data models often aid communication between the business people defining the requirements for a computer system and the technical people defining the design in response to those requirements; they are used to show the data needed and created by business processes [21]. In healthcare, the data models are crucial to providing better patient outcomes with greater levels of safety [22]. In [23] the authors compare four blockchain technology platforms and focus on their business-level properties including actors and roles, services, processes, and data models. In [24] the authors

design and implement a standardized framework to generate and evaluate patient-level prediction models using observational healthcare data, based on existing best practices.

C. DATA MANAGEMENT IN HEALTHCARE

Data Management in healthcare includes organizing, cleaning, retrieval, data mining, and data governance. It also includes the method of validating whether there is some scrap data or any missing values. The healthcare industry is one of the world's biggest and widest developing industries and healthcare management around the world is changing from disease-centred to a patient-centred model and from volume-based to a value-based healthcare delivery model [25].

In [26] the authors developed a privacy protection method for health, they established the risk access control model based on fuzzy theories. In [27] the authors show that there is a need for a secure and efficient health data management system that will allow physicians and patients to update decentralized medical records. They study the evolution and requirements of health data management systems over the years. They conclude that there is a need for a comprehensive real-time health data management system that allows physicians, patients, and external users to input their medical and lifestyle data into the system.

D. CYBER-THREATS IN HEALTHCARE IT

A Cyber threat is a malicious act by an individual or organization to steal data and damage the computer, systems, and networks. The threats included in cyber-attacks are malware, phishing, denial of services and data breaches. A smart healthcare environment necessitates the use of storage and network technologies. The use of such technologies adds to the risk of violating patients' data privacy [28]. In [29] the authors study the opportunity and challenges of big data and Cyber-Physical Systems (CPS) in the healthcare field. They mention three important points:

- The healthcare industry continues to be one of the most susceptible to publicly disclosed data breaches.
- Traditional security methods are no longer capable of fully defending the network against advanced intrusion attacks.
- A single system that considers all challenges (reliability, scalability, security, and ease to use) in healthcare big data does not exist [29].

In [28] the authors presented a reference to smart healthcare architecture and its components. The architecture refers to the use of the Federal Information Security Management FISMA and the Health Insurance Portability and Accountability Act (HIPAA). They also provided a classification of the various studied threats targeting the previously described principles and regulatory controls. In [30] the authors present a systematic literature review on cyber risk in the healthcare sector they highlight the need for further studies to empirically investigate the cyber risks especially those connected to some classes and subclasses of operational cybersecurity

FIGURE 1. Blockchain blocks the first block of the chain called genesis, which is common to all clients in a blockchain network and has no parent.

risks. Reading through [31] we notice that the authors have detailed ways hackers can attack hospital data networks, medical device data systems, and hospital building control systems. They have also made good coverage of the possible cyber-attack that can happen in healthcare facilities. In [32] the authors mentioned the growth in the number of cyber-attacks during the COVID-19 pandemic and summarised the reported cyber-attacks/data breaches in healthcare and academic organizations during the outbreak. They highlighted the need for a solution that can prevent the attack from happening and upgrade the traditional tools. The authors in [33] presented a survey on security and privacy issues in modern healthcare systems. They mentioned security and privacy requirements such as confidentiality, non-repudiation, integrity, availability, and authentication. Other researchers have also highlighted existing security and privacy attacks on healthcare devices and applications like unavailability attacks [34], [35], hardware modification attacks [36], [37], Data sniffing attacks [38], [39], information leakage [40], [41], data modification [42], [43] and communication delay attacks [44]. In [45] and [46], the authors mentioned that Blockchain-based approaches are one of the solutions that can keep patient health data safe from tampering.

E. BLOCKCHAIN FRAMEWORKS

Since the emergence of blockchain technologies, many frameworks have been developed to serve diverse industries, based on the distributed computing concept, Bitcoin white paper was introduced by Satoshi Nakamoto [47], which laid out the basis for blockchain technology. All the blockchain frameworks share the same ledger concept represented in FIGURE 1.

Blockchain can be represented as many blocks connected together, each block contains the hash code of the previous blocks. Blocks are defined as groups of transactions. They are distinguished from one another by an identifier, a unique code called a ''hash'', which varies in size depending on the amount of data they contain. The first step of a transaction within a blockchain is the integration of the information characterising this transaction, for example, the sender and receiver public identifier of the data or any related data to the use case. Nowadays, after the evolution of blockchain, we can

TABLE 1. Accessibility classification of blockchain frameworks.

Blockchain Framework/Platform	Type
Bitcoin[47], Ethereum [50]	Public
Hyperledger Sawtooth [51]	Public/private
Hyperledger fabric [52], Corda, Ripple [53], Quorum [42]	Private

find many emerging blockchain frameworks and underlying concepts. We can classify blockchain frameworks into two categories: public and permission blockchains as mentioned in TABLE 1. Public blockchains are all those in which the register of transactions is readable by everyone everywhere. the transactions stored in these ''Ledgers'' cannot be modified, cannot be deleted, can be read by everyone, are ultra-secure based on cryptography, have no central governing body and are totally decentralised. The Permission Blockchain register allows the storage and the transmission of information in a secure and decentralized manner, but with a system of access permission, reading, and verification stricter than that of a public blockchain. It is however recommended that the said register should be reserved for highly restricted networks. Another concept that was integrated into the blockchain is the smart contract technology, the smart contract creates a significant impact in many domains especially since it can integrate controls and policies into the blockchain [48], [49].

In [54] The authors of this study examine the integration of blockchain technology with IoT. The combination of blockchain with IoT is known as Blockchain of Things (BCoT). This study provides an in-depth examination of BCoT and examines its implications. The authors identify six open research issues for blockchain of things as follow resource constraints, security vulnerability, privacy leakage, incentive mechanism in BCoT, Difficulty in Big Data analytics in BCoT and scalability of BCoT.

III. COMPARATIVE ANALYSIS AND CONTRIBUTION OF THE PROPOSED APPROACH

Many recent studies have been conducted to illustrate the benefits of blockchain technology in the healthcare industry. In [55] the authors propose a blockchain-based health exchange information system, they implement the blockchain as a clinical data repository that provides patients with a distributed ledger record containing records of all the events and allows them to seamlessly access their electronic health records through healthcare providers application interfaces. In [56] The authors propose a blockchain-applied personal health record (PHR) application and validate its user experience. The proposed system shares the patient's personal information in an off-chain mode and prevents data forgery and falsification by storing encrypted data through an on-chain mode. However, the authors focused rather on the user experience and there is no physical system evaluation. In [57] The authors proposed a blockchain-based architecture to avoid centralized storage issues and deployed a blockchain network built on Hyperledger fabric. In [58] the authors propose and discuss a high-level patient-centric blockchain healthcare model. In [59] the authors proposed the Patient-Chain platform: a patient-centred Blockchain-based healthcare system as a control and management system for emergency access to secure patients' data. The Patient-Chain system is constructed on the authorized Blockchain Hyperledger Fabric. It established numerous laws and regulations through the use of smart contracts and time duration to deal with emergency accesses. In [60] the study provides a solution based on blockchain and artificial intelligence technology. The blockchain will safeguard data access and AI-based federated learning will be used to construct a strong model for global and real-time applications. In [61] the author provides a rigorous examination of recent blockchain-based systems for protecting medical data, both with and without cloud computing. In this work, they use blockchain to build and analyse several approaches. The study gaps, problems, and future roadmap are the findings of this article that promote rising Healthcare 4.0 technology, according to the research investigation. In [62] the study aimed to give decentralised mechanisms for processing personal data to both service providers and data owners, while also leveraging data provenance and transparency by exploiting advanced characteristics of blockchain technologies. The proposed approach allows data owners to require data usage consent, guarantees that only authorised parties may handle personal data, and registers all data operations in an immutable distributed ledger. Data transactions were specified and managed to utilise smart contracts and cryptographic techniques. In [63] the authors suggest a secure and auditable private data sharing (SPDS) strategy for smart grid data processing-as-a-service. They present a blockchain-based framework for trust-free private data computation and data usage tracking, in which smart contracts are used to specify fine-grained data usage policies (i.e., who can access what types of data, for what purposes, and at what cost), while distributed ledgers maintain an immutable and transparent record of data usage. Off-chain smart contract execution mechanisms based on trustworthy execution environments are also used to handle secret user datasets and reduce compute costs in blockchain systems.

All previous studies concentrated on one or two blockchain challenges; however, not all studies tackled the healthcare domain needs. In addition, healthcare use-case scenarios were superficially described and analysed.

In this paper, we proposed a blockchain-based patient-centric health data sharing approach, i.e., it involves the patient in the process using their consent. In fact, ensuring the security and privacy of patients' sensitive data requires an effective involvement of the patient in the access evaluation process. It is of paramount importance to give the patient control over their data, and the entities with whom it can be shared as well as the purpose for such sharing. Indeed, the patient should be aware of how their data is being shared with others and such sharing should be done with their consent.

TABLE 2. Related work comparison table.

Author	Year	Objective	Pros	Cons
Hannah S Chen et al[58]	2019	A blockchain is a system for storing and sharing information that is secure because of its transparency	Proposes a blockchain healthcare smart contract-based model	Implementation
***Yuntao Wang et al* [63]**	2020	SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain	Proposes a novel blockchain-based framework for trust-free private data computation and data usage tracking	Not healthcare-related
Bassem Zaabar et al[57]	2021	An architecture that takes advantage of decentralized databases to avoid centralized storage issues	A smart contract is executed through the Hyperledger Fabric network for access control.	No patient application in the process and regulation compliance
CHELLADURAI et al[55]	2022	An approach to the exchange of health information on a blockchain platform to build a smart e-health system	Used qualitative and quantitative evaluation metrics	No Architecture
Ji Woong Kim et al[56]	2022	A work introducing a novel blockchain-applied personal health record (PHR) application and validate its user experience	shares the portion of the patient's personal information off-chain and avoids data fraud and falsification by keeping encrypted data on-chain. It also improves the user experience	Implementation is not clear. No system evaluation
Le et al [59]	2022	A patient-centred Blockchain-based healthcare system as a control and management system for emergency access to secure patients' data	It tackles specific healthcare use cases	Implementation is not clear no regulations are mentioned
Aich et al [60]	2022	A blockchain to safeguard data access and AI-based federated learning will be used to construct a strong model for global and real-time application	It suggests an AI and blockchain combination	No patient engagement and the application wasn't developed and tested.
Mahajan et al [61]	2022	A systematic study of modern blockchain-based solutions for securing medical data with or without cloud computing	The reviewed approaches have implemented and evaluated Blockchain technologies for the provision of EHR	Most of the methods introduced the models without the evaluations with state-of-art methods or similar methods. The focus was more on the cryptographic aspects and less attention was given to data management and governance
Our proposed approach	2022	An attempt to design and propose an efficient blockchain-based healthcare sharing system with	It proposes a permission-based system with cryptography key. It	It concentrates on data sharing actions that are subject to a request for data access
		enhanced security and privacy involving patient consent.	designs an access control policy algorithm with smart contract to manage patient consent following GDPR guidelines	between health organisations. Another type of systematic or real-time transfer will be tackled in future work

TABLE 3. Comparison between hyperledger fabric and ethereum.

Characteristic	Ethereum	Hyperledger Fabric
Objective	Ethereum is the platform for creating B2C businesses and decentralized applications. It is created with the purpose of executing smart contracts on the Ethereum Virtual Machine (EVM) and creating decentralized applications for mass consumption using that.	Hyperledger is designed to create B2B businesses and cross-industry applications. It helps companies or industries to collaborate with developers, who work with Distributed Ledger Technology (DLT). Customized blockchain applications with limited access can be created with this.
Privacy	Ethereum is a public network. All transactions are fully transparent and anyone with access to the Internet can view these transactions.	Hyperledger is limited access or authorized blockchain network. This is highly secure and confidential. Organizations or individuals with the Authorization Certificate can only view all transactions on the network.
Governance	The Ethereum network is governed by Ethereum developers only. Vitalik Buterin is the lead developer and founder of Ethereum. This is primarily an example of internal development rather than collaboration.	The Hyperledger framework is governed by the Linux Foundation. IBM is also one of the major contributors to this framework. It is the product of the massive collaboration of these two companies that have proven to be a huge success.
Participation	Ethereum is a public and permissionless network. Anyone with access to the Internet can download the software and start running Ethereum.	Hyperledger maintains strict control over participation in this network. Only authorized members and peers selected by authorized members can use the Hyperledger platform and its tools. This hides valuable and confidential information from external parties and prevents them from manipulating it.
Smart contracts	Ethereum first proposed smart contracts. A smart contract is a computer program or condition written in code that is automatically triggered when certain conditions are met. It controls the transfer of digital assets between the parties under the contract. It is immutable; once the condition is created, it cannot be changed by any third party.	Like smart contracts, Hyperledger Fabric also allows member organizations to run code on peers that create transactions under a specific condition. These are known as chaincode.
Proof of Work (PoW) or consensus mechanism	Because Ethereum is a decentralized network, a proof-of-work (PoW) or consensus mechanism runs throughout the blockchain. It allows participating nodes in the decentralized network to reach a consensus or agree on things like account balances and the order of transactions, preventing users from making fake transactions and doubling their coins.	Since Hyperledger is a private and authorized network, it does not need any PoW or consensus mechanism to validate a transaction. If two participating parties agree on a specific transaction, no third party can see or intervene in the specific transaction. This helps to improve scalability and transaction rates as well as the performance of the overall network.
Speed of transactions	Since Ethereum is a public domain, it has a PoW mechanism, which reduces the transaction speed of Ethereum. That's something close to 20 transactions per second.	To be an authorized blockchain network, the Hyperledger fabric does not need a PoW mechanism as heavy as Ethereum. This increases the transaction speed. That's about 2000 transactions per second [65]. Which is much larger than Ethereum.
Crypto-currency	Ethereum has its own native cryptocurrency called ETHEREUM (ETH). Any participating node can mine ETH by paying for gas.	Hyperledger does not have its native crypto-currency and does not involve mining.

Accordingly, the architecture of the blockchain-based sharing system is proposed. Various methods and configurations for the blockchain-based transaction in the network are deployed. In the proposed system, a shared symmetric key and private key allow the system to be distributed to other participants in the blockchain network. We proposed a novel healthcare interoperability mechanism using on and off-chain data management by meeting the requirements of GDPR and addressing the blockchain challenges in the healthcare domain. TABLE 2 presents a comparison of related works we have reviewed as well as the added value of our proposed approach.

IV. SYSTEM DESIGN AND MODELING APPROACH

A. TECHNOLOGY CHOICE

In the healthcare industry, data cannot be freely accessible by anyone, the data flow should be allowed on a private access mode basis. In this context, only for the authenticated staff for that, we can eliminate all the un-permission blockchain frameworks.

In [64] the authors compared three blockchain frameworks bitcoin, Ethereum, and Hyperledger Fabric, they observed that the Hyperledger Fabric blockchain framework possesses the more complete features for developing healthcare applications, so we will adapt healthcare requirements with the blockchain data models using the Hyperledger Fabric framework. In TABLE 3 we present the comparison of the Hyperledger Fabric and Ethereum frameworks.

B. HYPERLEDGER FABRIC MODEL

The Hyperledger fabric [52] models contain basic elements that define the logic in the network, which are:

- Assets: Asset definitions enable the exchange of almost any type of data that requires protection while being transmitted over a network, from whole foods to antique cars to currency futures in our case it is patient data [52].
- Chaincode: a smart contract that defines a set of assets and provides the functions for operating on the assets and changing the states. It also implements application-specific rules and policies. Function execution may result in state changes that are recorded on the ledger [52].
- Endorsement policies define which peers need to agree on the results of a transaction before it can be added to the ledger [52].
- Ledger Features: The immutable, shared ledger encodes the entire transaction history for each channel and includes query capability for efficient auditing and dispute resolution [52].
- Privacy: Channels and private data collections enable private and confidential multi-lateral transactions that are usually required by competing businesses and regulated industries that exchange assets on a common network [52].
- Security & Membership Services: Permissioned membership provides a trusted blockchain network, where participants know that all transactions can be detected and tracked by authorized regulators and auditors [52].
- Consensus: A unique approach to consensus enables the flexibility and scalability needed for the enterprise. In this paper, we will follow the Hyperledger Fabric Model as we apply our approach to the ledger and the chaincode elements [52].

C. MODEL APPROACH LEDGER

As we mentioned in [66], In our approach, we focus on data management and provenance tracking to document the actions taken to treat a patient like a department transfer or data sharing between healthcare facilities. Hyperledger fabric blockchain ledger has two parts: (1) a first part that is a word state, it contains the current values of a set of ledger states, in our case, it is the patient account that holds the patient identification and the owner of the account that is the patient and the healthcare facility with the consent of the patient, the world state can change frequently since states can be created, updated, and deleted. The second part is the (2) blockchain where there are all the records of the changes that determine the world state. The blockchain blocks collect all the changes in the word states so we can read all the transactions and understand the history of changes, so providing and enforcing data integrity. As represented in FIGURE 2, the ledger L, includes a word state W that contains three states with keys: Patient0, Patient1, and Patient2 with version number 0 meaning that they have not been updated since they were created. And includes a blockchain, B that contains two blocks, 0 and 1. Block 1 contains three transactions: T1 to T3 refers to transactions that created the initial states for Patient0 to patient2 in W and block1 linked to block0. As demonstrated we use JSON to structure and transmit data on the blockchain network.

All the data will be disseminated in a permissioned blockchain environment, this means that all the transacted data are encrypted, hence, providing confidentiality.

D. MODEL APPROACH CHAINCODE

Chaincode defines the asset's structure and the business logic for the transactions, its functions execute against the ledger's current state database and are initiated through a transaction proposal. The execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers. In our approach we implement an access control chaincode pattern, to specify which blockchain network member can query private data in a collection. We store an access control list for a private data collection key, then in the chaincode get the member submitter's credentials and verify they have access before returning the private data. Similarly, we require a pass a passphrase into chaincode, which must match a passphrase stored at the key level, in order to access the private data. Note, that this pattern can also be used to restrict member access to public state data.

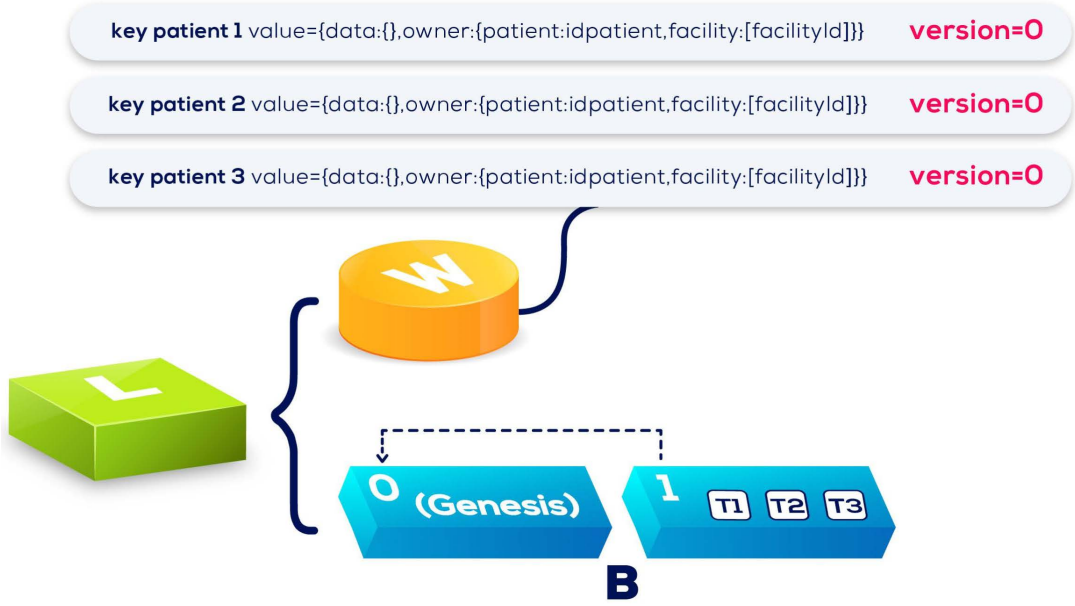

FIGURE 2. Ledger lifecycle representation.

It is worth recalling here that we are referring to two main use cases (1) the data is not stored in the blockchain and (2) the data is stored in the blockchain. In the first use case, the data will be stored in a private database in the healthcare facility for example and connected directly to the Fabric Client (FC). The FC will connect and monitor the data flow with the blockchain network. The data flow will be treated as transactions in the blockchain. In the second use case, the data will be stored in the blockchain, so the data will be treated as private data and any change accruing to it will be recorded in the blockchain. The difference between the two use cases is that the data can be permanently deleted in the first one, but in the second use case, we can purge the data. Purged private data cannot be queried from the chaincode, and is not available to other requesting peers.

E. ILLUSTRATIVE SCENARIO AND CONNECTIVITY MODEL

Informed consent to medical treatment is fundamental in both ethics and law. Patients have the right to receive information and ask questions about recommended treatments so that they can make well-considered decisions about care. Successful communication in the patient-physician relationship fosters trust and supports shared decision-making. The process of informed consent occurs when communication between a patient and physician results in the patient's authorization or agreement to undergo a specific medical intervention. In seeking a patient's informed consent (or the consent of the patient's surrogate if the patient lacks decision-making capacity or declines to participate in making decisions), physicians should:

- Assess the patient's ability to understand relevant medical information and the implications of treatment alternatives and to make an independent, voluntary decision.
- Present relevant information accurately and sensitively, in keeping with the patient's preferences for receiving medical information. The physician should include information about:
- The diagnosis (when known)
- The nature and purpose of recommended interventions
- The burdens, risks, and expected benefits of all options, including forgoing treatment
- Document the informed consent conversation and the patient's (or surrogate's) decision in the medical record in some manner.

When the patient/surrogate has provided specific written consent, the consent form should be included in the record. In emergencies, when a decision must be made urgently, the patient is not able to participate in decision-making, and the patient's surrogate is not available, physicians may initiate treatment without prior informed consent. In such situations, the physician should inform the patient/surrogate at the earliest opportunity and obtain consent for ongoing treatment in keeping with these guidelines. In our case, there is no need to use a third-party system that can affect the privacy and confidentiality of the patient, and if there is a need to share data to have a second opinion on the permissioned nature of the fabric network, and the chaincode implemented in the network will ensure the protection of the data. As shown in the use case in FIGURE 3, the healthcare facility 1(HF1) physician requests the patient's medical history from the HF2 physician. To ensure best practice and continuity of care for the patient. In our approach, the request will be processed by the chaincode to verify the identity of all stakeholders and a valid request for access to private medical data must be sent with the patient's consent. The blockchain will record all transactions to track the provenance of the data and ensure

the integrity of the health data. when the physician in HF2 receives the demand, it will have the option to allow access to the specific data by read-only or read-write if the data is on-chain or share the data if the data is off-chain. To ensure secure communication, and determine the exact permissions over the medical data and access to information that all stakeholders have in a blockchain network, we used two key concepts to manage valid identities in the network. The first one is the Public Key Infrastructure (PKI) is a collection of internet technologies that provide secure communications in a network. The PKI have four core elements:

- Digital Certificates: a document that holds a set of attributes relating to the holder of the certificate Hyperledger fabric uses the X.509 standard [67] which allows the encoding of a party's identifying details in its structure. For example, Jane Doe the head of the oncology department of healthcare facility 1 in Paris, Paris might have a digital certificate with a SUBJECT attribute of C = FR, ST = Paris O = Healthcare Facility 1 CN = Jane Doe /UID = 123456. Jane's certificate is similar to her government identity card — it provides information about Jane that she can use to prove key facts about her.
- Authentication, Public keys, and Private Keys: Technically speaking, digital signature mechanisms require each party to hold two cryptographically connected keys: a public key that is made widely available and acts as an authentication anchor, and a private key that is used to produce digital signatures on messages.
- Certificate Authorities: A Certificate Authority dispenses certificates to different actors. These certificates are digitally signed by the CA and bind together the actor with the actor's public key (and optionally with a comprehensive list of properties). As a result, if one trusts the CA (and knows its public key), it can trust that the specific actor is bound to the public key included in the certificate, and owns the included attributes, by validating the CA's signature on the actor's certificate.
- Certificate Revocation Lists: it is a list of references to certificates that a CA knows to be revoked for one reason or another, using a CRL to check that a certificate is still valid. If an impersonator tries to pass a compromised digital certificate to a validating party, it can be first checked against the issuing CA's CRL to make sure it's not listed as any longer valid.

The Second key is the Membership Service Provider (MSP) The MSP identifies which Root CAs and Intermediate CAs are accepted to define the members of a trusted domain by listing the identities of their members, or by identifying which CAs are authorized to issue valid identities for their members. The MSP turns identity into a role by identifying specific privileges an actor has on a node or channel. PKIs and MSPs work together in the same way, a PKI provides a list of identities, and an MSP says which of these are members of a given organization that participates in the network.

V. SECURITY ANALYSIS

The emergence of the Hyperledger Fabric blockchain is accompanied by security issues and concerns (some of which have yet to be investigated) that can be damaging to DLT operation and performance if not well addressed [68]. Using STRIDE [69] threat modelling technique adoption this section provides a brief summary of such threats as well as potential strategies for preventing them as presented in TABLE 4.

VI. RESULTS AND DISCUSSION

As we mentioned in the previous section, we designed a healthcare blockchain model based on the Hyperledger fabric model, successfully implemented it in the local workspace using docker [75], and tested it using the Hyperledger Test Network. with this back-end implementation, we can create, read, update, and purge an asset. We can ensure the integrity and security of the data conformed to essential GDPR [10] requirements. LISTING 1 and LISTING 2 describe parts of JavaScript code to create and read an asset from a word state as we mentioned in Section IV-C. All the changes that occur to the word state will be archived in the blockchain. This backup the provenance tracking that supports the integrity of the model.

As represented in FIGURE 4 in our approach we focused on enforcing patient consent as a condition to satisfy so the transfer could take place. The patient is a centric entity for governing their data so consent will be asked in the first interaction with them. Personal data concerning health should include all data about the health status of a data subject which reveals information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration form, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and the Council_ to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test (Recital 35 GDPR). Consequently, all future data flow and transactions will highly be depending on the consent of the first data holder that is the patient. Once consent is given, the health facility will be the governing body of the data, this will authorize and enable the data transfer and the use of the following specific activities the patient has agreed upon. All the transactions are made in a protected permissioned environment. However, the public data in the context of our Hyperledger fabric-based approach are public only for authorized, authenticated users.

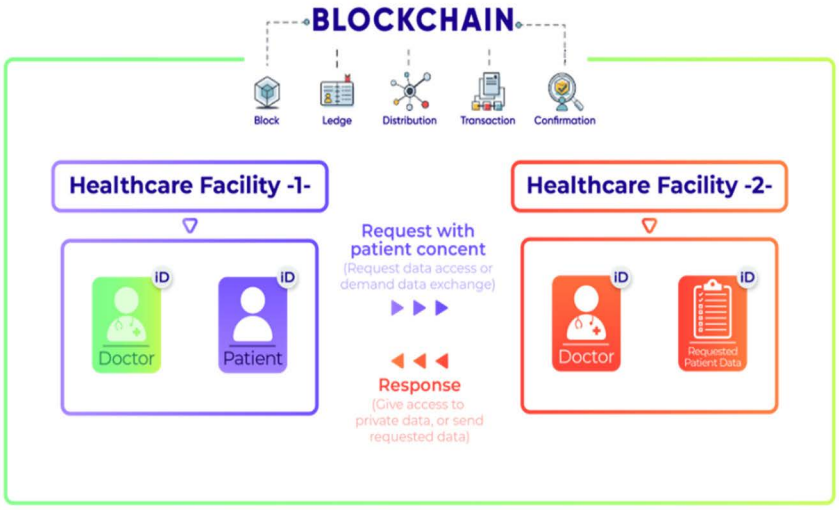

FIGURE 3. Use a case scenario of health data share between two facilities.

In our approach, the patient can give permission and consent to healthcare providers to use their data. When data sharing is detected in the system, there will be an event generated to record the data flow and track the provenance of the data. This record is then submitted to the blockchain network as assets and transformed into a transaction. The data can be on-chain or off-chain. If it is on-chain it must be stored as private data so we can purge it if needed. A list of transactions will be used to form a block, and the block will be validated by nodes in the blockchain network. After a series of processes, the integrity of the record can be preserved, and future validation on the block and the transaction related to this record is available. Each time there is an operation on personal health data, a record will be reflected in the blockchain. This ensures that every action on personal health data is accountable. As is shown in FIGURE 5 we implement a membership service provider utilizing the Hyperledger Fabric issuing enrolment certificates and transaction certificates for participating nodes in the Hyperledger Fabric blockchain network and participating Fabric clients and generating the access control list during channel establishment according to user settings and operations. The chaincode execution is launched by invoking transactions. A channel is formed to isolate individual activities among authorized parties. To provide isolation between different data sharing domains, the Certificate Authority (CA) provides several certificate services to users of a blockchain. More specifically, these services relate to user enrolment, transactions invoked on the blockchain and TLS-secured connections between users or components of the blockchain [52]. In our case, the CA issues a certificate to the Fabric client blockchain network peers for transaction validation and the *orderer* [52] for ordering service. A channel is like a virtual blockchain network that sits on top of a physical blockchain network with its own access rules. Channels employ their own transaction ordering mechanism and thus provide scalability, ultimately allowing for effective ordering and partition of huge amounts of data. In FIGURE 5, we established two channels for two use cases the on-chain and the off-chain data collection. both patient and doctor may perform data collection and synchronization on their mobile platforms, and the healthcare mobile application will send web requests to the fabric client (FC) for data synchronization or query. Healthcare providers and research faculties also communicate with the FC to request or update health data. With permission from the patient, these requests will be allowed to participate in a certain channel. The Fabric client communicates with the Fabric blockchain network peer. Distributed peers will validate the incoming requests and propose transactions by executing chaincode. The ordering service is responsible for checking transaction signatures and ordering them with channel IDs. For each channel, there is a sub-ledger, as part of the system ledger, to record all transactions in the form of blocks.

For privacy concerns, the patient can selectively share health data with data requesters, based on the necessity of how personal health data is required to assist the healthcare service. To issue a specific certificate, the patient or doctor can state clearly in the certificate what category of personal data is allowed access and whether read-only or read-write access is allowed depends on the Access Control Lists that manage access to resources by associating a Policy with a resource, in our test we used the default ACLs implemented in the test network. Moreover, within different channels, different grained information is shared. In this sense, our approach provides privacy protection and access control policy, enhancing the data ownership of individuals. In our approach, using Hyperledger fabric, the exchange of the data will be more secure providing more integrity, confidentiality, and privacy to the data flow. Several research papers have been published studying and testing the performance capabilities of Hyperledger Fabric. The latest scaled Fabric to 20,000 transactions per second [65]. Hyperledger Fabric, being a permissioned platform, enables confidentiality through its channel architecture and private data feature.

TABLE 4. Threat analysis of blockchain technologies.

Threat	Overview	Mitigation
Insider threats	To provide a generalised platform for establishing a permissioned blockchain, Hyperledger Fabric relies on some trusted parties and centralised services (i.e. Membership Service Provider (MSP) admins and the OS), which makes these services vulnerable to Insider threats, when a peer becomes malicious and behaves incorrectly, for example, when it tries to maximise its profit or becomes corrupted by an attacker. DDoS assaults, Crash faults, 51 per cent attacks, Sybil attacks, and Man in the Middle attacks might all be enabled by an insider threat.	Insider threats may be prevented in the cyber-trust project by protecting the privacy of the peers (clients, peers, and ordering nodes). This can be accomplished by employing a preventative strategy against internal Hyperledger Fabric assaults, such as the privacy-preserving data aggregation technique provided in [70] for Smart Grids against internal attackers. It is also necessary to protect the Hyperledger Member Service, which is one of the fundamental components that Hyperledger Fabric offers to facilitate dynamic entity registration, identity management, and auditing [71]. This is possible with current Trusted Execution Environments (TEEs), such as Intel's Software Guard Extensions (SGX) [72]. This promising method was employed as an additional security element in peer communications in [71]. With SGX remote attestation and isolated execution inside the CPU capabilities, each distributed node may be enrolled as a trusted entity, lowering the attack surface significantly.
DDoS (Distributed Denial of Service)	Denial of Service (DoS) is a type of cyber-attack in which the attacker uses a network connection to interrupt the normal traffic of a targeted service, rendering it inaccessible to legitimate users. The attack can be initiated by sending repeated SYN message requests (i.e. "SYN flood") or packets bigger than the maximum byte allowed (i.e. "ping of death") [73]. A DoS assault can be conducted automatically by a single machine; however, if a DoS attack is launched by numerous machines, sometimes referred to as zombies or bots, it is referred to as a Distributed Denial of Service (DDoS) attack. The Hyperledger Fabric network is DDoS resilient by design, as it is dispersed and redundant.	DDoS assaults caused by modifying or interrupting Chaincode execution can be prevented by running the Chaincode on a trustworthy execution environment such as SGX. This verifies that the chaincode adheres to its specifications.
Wormhole attacks.	In this attack, an insider hostile peer within a private network establishes a virtual private network (or channel) with the outside network and leaks	A wormhole attack is a novel attack that works on all major permissioned blockchains, including Hyperledger Fabric, that allows an attacker to steal

TABLE 4. *(Continued.)* **Threat analysis of blockchain technologies.**

	information from its private network [74]. An extra security layer (i.e. access control mechanism) is employed in the Hyperledger network by constructing private channels between network participants. Only peers within the channel have access to the channel's ledger, and their identities are known to all other members of the channel. The employed access control approach is based on trusting every participant of the channel. As a result, if a single peer member is penetrated or becomes hostile and colludes with the external adversary, a wormhole attack is feasible, which may result in the exposure of sensitive information of all channel participants. [74]	data from honest peers in the same channel. As a result, an innovative strategy to secure communications while maintaining privacy inside the channels is critical. For example, work in [74] advocated anonymizing the senders and recipients of channel transactions.
MitM & SSL Stripping attacks	Each peer in a Hyperledger network includes a client-side interface for receiving input data and allowing clients to invoke transactions on the fabric, where transactions often entail confidential data being supplied as input. Insecure interfaces can lead to information leakage, particularly when the encryption provided by HTTPS is removed (called SSL Stripping). SSL Stripping is a severe security threat to the Hyperledger network since its access control method is solely based on establishing trust among mutually untrustworthy peers [68]. Once attackers get access to the network, they can operate as a Man-in-the-Middle (Mit M) to interrupt network connections and obtain data in plaintext.	SSL stripping attacks intercept and decrypt sensitive data transferred over the network. This is one of the most hazardous Man in the Middle (MitM) attacks since it is extremely simple to initiate. An SSL certificate alone will not protect you from this attack. As a result, an intrusion detection system (IDS), such as the one given as part of the project, can be used to prevent such threats.

In channels, participants on a Fabric network establish a sub-network where every member has visibility to a particular set of transactions. Thus, only those nodes that participate in a channel have access to the smart contract (chaincode) and data transacted, preserving the privacy and confidentiality of both. Private data allows connections between members on a channel, allowing much of the same protection as channels without the maintenance overhead of creating and maintaining a separate channel. All the data flow will be registered in the ledger and validated by the chaincode rules this add an integrity layer to all the process.

VII. SYSTEM PERFORMANCE ANALYSIS

In this section, the evaluation of the proposed system, and results are shown concerning performance latency and throughput.

A. SIMULATION SETTINGS

Hyperledger caliper is a benchmarking tool that is used for the blockchain network. It supports various blockchain frameworks, such as Hyperledger Fabric, Hyperledger Besu, Ethereum, and FISCO-BCOS. In this paper, we used the caliper tool to verify and evaluate the performance of the

```
async CreateAsset(ctx, id, data, patient, facility,
PatientConsent) {
      const asset = {
         ID: id,
         Data: data,
         Access: [PatientID, facilityID ],
         Consent: PatientConsent,
      };
      ctx.stub.putState(id,
Buffer.from(JSON.stringify(asset)));
      return JSON.stringify(asset);
   }// ctx Context
// ReadAsset returns the asset stored in the world state with
the given id.
   async ReadAsset(ctx, id) {
      const assetJSON = await ctx.stub.getState(id); // get the
asset from chaincode state
      if (!assetJSON || assetJSON.length === 0) {
         throw new Error(`The asset ${id} does not exist`);
      }
      return assetJSON.toString();
   }
```

LISTING 1. Piece of code from the model definition in the chaincode.

system and its various parameters, including latency, throughput, CPU usage, memory consumption, and disk write/read for the evaluation of the system. The simulation PCs have the following configurations:

- Dual-core Intel Core i7 3,1 GHz CPU with 4MB L3 cache
- 16GB memory
- 1 Gbit/s network
- 250GB SSD
- Docker Desktop v 4.8.1
- Hyperledger Fabric v 2.2
- Hyperledger caliper v0.4.2

B. SIMULATION EXPERIMENT AND RESULTS

Several observations are made in order to comprehend and evaluate the Hyperledger platform of blockchain technology. The experiment is carried out using various measures and is carried out in five rounds of putting the transaction into the ledger's network, with 1000 transactions written into each round at various speeds of 50, 100, 150, 200, and 250 transactions per second. The transaction time exceeds that of the blockchain network. FIGURE 6(a) depicts various lines containing the time required to execute transactions in the network's peculiar structure. 1HF1peer, 2HF1peer, and 2HF2peer represent distinct transaction performances. The results are collected in five rounds, each having 1000 transactions at varying tps speeds. 5000 transactions are completed in 120 seconds by the 1HF1peer. Similarly, 2HF1peer reaches 3000 transactions in the 120s, but 2org2peer only

```
// TransferAsset updates the access field of assets with
given id in the world state.
   async TransferAsset(ctx, id, Requester) {
      const assetString = await this.ReadAsset(ctx, id);
      const asset = JSON.parse(assetString);
                  if (asset.Consent == false ) {
        return false
      }
      asset.Access.push = Requester;
      return                              ctx.stub.putState(id,
Buffer.from(JSON.stringify(asset)));
   }
```

LISTING 2. Transfer asset method in the chaincode.

reaches 2000 transactions. As a result, it is evident that as the number of organisations and peers grows, so does the time required to perform transactions. In the transaction delay mathematical calculation. Assume TL is transaction latency, which is the time it takes to use the network. CT is the transaction confirmation time, which varies with the network threshold NT.

$$\text{Transaction latency TL} = (\text{CT} * \text{NT}) - \text{ST} \tag{1}$$

FIGURE 6 depicts the average delay of performance testing using the calliper report (b). Latency is measured in seconds in this graph. It represents the delay of communication and the success rate of writing transactions. 1HF and 1peer have substantially lower latency than 2HF1peer and 2HF2peers. When the transaction rate increases in successive rounds, so do the latency time. Higher delay is observed in more healthcare institutions and peers. Higher throughput results in lower latency. Latency and throughput are thus inversely proportional. Assume that TT is transaction throughput, which is the success rate of the transaction with a defined tps in the mathematical formula. The transaction committed on the whole network is referred to as TCT. The invalid or failed transactions are subtracted with total transactions time TTS at many committed nodes NCN.

$$\text{TT} = \text{TCT}/\text{TTS} * \text{NCN} \tag{2}$$

FIGURE 6(c) plots throughput vs transaction rates. The throughput is measured in comparison to 1HF 1peer, 2HF 1peer, and 2HF 2peers.

The maximum throughput is achieved in 1HF 1peer network settings, with throughput decreasing to 20 tps and 10 tps, respectively, in 2HF 1peer and 2HF 2peer network settings. This results in larger latency and communication gaps, allowing for improved performance.

Resource utilisation on multiple nodes is evaluated: When doing network calliper testing, several metrics such as average CPU utilisation, memory, incoming traffic, outgoing traffic, disc read/write, and so on are monitored. TABLE 5 depicts many peer nodes with varying traffic and memory and CPU use.

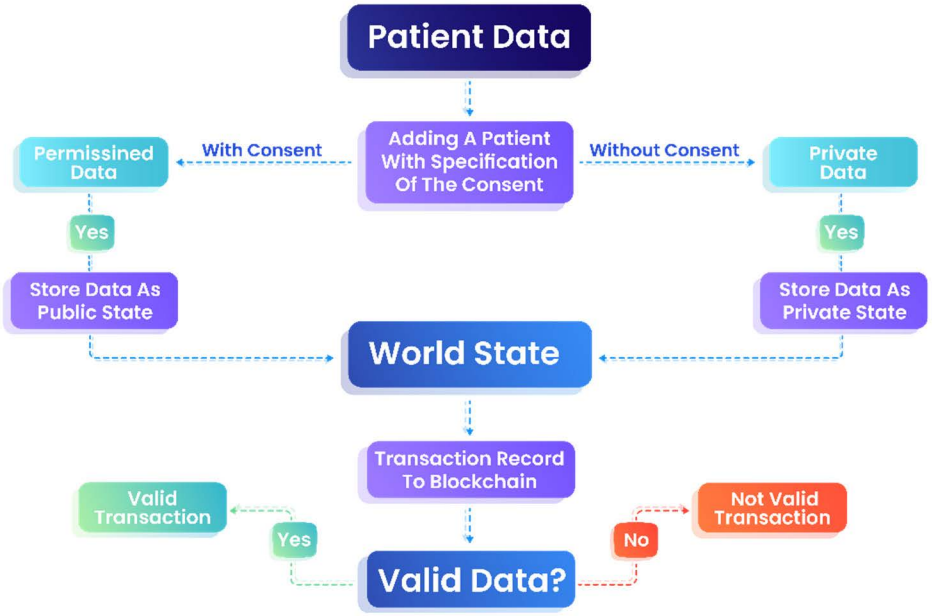

FIGURE 4. Data access flowchart.

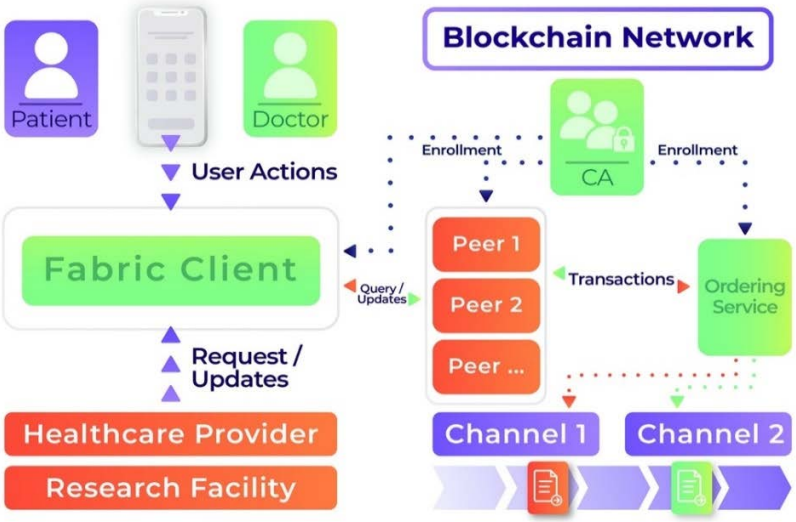

FIGURE 5. Architectural model of patient data exchange approach using hyperledger fabric.

TABLE 5. Resource consumption of various parameters.

Type	Name	Memory(avg)	CPU(avg)	Traffic In	Traffic Out	Disc Write
Docker	peer1.hf1.example.com	276.0MB	6.58%	4.3MB	440.4KB	6.2MB
Docker	peer0.hf.example.com	207.5MB	11.61%	6.6MB	3.5MB	6.2MB
Docker	peer0.hf2.example.com	206.0MB	12.13%	6.6MB	3.6MB	6.2MB
Docker	peer1.hf2.example.com	224.1MB	6.75%	4.3MB	439.0KB	6.2MB
Docker	orderer.example.com	59.9MB	2.12%	3.9MB	15.5MB	4.6MB

VIII. LIMITATIONS AND FUTURE WORK

This paper proposes an approach using blockchain technology in the healthcare domain with the Hyperledger Fabric Blockchain. This approach is built to manage sensitive healthcare data across multiple healthcare and research facilities ensuring the consent of the patient and the protection of his sensitive data by a decentralized model that proves his immunity against the current cyber threats. In our approach, we create a data transfer chaincode that is helpful to prove and manage the consent procedure. All network participants with authorized access and who have the privileges could see the same information at the same time, which ensures full transparency. All transactions are immutably recorded and time-stamped. In our work, we present multiple use cases

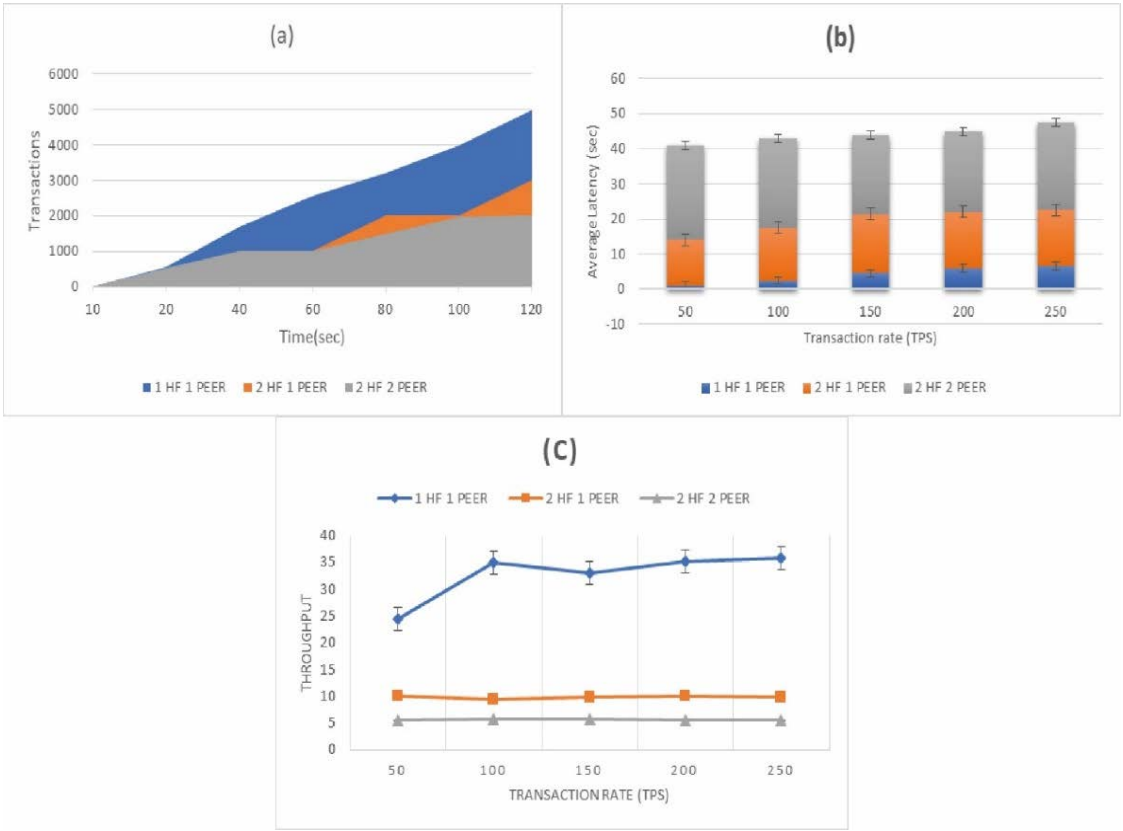

FIGURE 6. Resource consumption.

to show the generalisability and fluidity of our approach, so our approach can be implemented in a variety of medical scenarios. On the other side, we need to work more on the healthcare data model by integrating standardized models like the HL7 Reference Information Model (RIM) [76] or the FHIR API [77] to add more healthcare specificity and add an interoperability layer to the approach. We need to add more endorsement policies to ensure compliance with the current legislation. However, the ownership of the current medical data is still an issue, and currently, there are no rules for using blockchain to manage ownership by regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) [33] and other European regulations (i.e., GDPR).

IX. CONCLUSION

In this paper, we have presented a scalable healthcare secure data sharing approach based on blockchain technology. We focused on data governance functioning in a permissioned blockchain. We have developed a chaincode to transfer data between health facilities with the consent of the patient and we test it in a docker simulation environment generating a performance analysis. The approach of decentralized and distributed character allows a strong availability of the system; the traceability is ensured by the conservation of all the transactions in the register and the integrity is guaranteed by the system of cryptography which combines public key and private key. In future work, we are planning to develop a privacy detailed regulatory compliance case study which will result in additional layers to the blockchain architecture presented in our approach. This demonstrates blockchain's capabilities and relevance in a variety of domains, demonstrating that it might be the next breakthrough technology to replace present healthcare systems.

REFERENCES

[1] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J. Med. Internet Res.*, vol. 20, no. 5, Art. no. e10059, 2018.

[2] S. G. Narayana, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems," *Health Inform. J.*, vol. 16, no. 3, pp. 201–209, 2010.

[3] R. S. Evans, "Electronic health records: Then, now, and in the future," *Intermountain Healthcare Biomed. Inform.*, vol. 25, no. 1, pp. S48–S61, 2016.

[4] S. A. E. Hoffman, "Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure," *Inf. Secur., Emerg. Voices*, vol. 24, no. 1, pp. 1–20, 2020.

[5] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[6] M. Finck, "Blockchains and data protection in the European union," *Eur. Data Protection Law Rev.*, vol. 4, p. 17, 2018.

[7] A. R. Lee, M. G. Kim, and I. K. Kim, "SHAREChain: Healthcare data sharing framework using blockchain-registry and FHIR," in *Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM)*, 2019, pp. 1087–1090.

[8] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, pp. 1–10.

[9] S. Khezr, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.
[10] P. Voigt, *The Eu General Data Protection Regulation (GDPR)*, vol. 10, no. 3152676, 1st ed. Cham, Switzerland: Springer, 2017, p. 10.5555.
[11] M. R. Islam, "A review on blockchain security issues and challenges," in *Proc. IEEE 12th Control Syst. Graduate Res. Colloq. (ICSGRC)*, Aug. 2021, pp. 227–232.
[12] J. Sengupta, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Network Comput. Appl.*, vol. 149, no. 1, 2020, Art. no. 102481.
[13] K. Peng, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12004–12020, Aug. 2021.
[14] N. Fatima et al., "Security and privacy issues of blockchain technology in health care—A review," *ICT Anal. Appl.*, pp. 193–201, 2022.
[15] M. Madine, "Appxchain: Application-level interoperability for blockchain networks," *IEEE Access*, vol. 9, pp. 87777–87791, 2021.
[16] A. A. Siyal, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.
[17] L. Campanile et al., "Risk analysis of a GDPR-compliant deletion technique for consortium blockchains based on pseudonymization," in *Proc. Int. Conf. Comput. Sci. Appl.* Springer, 2021, pp. 3–14.
[18] D. C. Kaelber and D. W. Bates, "Health information exchange and patient safety," *J. Biomed. Inform.*, 40, no. 6, pp. S40–S45, 2007.
[19] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Inform. Res.*, vol. 25, no. 1, pp. 51–56, 2019.
[20] S. Kraus, "Digital transformation in healthcare: Analyzing the current state-of-research," *J. Bus. Res.*, vol. 123, pp. 557–567, Feb. 2021.
[21] J. P. Mo and A. Sinha, *Engineering Systems Acquisition and Support*. Amsterdam, The Netherlands: Elsevier, 2014.
[22] Y. K. Alotaibi and F. Federico, "The impact of health information technology on patient safety," *Saudi Med. J.*, vol. 38, no. 12, p. 1173, 2017.
[23] A. Ellervee and R. N. Matulevicius Mayer, "A comprehensive reference model for blockchain-based distributed ledger technology," in *Proc. ER Forum/Demos*, 2017, pp. 306–319.
[24] J. M. Reps, "Design and implementation of a standardized framework to generate and evaluate patient-level prediction models using observational healthcare data," *J. Amer. Med. Inform. Assoc.*, vol. 25, no. 8, pp. 969–975, 2018.
[25] S. Senthilkumar, "Big data in healthcare management: A review of literature," *Amer. J. Theor. Appl. Bus.*, vol. 4, no. 2, pp. 57–69, 2018.
[26] M. Shi, R. Jiang, X. Hu, and J. Shang, "A privacy protection method for health care big data management based on risk access control," *Health Care Manag. Sci.*, vol. 23, no. 3, pp. 427–442, 2020.
[27] L. Ismail, "Requirements of health data management systems for biomedical care and research: Scoping review," *J. Med. Internet Res.*, vol. 22, no. 7, 2020, Art. no. e17508.
[28] S. M. Ahmed and A. Rajput, "Threats to patients' privacy in smart healthcare environment," in *Innovation in Health Informatics*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 375–393.
[29] J. C. Cabello et al., "Big-data and cyber-physical systems in healthcare: Challenges and opportunities," in *Handbook of Big Data Privacy*, 2020, pp. 255–283.
[30] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," *Sustainability*, vol. 12, no. 17, p. 7002, 2020.
[31] L. Ayala, "How hackers gain access to a healthcare facility or hospital network," in *Cybersecurity for Hospitals and Healthcare Facilities*. Berkeley, CA, USA: Apress, 2016, pp. 9–18.
[32] M. Muthuppalaniappan and K. J. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *Int. J. Quality Health Care*, vol. 33, no. 1, 2020, Art. no. mzaa117.
[33] A. I. Newaz, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.
[34] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Comput. Commun.*, vol. 154, pp. 509–527, Mar. 2020.
[35] M. Ilyas, "A survey of DDoS attack detection strategies in cloud," *VFAST Trans. Softw. Eng.*, vol. 8, pp. 55–63, 2020.
[36] A. P. Kuruvila, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *Int. J. Elect. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107150.
[37] C. Yang, J. Hou, M. Wu, K. Mei, and L. Geng, "Hardware trojan attacks on the reconfigurable interconnections of convolutional neural networks accelerators," in *Proc. IEEE 15th Int. Conf. Solid-State Integr. Circuit Technol. (ICSICT)*, Nov. 2020.
[38] R. Elnaggar, "Security against data-sniffing and alteration attacks in IJTAG," *IEEE Trans. Comput.-Aided Desgin Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1301–1314, Jul. 2020.
[39] D. Glăvan et al., "Sniffing attacks on computer networks," *Sci. Bull. Mircea Cel Batran Nav. Acad.*, vol. 23, no. 1, pp. 202A–207A, 2020.
[40] M. H. I. Chowdhuryy, H. Liu, and F. Yao, "BranchSpec: Information leakage attacks exploiting speculative branch instruction executions," in *Proc. IEEE 38th Int. Conf. Comput. Design (ICCD)*, 2020, pp. 529–536.
[41] S. N. Molotkov, "Physics, trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography," *J. Exp. Theor. Phys.*, vol. 130, no. 6, pp. 809–832, 2020.
[42] A. Baliga, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1809.03421*.
[43] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system ac state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2020.
[44] M. Ullmann and M. Vögeler, "Delay attacks—Implication on NTP and PTP time synchronization," in *Proc. Int. Symp. Precis. Clock Synchronization Meas., Control Commun.*, 2009, pp. 1–6.
[45] C. Peng and H. Sun, "Switching-like event-triggered control for networked control systems under malicious denial of service attacks," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3943–3949, Sep. 2020.
[46] S. He, "Three-dimensional salvo attack guidance considering communication delay," *Aerosp. Sci. Technol.*, vol. 73, pp. 1–9, Feb. 2018.
[47] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, vol. 4, 2008, p. 2. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[48] R. O'Shields, "Smart contracts: Legal agreements for the blockchain," NC Banking Inst., 2017, vol. 21, p. 177.
[49] M. Corrales, M. Fenwick, and H. Haapio, *Legal Tech, Smart Contracts and Blockchain*. Singapore: Springer, 2019.
[50] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2017.
[51] Z. Shi et al., "Operating permissioned blockchain in clouds: A performance study of hyperledger sawtooth," in *Proc. 18th Int. Symp. Parallel Distrib. Comput. (ISPDC)*, 2019, pp. 50–57.
[52] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[53] M. Benji and M. Sindhu, "A study on the corda and ripple blockchain platforms," in *Advances in Big Data and Cloud Computing*. Springer, 2019, pp. 179–187.
[54] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[55] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 693–703, 2022.
[56] J. W. Kim, "A blockchain-applied personal health record application: Development and user experience," *Appl. Sci.*, vol. 12, no. 4, p. 1847, 2022.
[57] B. Zaabar, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500.
[58] H. S. Chen, "Blockchain in healthcare: A patient-centered model," *Biomed. J. Sci. Tech. Res.*, vol. 20, no. 3, p. 15017, 2019.
[59] H. T. Le et al., "Patient-chain: Patient-centered healthcare system a blockchain-based technology in dealing with emergencies," in *Proc. Int. Conf. Parallel Distrib. Comput., Appl. Technol.* Cham, Switzerland: Springer, 2022, pp. 576–583.
[60] S. Aich et al., "Protecting personal healthcare record using blockchain & federated learning technologies," in *Proc. 24th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2022, pp. 109–112.
[61] H. B. Mahajan et al., "Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Appl. Nanosci.*, pp. 1–14, 2022, doi: 10.1007/s13204-021-02164-0.
[62] N. B. Truong, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1746–1761, 2019.
[63] Y. Wang, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2020.

[64] C. C. Agbo and Q. H. Mahmoud, "Comparison of blockchain frameworks for healthcare applications," *Internet Technol. Lett.*, vol. 2, no. 5, p. e122, 2019.
[65] C. Gorenflo, "FastFabric: Scaling hyperledger fabric to 20 000 transactions per second," *Int. J. Network Manag.*, vol. 30, no. 5, p. e2099, 2020.
[66] S. Barbaria, H. Mahjoubi, H. B. Rahmouni, A. Jemai, and H. Mrabet, "Combined blockchain and IoT high level architecture for patient monitoring systems," in *Proc. 35th Annu. Eur. Simulation Modelling Conf. (ESM)*, 2021, pp. 184–190.
[67] D. Chadwick, A. Otenko, and E. Ball, "Role-based access control with X.509 attribute certificates," *IEEE Internet Comput.*, vol. 7, no. 2, pp. 62–69, Mar. 2003.
[68] A. Dabholkar and V. Saraswat, "Ripping the fabric: Attacks and mitigations on hyperledger fabric," in *Proc. Int. Conf. Appl. Techn. Inf. Secur.* Singapore: Springer, 2019, pp. 300–311.
[69] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requirements Eng.*, vol. 20, no. 2, pp. 163–180, 2015.
[70] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Netw.*, vol. 22, no. 2, pp. 491–502, 2016.
[71] X. Liang et al., "Towards a trusted and privacy preserving membership service in distributed ledger using intel software guard extensions," in *Proc. Int. Conf. Inf. Commun. Secur.* Springer, 2017, pp. 304–310.
[72] V. Costan and S. Devadas, "Intel SGX explained," Cryptol. ePrint Arch., Paper 2016/086, 2016, pp. 1–118.
[73] C. Kolias, "DDoS in the IoT: Mirai and other BotNets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
[74] N. Andola, "Vulnerabilities on hyperledger fabric," *Pervasive Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101050.
[75] C. Anderson, "Docker [software engineering]," *IEEE Softw.*, vol. 32, no. 3, pp. 102–C3, May 2015.
[76] G. W. Beeler, "HL7 version 3—An object-oriented methodology for collaborative standards development," *Int. J. Med. Inform.*, vol. 48, nos. 1–3, pp. 151–161, 1998.
[77] J. C. Mandel, "SMART on FHIR: A standards-based, interoperable apps platform for electronic health records," *J. Amer. Med. Inform. Assoc.*, vol. 23, no. 5, pp. 899–908, 2016.

SABRI BARBARIA received the B.Sc. degree in biomedical engineering and the M.Sc. degree in medical imaging from the University of Tunis El Mana. He is the IHE Certified Professional and a Consultant in healthcare systems interoperability. He was involved in many medical informatics projects, specifically in data security and medical system modeling. He is a member of the Research Laboratory of Biophysics and Medical Technologies, Higher Institute of Medical Technologies of Tunis, Tunisia.

MARCO CASASSA MONT (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science. He was a Principal Cyber Security Architect and a Lead Scientist at HP Labs. He is currently a Principal Cyber Security Consultant at BMT, Defence and Security, U.K. He is also a $(ISC)^2$ CISSP and CCSP Certified Cyber Professional. He has over 20-years' experience in cyber security, enterprise and cloud solutions, strategic consulting, trusted advisory, and innovation. His research interests include cyber security for cloud, enterprise and deployed platforms, advanced threat detection, risk assessment, security strategies, and roadmaps.

ESSAM GHADAFI received the B.Sc. degree in computer science from the University of Tripoli, in 1998, and the M.Sc. degree (Hons.) in advanced computing and the Ph.D. degree in cryptography and information security from the University of Bristol, in 2008 and 2012, respectively. He worked as a Postdoctoral Researcher with the University of Bristol and University College London. He is currently a Senior Lecturer in cyber security at Newcastle University, U.K. He led and participated in various research projects. His experience also includes supervising Ph.D. students. His research interests include cryptography and information security.

HALIMA MAHJOUBI MACHRAOUI received the Diploma of Advanced Studies degree in radiological physics and the Ph.D. degree in radiological and medical physics from Paul Sabatier University, Toulouse, in 1986 and 1992, respectively, and the University Habilitation degree in radiological physics from the University of Tunis, in 2001. In May 2006, she occupied the post of an Expert of the National Commission for Health and Medical Technologies. She has been the Director of the Research Laboratory in Biophysics and Medical Technologies, Higher Institute of Medical Technologies of Tunis (ISTMT), since 2012. She has also acted as the Director of the ISTMT (2012–2017). She is currently a Professor of biophysics. She is the Vice President of the University of Tunis El Manar responsible for scientific research, technological development, and partnership with the society. Her main research interest includes medical technologies, including ICT for health.

HANENE BOUSSI RAHMOUNI received the B.Sc. (Hons.) and Ph.D. degrees in computer science from the University of the West of England (UWE), Bristol, U.K. She is currently a Senior Lecturer in information science at the Faculty of Environment and Technology, UWE. She was involved in various research projects funded by the European Commission at UWE and the HealthGrid Organisation, France. She has also given numerous presentations to scientific audiences, technologists, and decision makers. Her research interests include many aspects of design, development and implementation of distributed information systems using (databases, data science, knowledge representation, ontologies and semantic web technologies, artificial intelligence, security and data protection) technologies.