IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 August 2022, accepted 23 August 2022, date of publication 29 August 2022, date of current version 8 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3202902

RESEARCH ARTICLE

A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT

AHMAD N. GOHAR[1,2], (Senior Member, IEEE), SAYED ABDELGABER ABDELMAWGOUD[1], AND MARWA SALAH FARHAN[1,3]

[1] Faculty of Computers and Artificial Intelligence, Helwan University, Helwan 11795, Egypt
[2] Client Innovation Centre, IBM, Giza 12577, Egypt
[3] Faculty of Informatics and Computer Science, The British University in Egypt, El Shorouk City 11837, Egypt

Corresponding author: Ahmad N. Gohar (ansgohar@gmail.com)

ABSTRACT Due to the distributed and non-integrated nature of the healthcare systems which results from the application-centric view it leads to a challenging task to manage healthcare data exchange (heterogeneity problem). On the other hand, Blockchain technologies are emerging as promising and cost-effective means to meet some of these requirements due to their inherent design properties, such as secure cryptography and a resilient peer-to-peer network. Likewise, Blockchain-based applications can benefit the healthcare domain via their properties of asset sharing, and audit trails of data access. Existing work mainly pays attention to centralized and blockchain-based mechanisms. But it doesn't realize the increase need for better data interoperability amount multiple healthcare systems and services. This requires shifting from the application-centric solutions toward the patient-centric solutions. This paper presents A secure and efficient framework based on Blockchain, Cloud, and IoT named Patient-Centric Healthcare Framework (PCH) for better healthcare systems interoperability. A tiered-based architecture (5 tiers) with collaboration is designed for the feasible realization of PCH. Also, the design and implementation aspects start from the layering diagram, system context, and detailed reference architecture that emphasizes the detailed component topology and interactions within the framework. An electronic medical record is used to show how healthcare data is processed with the required security considerations. Then, an evaluation of PCH against the existing Blockchain-based healthcare frameworks is conducted. The results analysis demonstrates that PCH offers practical solutions to protect healthcare data and support efficient data sharing with better interoperability.

INDEX TERMS Blockchain, chaincode, digital health, distributed ledger technology (DLT), eHealth, EHRs sharing, electronic health records (EHRs), endorsement, fabric, health information exchange, Hyperledger, ordering service, smart contracts.

I. INTRODUCTION

The fundamental promise of the Blockchain is the underlying information technology (IT) architecture and its 'unbreakable' chain of data entries that allow for secure and open transactions. The decentralized and distributed blockchain database that contains data allows for an auditable and distributed ledger to see every transaction. The open-source attributes of the Blockchain make the technology a natural fit for the requirements associated with the complexities of the transaction-laden systems related to health information technology in the public and private sectors. The advantages of Blockchain are apparent, but with any new technology, there are questions about efficacy and efficiency [1]. Blockchain technology (BCT) was initially designed for its best-known implementation in economics and cryptocurrencies, but today

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

its utility is expanding in several other areas, including the biomedical field. The potential of blockchain technology can be witnessed in medicine, genomics, telemedicine, telemonitoring, e-health, neuroscience, and personalized healthcare applications by its mechanism of stabilizing and securing the data set with which users can interact through different types of transactions [2].

A. BLOCKCHAIN TAXONOMY

Blockchain types are discussed from two different perspectives: a technological perspective with a high level of abstraction and a business perspective. Blockchain is categorized into a private, consortium, and public Blockchain from a technical perspective. From a business perspective, those types are regrouped into two categories: closed Blockchain for private or consortium Blockchain which are allied with a limited environment such as a company, group of companies or one specific value chain, and open Blockchain for public Blockchain which supports a permission-less variety of Blockchain [3].

1) CLOSE BLOCKCHAIN

From a business perception, due to the similar advantages that both private or consortium blockchains offer for an enterprise, this solution uses Blockchain in a fixed environment or, in other words, is an enterprise-focused solution that by allowing no change in the environment, the only beneficial effect of Blockchain comes from an optimization of the process. Closed blockchain solutions, mainly consortium one, help to produce transparent markets where the known market players (owners of the current infrastructure) benefit from creating a closed blockchain system that is very controlled. A lock-in effect occurs when the users are part of the secure dominant system. The dominant players can decide if new market players may enter the system or not, forcing users to buy additional updates or hardware [4].

2) OPEN BLOCKCHAIN

A public blockchain can result in disruptive changes and lead to a programmable economy. An open blockchain allows anyone can build solutions to be used by anybody else. This can form new economic models such as a zero-margin economy where the new market players like machines who own themselves break the current industry and market models barriers and permit machine-to-machine transactions. Blockchain could be applied to many business application fields as many public blockchains arise step by step, practically the same as a consortium [5].

B. NECESSITY FOR BLOCKCHAIN IN HEALTHCARE

Several problems as shown in Fig. 1 with centralized EHR systems exist like healthcare data breaching issues, a single point of failure, personal and sensitive personal information privacy issues, and interoperability issues between multiple systems/data sources. Those main problems can be summarized as follows [6], [7], [8].

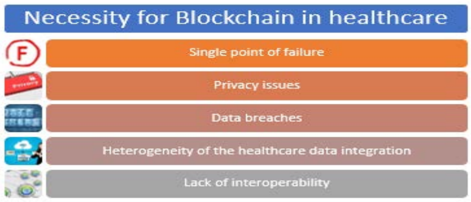
Necessity for Blockchain in healthcare
F
Single point of failure
Privacy issues
Data breaches
Heterogeneity of the healthcare data integration
Lack of interoperability

FIGURE 1. Necessity for blockchain in healthcare.

1) SINGLE POINT OF FAILURE

Depending on the centralized systems often suffers from the fear of data crashes due to the presence of most of the data in one place; thus, one node/server failure results in the downfall of the system entirely [9].

2) PRIVACY ISSUES

In the health sector privacy issues have led to decreased patients' trust in the EHR. Thus, if the privacy of sensitive health information is weak, then public confidence becomes difficult to be maintained in the health care delivery system. Despite the expanded convenience and feasibility offer by the EHR, patients are in continuous fear regarding their health information's integrity and privacy [10], [11].

3) DATA BREACHES

EHRs are likely to be attacked by hackers with a comprehensive awareness of network navigation, which remains unprotected. As attackers can see all information within the EHR files such as patients or doctors' names, addresses, payment information, medications, and history records. Despite EHR benefits the process of health care, but, it can also be vulnerable to attacks if they were not adequately secured [12].

4) HETEROGENEITY OF THE HEALTHCARE DATA INTEGRATION

There are different types of data including structured, semi-structured, and unstructured. Statistically, 80% of medical data are unstructured, which further complicates the management of these data. The major source for healthcare applications is patient records. Data integration is the task of combining different data sources and providing a unified view of the data. Such integrated data are needed to be standardized and kept in a repository. However, integrating data from a variety of sources is not a trivial task, due to the large volumes of heterogeneous data during mapping, ranking, and key matching. Moreover, structural, and semantic heterogeneity is another problem that faces data integration [13].

5) LACK OF INTEROPERABILITY

Robust EHR interoperability is vital for providing effective patient-centered care that it is lacked in most EHR systems as being shown in recent findings. When a patient visits a specialist or an emergency and receives treatment, the healthcare provider must access the patient's health history with a broader, up-to-date view of the patient information carried at the point of care for ensuring the highest levels of clinical quality whereas effective interoperable systems likely improve the provider's productivity field. Thus when data standards are varied, systems became less interoperable because all the records are not compatible with the procedures [14].

The remainder of this paper is structured as follows; section 2, analyzes the existed related work. Section 3 presents industry preliminaries for Blockchain technologies. The proposed framework architecture for resolving heterogeneity, integrity, and retrieval of healthcare data is discussed in section 4. Section 5 offers the detailed framework reference architecture, while sections 6-8 give an overview of the implementation details and its obstacles. Section 9 supported the use-case scenario. Finally, sections10-12 conclude with results, discussion, and research conclusion.

II. RELATED WORK

This section focuses on discussing how healthcare data sharing/management leverages Blockchain infrastructure, technologies such as cloud computing and big data, the detailed implementation of the Blockchain in the healthcare industry, and the interoperability in the healthcare environment.

A. HEALTHCARE DATA MANAGEMENT WITHOUT BLOCKCHAIN

Sharing healthcare data among interested stakeholders (e.g., public health institutions, patients, etc.) has been explored concerning multi-source, heterogeneous data using Cloud computing, IoT, and Big Data analytics techniques. The data management layer of their proposed architectures suggests strategies that depend on distributed parallel computing and distributed file storage grounded on memory analysis to cope with real-time analysis of big data warehoused on their infrastructure [15]. Compared with the proposed techniques, the collected data on-chain design is neither stored nor processed. The metadata on-chain (hashed data, data reference URLs, and permissions) are reserved that allowing a secure, private, and auditable way for data sharing.

B. HEALTHCARE DATA MANAGEMENT WITH BLOCKCHAIN

Blockchain has been proposed by the authors of this work as a suitable infrastructure for sharing healthcare data. In addition, the usage of the Hyperledger Fabric Blockchain network to enhance the consent transparency and traceability given by patients involved in clinical trials has discoursed in the frames of this work.

Dubovitskaya *et al.* [16] proposed a framework for empowering eHealth based on Blockchain, applying radiation oncology data management. This prototype was developed using Hyperledger Fabric, and its architecture consists of a frontend user interface and a backend composed of two components: membership service and certification authority. This proposal is one of the Blockchain frameworks for business that uses the Cloud environment. Still, it saved the critical data off-chain, which empire the security, and generally, this is considered a very shallow idea level that missed the implementation aspect.

Liang *et al.* [17] designed and implemented a mobile-based healthcare system for personal health data collection, sharing, and collaboration between individuals, healthcare providers, and insurance companies based on blockchain technology. In addition, the system was extended to accommodate the health data usage for research purposes. The algorithm used to handle data records can simultaneously preserve integrity and privacy. The main advantage of the framework is adopting the channel concept that Hyperledger Fabric supports to deal with the isolated communication required by specific scenarios. Still, the main missed section is the implementation details for reference.

Li *et al.* [18] introduce a decentralized medication management system (DMMS) that uses a blockchain ledger to manage medication histories. However, the Proof-of-concept (POC) shows an integrated standard healthcare application using a primitive definition for the healthcare entities. However, using the Hyperledger Composer terminologies while implementing Hyperledger Fabric requires a common healthcare framework to integrate with.

Jamil *et al.* [19] proposed A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital based on Hyperledger Fabric describing its design, implementation, and performance evaluation. An intelligent contract developed in the solidity programming language in combination with permissioned blockchain architecture that is used to achieve transparency, security, and privacy of the proposed system, carrying out several experiments to test the suggested system's performance in terms of transaction response time, throughput, latency, and resource utilization.

Yang *et al.* [20] present a privacy-preserved blockchain scheme for collaborative medical decision-making, including the security of Blockchain and personal data privacy and identifying the reasons for the lack of medical collaboration and the associated risks. Concerning the proof of familiarity (PoF), a consensus gathering algorithm is designed to assimilate healthcare stakeholders' medical decisions (patient, doctor, insurance company, cured patient). The proposed PoF consensus algorithm efficiency is confirmed with multichain 2.0(an open-source blockchain simulation platform). A two-layer security measure is followed while preserving the stakeholders' identity; the First layer is concerned with storing the identities of patients, cured patients, doctors, and insurance companies locally. The second layer is concerned with hashing those identities stored in a block. In addition, modified blockchain architecture is used (off-the-chain) for securing clinical data. Allowing the trusted participation of the medical decision-giving entities to afford improved clinical decisions.

Sharma and Balamurugan [21] proposed a system to deploy a Blockchain-based EHR network and implement basic functionalities in the network with the primary objective

TABLE 1. State-of-art Blockchain-based approaches to secure EHR systems.

Metric	Jamil et al. [19]	Musamih et al. [23]	Rajput et al. [24]	P.Zhang et al. [26]	Antonio et al. [28]	A.Azaria et al. [29]
Tamper-proof	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy
Non-Repudiation	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy
Attack Resistance	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy	Fully Satisfy
Access Control	Fully Satisfy	Not Satisfy	Fully Satisfy	Not Satisfy	Partially Satisfy	Fully Satisfy
Access Revocation	Fully Satisfy	Not Satisfy	Fully Satisfy	Not Satisfy	Not Satisfy	Fully Satisfy
Privacy-Preserving	Fully Satisfy	Partially Satisfy	Not Satisfy	Not Satisfy	Not Satisfy	Fully Satisfy
Patients Control Access	Fully Satisfy	Not Satisfy	Not Satisfy	Partially Satisfy	Partially Satisfy	Not Satisfy
Different user types	Fully Satisfy	Not Satisfy	Not Satisfy	Partially Satisfy	Partially Satisfy	Not Satisfy
Block Search	Not Satisfy	Not Satisfy	Not Satisfy	Not Satisfy	Fully Satisfy	Not Satisfy
Data Format	JSON	JSON	JSON	FHIR	FHIR	JSON
Blockchain platform	H. Composer	Ethereum	H. Fabric	Ethereum	Ethereum	H.
Architecture	Partially Satisfy	Partially Satisfy	Not Satisfy	Fully Satisfy	Partially Satisfy	Not Satisfy
Implementation	Fully Satisfy	Not Satisfy	Partially Satisfy	Fully Satisfy	Not Satisfy	Partially Satisfy
Interoperability	Not Satisfy	Not Satisfy	Not Satisfy	Foundational I	Not Satisfy	Not Satisfy

[N] Not satisfied, [P] Partially satisfied, [F] Fully Satisfied.

of framing data privacy and security issues in electronic healthcare as the proposed framework maintains the balance between data privacy and data accessibility. Nevertheless, on the other hand, the idea and implementation need a further extension by implementing various smart contracts to handle the advanced functionality of the EHR system. In addition, different sectors like billing, transportation, etc., can be added to the network to implement a full-fledged healthcare management system. To make it interactive, it can be integrated with a web application.

Tanwaret al. [22] proposed a blockchain-based EHR system architecture composed of four participants: Patient, Clinician, Lab, and System admin. In this system, various assets or smart contracts are defined, including, but not limited to: CreateMedicalRecord, GrantAccessToClinician, GrantAccessToLab, RevokeAccess, RevokeAccessToLab. The proposed work eliminates the central authority and a single point of failure in the system. System security is achieved through immutable ledger technology as any user cannot modify the ledger. Also, performance evaluation of the proposed system is completed using the Caliper for various scenarios by configuring block size, block creation time, endorsement policy, and proposed optimization for evaluation metrics, such as latency, throughput, and network security for better results. By optimizing the performance of the proposed system, it is improved by 1.75x, and latency is decreased by 1.5x.

Musamih *et al.* [23] investigated the challenge of drug traceability within pharmaceutical supply chains, highlighting its significance primarily to protect against counterfeit drugs, then presented an Ethereum blockchain-based approach leveraging smart contracts and decentralized off-chain storage for efficient product traceability in the healthcare supply chain. They explained the system architecture and detailed algorithms that govern the working principles of the proposed solution. Then they performed testing and validation and presented the system's cost and security analysis to evaluate its effectiveness to enhance traceability within pharmaceutical supply chains. The proposed solution leverages cryptographic fundamentals underlying blockchain technology to achieve tamper-proof logs of events within the supply chain. It utilizes smart contracts within the Ethereum blockchain to achieve automated recording of events accessible to all participating stakeholders. Additionally, the proposed solution is cost-efficient regarding the amount of gas spent executing the different functions triggered within the smart contract.

Rajput *et al.* [24] suggested a novel access control framework that preserves personal health record (PHR) data privacy in patient's emergency conditions. It works grounded on permissioned Blockchain Hyperledger Fabric and Hyperledger Composer playground for assessing the framework's performance. The experimental results declared that this framework guarantees the secret data sharing of the PHR through considering the auditing, immutability, and emergency access control policies. Furthermore, as the PHRs are exchanged/shared among different participants (agencies), a standard like HL7 FHIR is required for assuring the security of data sharing implementation.

Nguyen *et al.* [25] proposed a new cooperative architecture of sharing and offloading data for healthcare by leveraging Ethereum blockchain and edge-cloud computing. Also, a privacy-aware data offloading scheme is offered where under system constraints, the MDs can offload IoT health data to the edge server. Then, a new data-sharing is presented by using Blockchain and smart contracts enabling secure data exchange between diverse healthcare users. A reliable access control mechanism accompanying a decentralized InterPlanetary File System (IFPS) storage design on the cloud were developed. Additionally, the data-sharing scheme reaches efficient user authentication and significantly increases data retrieval speeds even though protecting the healthcare system from malicious access. By evaluating the system, it was proved that the smart contracts' operation cost is low, and system security is guaranteed, showing the healthcare applications' scheme feasibility.

The relative comparison of the state- of-the-art blockchain-based approaches to secure EHR systems is given in Table 1.

Tamper-proof and Non-Repudiation dimensions are fulfilled by all the mentioned frameworks as those as the basic features that is mandatory for all frameworks. Attack Resistance are fulfilled by all frameworks except Zhang *et al.*'s framework [26]. Although Access Control is an important feature however booth Musamih *et al.* [23] and Zhang *et al.* [26] didn't address it in the framework. Also the Access Revocation as an advanced level is addressed by Jamil *et al.* [19], Rajput *et al.* [24], and Chukwu and Garg [27].

Blockchain platform used main two frameworks; Musamih *et al.* [23], Zhang *et al.* [26], and Fusco *et al.* [28] adopted Ethereum. On the other hand the remaining frameworks used Hyperledger umbrella. To be specific Jamil *et al.* [19] use Hyperledger Composer while Rajput *et al.* [24] use Hyperledger Fabric.

Design and architecture perspectives were loosely detailed. Architecture view point detailed only by Fusco *et al.* [28]. Although detailing the implementation is addressed by Jamil *et al.* [19] and Rajput *et al.* [24]. Finally, the interoperability perspective is only addressed by Fusco *et al.* [28].

III. PRELIMINARIES

This paper employs a Hyperledger Fabric blockchain platform for building our e-health PCH framework. Typically, Hyperledger Fabric is one of the many Hyperledger projects hosted by The Linux Foundation. A significant advantage of Hyperledger projects is its flexible and adaptable features, that allow building of blockchain applications for instance, e-healthcare. The Hyperledger network's main components employed in the proposed framework design are reviewed.

A. HYPERLEDGER FABRIC

An enterprise-grade open-source permissioned framework implementation for both permissioned and private business blockchain networks with a modular design and high specificity through trust models and pluggable components. It is constructed as a core for development of solutions through a modular architecture allowing components, for instance ledger database, membership facilities, and consensus mechanism, for plug-and-play. It leverages container technology and provides enterprise-ready network security, confidentiality, and scalability [30].

Network exists for the reason that organizations contribute their resources to the collective network. The ordering service sent to peers on a channel transactions packaged into blocks for guaranteeing delivery of transaction in the network, and communicating with peers and supports them with supported configuration mechanisms for the ordering service such as Kafka and Solo [31].

A Hyperledger Fabric network has these components, as shown in Fig. 2: Asset can be described as something has value such as state and ownership, embodied in Hyperledger Fabric as a set of key-value pairs. While world state defines the state of ledger at a specified point in time. The smart contracts of Hyperledger Fabric are termed Chaincode that is a software written in Node.js or Golang stating the assets along with their related transactions; in other words, it can be considered as the system's business logic. Thus, for an application needs to interact with the ledger Chaincode is invoked. Peer nodes are considered as a fundamental element of the network because of their ledgers and smart contracts' hosting. A peer executes chaincode, accesses ledger data, endorses transactions, and interfaces with applications. Some peers can be endorsing peers or endorsers. Channels are a logical structure designed by peers assembly, and this capability allows them to create a separate transactions ledger [32].

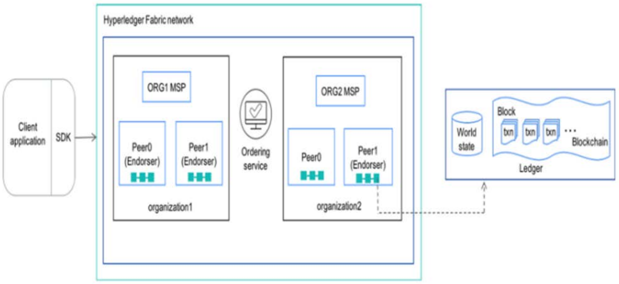

FIGURE 2. The components of a Hyperledger Fabric network.

B. ASSETS

In an ideal world, assets are digital or intangible, but you must develop solutions for physical assets. In a typical business scenario, participants are known and identifiable because of existing relationships. Asset ownership is transferred through transactions, which must follow a set of business terms [33].

C. SHARED LEDGER

A ledger consists of two distinct however related parts: a "blockchain" and the "state database," also identified as the "world state". Unlike other ledgers, blockchains are immutable; after a block is added to the chain, it cannot be changed. In contrast, "world state" is a database encompassing the current value for a set of key-value pairs whether added, modified, or deleted transactions in the Blockchain that has been validated and committed [34].

D. BLOCKCHAIN

The Blockchain is composed of a chain of blocks, and a new block is always appended to the end of the chain. A block might consist of zero or several transactions, depending on how the block configuration was defined either as Time-based, Transaction-based, Memory-based.

The crucial aspect that makes the Blockchain immutable is a mathematical hash function. As shown in Fig. 3, each block contains a previous block's hash, which is included in calculating the next block's hash. This hash signifies whether any block has been tampered with, and then the corresponding hash value changes and the Blockchain is no longer linked together, as shown in Fig 3. Because the genesis block is the first block in the chain and does not contain any previous blocks. It usually includes an arbitrary key-value to initialize the hash function [35].

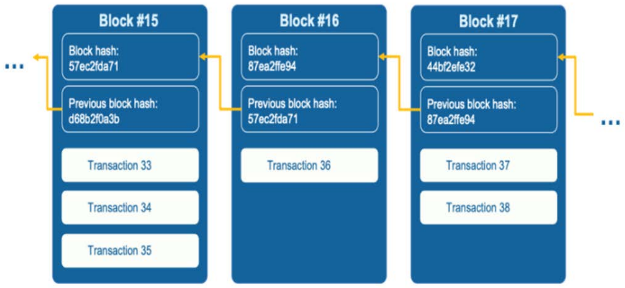

FIGURE 3. **Blockchain block structure.**

E. WORLD STATE (STATE DATABASE)

Also known as "current state," which is a one of the Hyperledger Fabric Ledger components representing the latest values for all keys involved in the chain transaction log. Chaincode runs transaction proposals against world state data since the world state offers direct access to the latest value of these keys instead of calculating them through the entire transaction log traversing. Every time the value of a critical change or when a new key is added, the world state changes. Consequently, the world state is crucial to a transaction flow as the key-value pair current state must be known before changing it. Thus for each valid transaction included in a processed block, the Peers bind the latest values to the ledger world state [36], [37].

F. SMART CONTRACT (CHAINCODE)

A smart contract can be described as a code called by a client application external to the blockchain network managing access and modifications for a set of key-value pairs in the World State. In Hyperledger Fabric, smart contracts are termed chaincode, that is installed onto peer nodes and instantiated to one or more channels [38].

1) USER CHAINCODE

Typically, a user chaincode handles business logic approved by network members, so it is like a "smart contract." A chaincode can be called for querying or updating the ledger in a proposed transaction. Assumed the appropriate permission is given, to access its state, a chaincode may call another chaincode, either in the same channel or in different channels [30].

2) SYSTEM CHAINCODE

As normal user chaincode, the system chaincode has the same programming model which is built into the peer executable, distinct from user chaincodes. Fabric implements various system chaincodes [34], [37].

G. PEER NODES

At the heart of the Hyperledger Fabric network is a network of peers (or peer nodes) as shown before in Fig. 2. The peers are hosted by the business participants, endorse transactions, and commit the transactions to the ledger. Each peer runs and maintains the shared ledger, including the Blockchain of transactions and the world state database. There are two roles for a peer: endorser and committer. Every peer is always a committer, but not necessarily always an endorser. As mentioned earlier, transactions must be endorsed, and only endorsed transactions may be committed and their output stored in the world state database [39], [37].

1) COMMITTING PEER

Every peer in the network is a committer. The committer-Receives the block of endorsed transactions from the ordering service, validates each transaction in the block, and commits the block to the shared ledger by appending the block of transactions to the Blockchain for a specific channel and updating the world state database for that channel with the updated asset information [39].

2) ENDORSING PEER

Peers can assume the unique role of an endorsing peer, that is, an endorser; Every smart contract may specify an endorsement policy denoting to a set of endorsing peers. This policy states the essential and adequate conditions for a valid transaction endorsement. For a smart contract, the endorsing peer endorses a transaction before it is committed. Endorsing peers endorse the updated proposed ledger to the application but do not spread over the proposed update to the ledger [37].

H. ORGANIZATIONS

Blockchain networks are composed of and administered by multiple organizations instead of a single organization. By these organizations, Blockchain network is established and managed as they contribute their resources, like nodes, certificate authorities, computing power, physical connections, and others, as without these contributions, the network cannot exist. The network expands and diminishes (as organizations join and leave the network), not dependent on a single organization. Typically, an organization operates multiple peer nodes for different reasons, such as redundancy or performance reasons [40].

I. MEMBERSHIP SERVICES PROVIDER

A Blockchain Framework for Managing and Monitoring Data in Multi-Site Clinical Trials offers an abstraction of a membership operation architecture. The MSP abstracts all the cryptographic mechanisms and protocols behind issuing and validating certificates and user authentication. The MSP is installed on each peer to ensure that transaction requests issued to the peer originate from an authenticated and authorized user identity [32].

Clients use these credentials to authenticate their transactions, and peers use them to authenticate transaction processing results (endorsements). Although connected to the system's transaction processing components, this interface aims to define membership services components so that alternative implementations of this component can be smoothly plugged in without modifying the core of the transaction processing components of the system [22].

J. ORDERING SERVICE

The orders from the ordering service, that is, a communication fabric that ensures delivery. When the client application needs the endorsed transactions committed to the shared ledger, it sends the transactions to the ordering service. The ordering service orders the transactions, groups them into a block, and sends them to their peers. This action determines how transactions are committed to the shared ledger [41]. The order is essential to ensure that the world state database updates are valid. Moreover, the ordering service can be executed in multiple ways, ranging from a centralized service that is used in development and testing to distributed protocols targeting other network as well as node fault models [32].

The ordering service exists on a first-come-first-serve basis for all channels in the network independently from the peer processes and order transactions. The ordering service supports pluggable implementations beyond the standard Solo, Kafka, and Raft varieties. The ordering service commands the overall network encompassing the cryptographic identity material tangled to each member [30].

K. CHANNEL

Fabric presents a channel concept as a "private" subnet of communication among two or more peers for providing a higher isolation level. The peer members and participants only see transactions on a channel. Both immutable ledger and chaincodes are on a per-channel basis. Additional, the consensus is applicable on a per-channel basis, thus for transactions across channels there is no defined order [30].

In Hyperledger Fabric, the concept of channels offers another approach to achieving data privacy among a subgroup of network participants. By design, participants inherently transact in the channel scope and maintain the ledger that is uniquely associated with this channel. As a result, channels work by data segregation, meaning that members of a specific channel have access to the data on that channel's ledger. The information is not accessible to non-members. A channel configuration defines the permissions at the channel level. The channel administrators agree on it, and it is stored on the channel's ledger in an immutable form as part of a configuration transaction, as shown in Fig.4 [34], [42].

L. CLIENT APPLICATION

Client applications continually connect to peers as soon as they must access chaincodes and ledgers. Transactions must be endorsed, where only endorsed transactions may be committed and their output stored in the world state database. The software development kit (SDK) that is provided by the Hyperledger Fabric Client (HFC) enabling client applications to connect to peers for getting transactions endorsed, submitting endorsed transactions to the network to be committed to the distributed ledger, that is by the process completion, they receive events from the Blockchain [43].

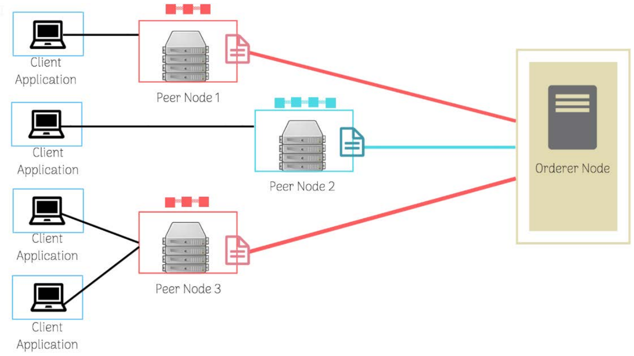

FIGURE 4. System architecture of Hyperledger Fabric showing private channels.

IV. PROPOSED FRAMEWORK

The amalgamation of the Blockchain, Cloud, Internet of Things (IoT), and analytics for holding and validating the health data of the patient and healthcare ecosystem in a unified, integrated healthcare framework. The proposed methodology uses the blockchain network to intercept and fetch the data generated from different healthcare systems and other wearable devices worn by the patient. Therefore, it is preferably used to store and maintain the patients' data in several transactions and provide access control support to diverse stakeholders.

Moreover, Blockchain architecture also supports medical research by maintaining the health status of the patient's identification and providing authenticated and trusted data for more accurate analysis. The Cloud model is used basically for minimizing the costs and sustaining the utilized capacity fluctuation of the system servers. The IoT is used mainly to collect healthcare information from multiple medical devices and smartphones. Analytics will visualize the outcomes from the semantic interoperability of the collected healthcare data.

We have attempted to redefine the standard set of layering the proposed framework from base layered architecture to introduce the tier concept for better isolation and separation of responsibilities. Measures that are used to evaluate the layered architecture of the software. We have also defined steps to verify the layers' logical separation to ensure the layered structure's quality.

This section will tackle the proposed patient-centric healthcare (PCH) framework from multiple viewpoints and details. It starts with the tier/layer model to the high-level grouping of the solution components. This is followed by more elaboration on the human and technical actors inside the proposed system actor model. Finally, the system context shows the boundaries of the proposed framework.

A. TIE/LAYER MODEL

The layered architecture pattern is the most common architecture pattern, which is an elements' logical structuring mechanism that constitutes the software solution. In contrast, the N-tier architecture pattern is considered as a system's physical structuring mechanism. So, the proposed PCH model [44] was upgraded to a modified one, as shown in this section; the updated model is composed of six main tiers that are physically separated; each tear may consist of more than one layer where a specific functionality component resided.

One of the layered architecture pattern's powerful features is the separation of concerns between components. The components inside a specific layer deal only with a logic that relates to that layer. This component classification makes it easy to build responsibility models and influential roles in the architecture. It makes it easy to develop, test, govern, and maintain solutions via this architecture pattern because of its precisely-defined component interfaces and limited component scope.

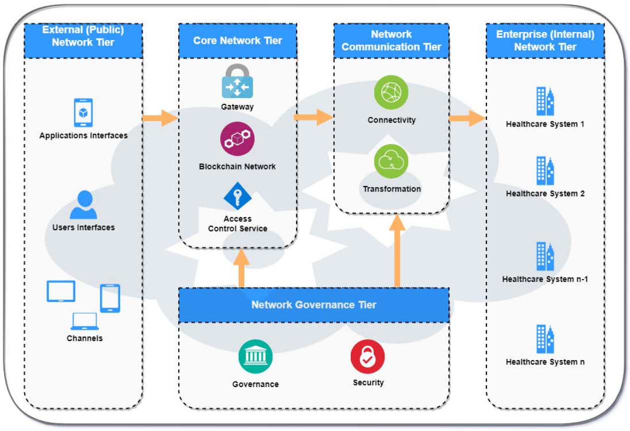

FIGURE 5. System architecture of Hyperledger Fabric showing private channels.

As shown in Fig. 5, the proposed framework is composed of 5 Tier as follows.

1) **External (Public) Network tier**, where the system users interact with the framework through the web, mobile, and web applications,
2) **Core Network tier**, where the solution logic and data store reside and are controlled,
3) **Network Communication tier** which plays the unified interface to integrate with all the healthcare applications,
4) **Enterprise (Internal) Network tier** which is composed of multiple healthcare networks/systems, and
5) **Network Governance tier** that insures and confirms all security and privacy aspects for the sensitive personal and healthcare information of the citizen.

B. SYSTEM ACTOR MODEL

An actor is an entity that interrelates with the system and needs to exchange information with the system. The actor is not part of the system itself and should represent anyone or anything that interacts with the system in the following ways: supplies input information to the system, receives data from the system, or both supplies input information to and receives data from the system. The research used to propose the following Healthcare actors can be categorized into (a) Acceptors, (b) Providers, (c) Supporters, and (d) Controllers' as shown in Fig. 6.

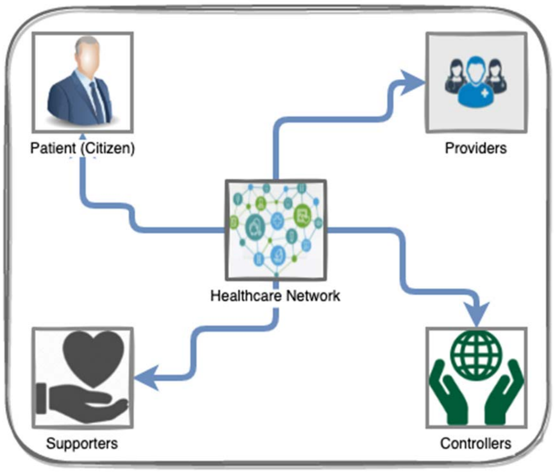

FIGURE 6. PCH Framework main actors' categories.

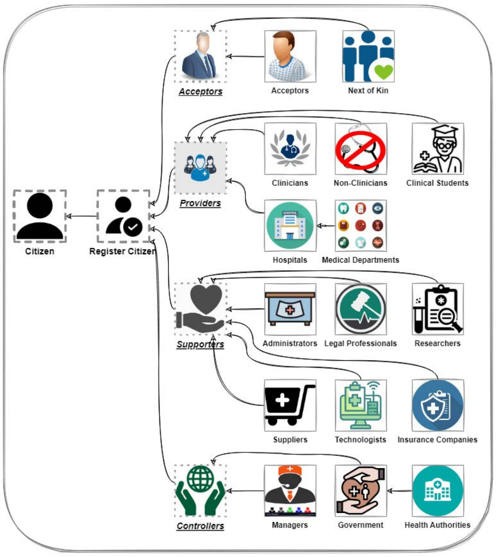

FIGURE 7. PCH Framework detailed system actor model.

Based on the multiple limitations [20], detailed and dynamic identification of the actors identifies a standard number (four) of human and organizational categories of healthcare actors, in an attempt to overcome any limitation, the adopted proposal, as shown in Fig. 7, more detailed and dynamic identification of the actors participating in the IS adoption process.

The combination of the human and organizational and the Actors' categorization can define healthcare actors. Based on this combination, a definition for healthcare actors is offered for further discussion: 'The healthcare actors involved in

TABLE 2. PCH framework actor matrix.

Actor Category	Actor Name	Actor Type	Description
Acceptor	Patients	Human	The Registered citizen that may request service from the system
	Next of Kin	Human	A person's closest living relative or relative
Provider	Clinicians	Human	Clinicians work directly with patients rather than in a laboratory or as a researcher.
	Non-Clinicians	Human	Non-clinical roles are those which do not provide any type of medical treatment or testing.
	Clinical Students	Human	Implementing clinical education of medical students in hospital.
	Hospitals	System	An institution which is managed, staffed and equipped for providing healthcare services, including inpatient care, surgery, emergent and urgent care, and has facilities for the diagnosis and treatment of disease.
	Medical Departments	System	Hospitals may have acute services such as an emergency department or specialist trauma center, burn unit, surgery, or urgent care.
Supporter	Administrators	Human	Health administrator is the one who managing, leading, overseeing, and administering the operation of dynamic, complex health care entities including hospitals, health care systems, nursing homes, pharmacies, and health insurance providers
	Legal Professionals	Human	The person who can receive healthcare, and who should pay for it. This is a surprisingly complicated area of law given how expensive healthcare can be.
	Researchers	Human	The person who practicing a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.
	Suppliers	Human	A person, or agency or any company that gives medical items such as a wheelchair or walker. a physician or other practitioner, or an entity other than a provider, that provides health care services under medicate
	Technologists	Human	A health care technologists can specialize in such areas as diagnostic imaging, laboratory testing, or surgical assisting. While job duties vary by specialization, technologists typically assist physicians
	Insurance Companies	System	Health insurance company is a type of insurance coverage that typically pays for medical, surgical, prescription drug and sometimes dental expenses incurred by the insured.
Controller	Managers	Human	Healthcare managers are appointed to positions of authority where they shape the organization by making important decisions.
	Government	System	Government's responsibility to protect and advance the interests of society includes the delivery of high-quality health care.
	Health Authorities	System	Health Authorities means the Governmental Entities which administer Health Laws including the FDA.

adopting information system can be defined as any human and organization that accepts, provides, supports or controls healthcare services.' All detailed information related to the categorization and description of each actor is listed in Table 2.

C. SYSTEM CONTEXT MODEL

A system context model in software engineering is a diagram that defines the boundary between the system or part of a system, and its environment, showing the entities that interact with it. This diagram is a high-level view of a system. The system's context view contains not only the entities outside the system's scope but also those directly related to the system.

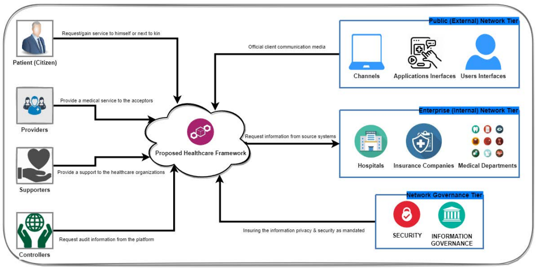
Patient (Citizen)
Request/gain service to himself or next to kin
Providers
Provide a medical service to the acceptors
Supporters
Provide a support to the healthcare organizations
Controllers
Request audit information from the platform
Proposed Healthcare Framework
Official client communication media
Public (External) Network Tier
Channels
Applications Inerfaces
Users Interfaces
Request information from source systems
Enterprise (Internal) Network Tier
Hospitals
Insurance Companies
Medical Departments
Insuring the information privacy & security as mandated
Network Governance Tier
SECURITY
INFORMATION GOVERNANCE

FIGURE 8. PCH Framework system context.

Fig. 8 shows the context view and portrays the system environment, boundaries, and the entities communicate with it. The external entities and their communications with the proposed healthcare framework were based on the concerns of the stakeholders from the system's actor section. Two external entities are considered obligatory: the public healthcare network and the enterprise (internal) network. The optional entity can be absent in simpler HISs such as the security and governance tier. Besides, some categorized actors may require specific entities.

Several entities execute two-way communication between each other. But only one type of communication per interaction is described due to space limitations; but in practice there are many more possibilities.

As shown before, the proposed framework interacts with all 16 actors (human & system) elaborated before. The communication media through the Channels will be listed in the ongoing sections. All healthcare systems, subsystems, and data where reside. All those communication and transaction should be governed through the governance and security components. The details of information flow between the main components are shown in Table 3.

V. REFERENCE ARCHITECTURE

The scope of the reference architecture is on concepts, logical elements, and associated models that can be used to apply and implement in a healthcare organization. The ultimate aim of this reference architecture is to help improve healthcare data interoperability on the semantic level. Its focus is on

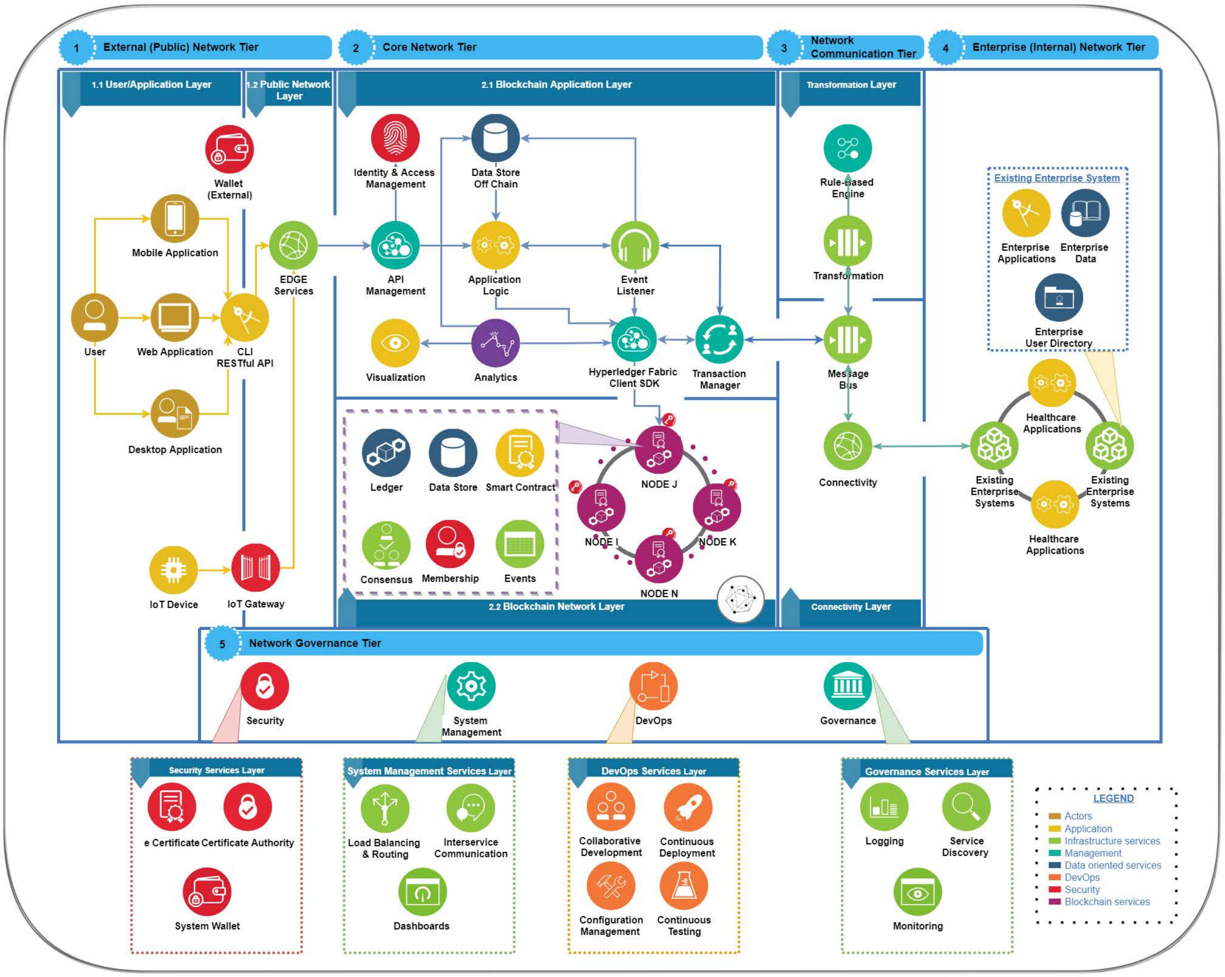

FIGURE 9. PCH Framework reference architecture.

TABLE 3. PCH framework system context information flow.

Source	Target	Information Exchange
Acceptor	Proposed Framework	Request/gain service to himself or next to kin.
Provider	Proposed Framework	Provide a medical service to the acceptors.
Supporter	Proposed Framework	Provides support to the healthcare organizations.
Proposed Framework	Controller	Request Audit information from the platform.
Channels	Proposed Framework	Official client communication media.
Enterprise Network	Proposed Framework	Request Information from source systems.

the citizen's health journey and how we aim for a healthy life and receive health services as patients. At every step on this journey, the reference architecture needs to support healthcare organizations to perform and deliver high-quality services safely and securely.

The breakdown illustrations how a system can be decomposed into several (sub-)modules and how they relate to each other. This view regularly can be considered as the basis for system's design, development, and documentation. The breakdown view supports checking the required modules' presence for all stakeholders. Such a breakdown view decomposes the system into five tiers with multiple layers, together with sub-modules and components.

As shown in Fig. 9, the proposed framework comprises tiered/layered subsystems; each subsystem is composed of multiple specialized components. The external (public) network layer allows users to access the proposed framework platform through the channels layer. The channel is formed of the media in which the users can interact with the platform. Then the Core Network tier abstracts the communication between the component mentioned in this section. It may be client on-premises location, cloud environment, and hybrid-cloud or multi-cloud topology. Those components can't communicate without the action performed by the Network Communication Tier. Those communications should be done between the Core Network environment and the Blockchain network. Due to the personal information (PI) and the sensitive personal information (SPI) transformed from the Enterprise Network Tier stored in the platform, the need for the Network Governance Tier appears.

A. TIER 1: EXTERNAL (PUBLIC) NETWORK

They start with the most outer tier exposed to the public domain in which the users and their interfaces interact with the network. This tier is composed logically of two main layers: the User/Application Layer and the Public Network Layer.

1) USER/APPLICATION LAYER

All the system users will reside inside this layer divided into two main categories: the users that send and receive the information from the system and the IoT devices that push the health care data.

The user will use the customized developed products such as Mobile applications, Web Applications, and Desktop applications to interact with the Representational state transfer (RESTful) APIs, which are kind of a software architectural style that was created to guide the design and development of the architecture for the World Wide Web and external systems. This was developed to ensure unified interfaces to all exterior applications.

The IoT Device collects citizen health information and passes it to the IoT Gateway to collect and aggregate it into valid information inside the next layer

2) PUBLIC NETWORK LAYER

Users and IoT devices use the external wallet to store their private credentials that allow access to the network. Upon validation and verification of transactions of the supported digital assets from the user's external wallet, it goes through the EDGE Service as an interface to the Core Network Tier. Users are those the network parties who form and distribute transactions inside the framework and accomplish processes utilizing the blockchain. These actors are coherent with the cloud computing actors together with roles from ISO/IEC ISO/IEC 17788 [45].

IoT Gateway is a physical device or software application that serves as the point of connection between the IoT application and end devices. All data moving to and from the IoT application server goes through the IoT Gateway. IoT Gateways are an essential part of our IoT infrastructure, so choosing a powerful and appropriate gateway is critical to the success of your project.

Edge services is a distributed information technology (IT) architecture in which client data is processed at the network's periphery, as close to the originating source as possible. Allowing data to safely flow from the Internet into the framework and providing support for end-user applications.

B. TIER 2: CORE NETWORK

After recognizing who uses the framework, let's define how requests access the platform and what components constitute the healthcare platform. The Core Network Tier comprises two layers: the Blockchain Application Layer and the Blockchain Network Layer.

1) BLOCKCHAIN APPLICATION LAYER

The first layer of the Core network tier is the Blockchain application layer, which serves as the network's brain composed of multiple subsystems and components—starting with the API Management platform, which addresses the spectrum of API lifecycle, monetization, and policy enforcement options. We leveraged the open-source API management to unify the interactions.

The second layer of security is Identity & Access Management (IAM), a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, framework auditors can control user access to critical information within their platform. We used for IAM the single sign-on (SSO) systems, two-factor authentication (TFA), and privileged access management. These technologies also provide the ability to store identity securely and profile data and data governance functions to ensure that only necessary and relevant data is shared.

With the support of the Application Logic components, the Event Listener component, and the Transaction Manager components, the core network tier manages the framework's transaction logic to ensure that the business processes are well executed under the agreed contracts.

Data visualization is translating information into a visual context, such as a map or graph, to make data easier for pulling insights from the collected data. The main goal of data visualization is to make it easier to identify patterns, trends, and outliers in system large data sets. This dimension is fulfilled from the Analytics components and the Visualization components.

The interaction with the Blockchain network stabilized through the Hyperledger Fabric Client SDK component that is considered as a programming library from client-side composed of a set of APIs that appears in the form of ''methods'' or ''calls,'' that can be used by client programs for accessing blockchain network functionalities and capabilities. Client programs can be written in Python, Node, Java, or any other supported languages. Additionally, SDK may also comprise development tools.

2) BLOCKCHAIN NETWORK LAYER

The Actual Blockchain components reside in the Blockchain network layer. At the same time, the modeling has to do with workflows. Since healthcare repercussions to a poorly defined or executed contract, great care must ensure that the warrant is issued correctly and free of potential weaknesses. The software also needs to be verifiable, secure, and reliable. The contract must be executed accurately and be free of possible faults. This layer comprises multiple Blockchain components like Node(s), Ledger, Data Store, Smart Contract, Consensus, Membership, Event.

Essential capabilities for blockchain solutions are supported in a blockchain network node or enterprise by the platform that is differently set up and implemented, thus in both blockchain platforms and solutions, the core capabilities should be considered. A ledger component is an arrangement of cryptographically connected blocks that hold transactions.

Smart contracts, occasionally termed chaincode, which are computer programs executed in a secure environment inside any network node's blockchain platform. Smart contracts encapsulate business logic comprising both contract terms and conditions that exist between agreeing participants. Additionally, they can be written in a programming language based on the blockchain platform while its code stored in the ledger determines the recorded healthcare transactions besides their information. Transactions can invoke smart contract stateful or stateless functions for performing business logic. Thus, if the code is required through the system integration component (Message Bus) then it will be able access external information and systems

The validity and order of transactions attached to the ledger can be approved by enabling consensus process to be used by the nodes inside the blockchain network. The consensus process preserves a consistently replicated register within the healthcare Blockchain network.

On the network, these services manage privacy, identity, auditability, and confidentiality. Membership only applies to permissioned blockchains that allow only specific actors submitting their transactions or validating the network. Those actors may be given various roles for performing a particular collection of operations.

On the other hand, for a non-permissioned blockchain, no distinctions of roles exist as participation does not need authorization, as well as all actors are able to equally submitting transactions or accumulating them into an acceptable and adequate block.

MSP used a secure container containing signed runtime components for instance, blockchain-supported programming languages libraries along with their corresponding runtimes, a secured operating system.

In the blockchain network, notifications of considerable changes or operations that are of interest to the blockchain network members are known as events. Event distribution appoints listeners to get the events from the blockchain, they always have event consumers who subscribe to events of interest and process them as they receive them and event producers who publish events of interest to the blockchain network. Moreover, appearing in an atomic broadcast, in a blockchain network the messages' sender sends it to all connected peer members in a similar instruction of sending sequence.

C. TIER 3: NETWORK COMMUNICATION

The primary purpose of the Network communication tier is to interact with the existing healthcare systems that are already in place and the citizen information scattered inside multiple vendors. To manage the vast transactions, we introduced the Message Bus component to combine a standard data model, a joint command set, and a messaging infrastructure to allow different healthcare systems to communicate through a shared set of interfaces. This tier comprises two main layers: the Transformation and Connectivity layers.

1) TRANSFORMATION LAYER

The semantic interoperability between health information systems is a significant challenge to improving clinical practice quality and patient safety. Thus, this layer comprises two main components: Transformation Component and the Rule-Based Engine Component. The transformations work to map the healthcare unstructured data format into a standard one using the power of the Rule-Based engine to manage and govern the process of data transformation.

2) CONNECTIVITY LAYER

To transform, the framework needs a specialized connectivity facility that helps connect different systems to map the connectivity protocols for the existing healthcare systems to maintain a stable transformation process.

D. TIER 4: ENTERPRISE (INTERNAL) NETWORK

The Enterprise (Internal) Network Tier comprises multiple existing healthcare applications and enterprise systems, including the Enterprise Application, the Enterprise Data, and the Enterprise User Directory. Those applications and systems store the operational information related to the healthcare information for the citizen. The main issue of this tier is that the modification of the existing systems will require much more cost to invest and will result in the refusal to proceed with the integration. So, this layer will remain intact, and the only modification will be through providing APIs from the proposed framework to integrate with.

An enterprise interacting with the blockchain network can create or use enterprise applications that may possibly act together with the smart contracts on top of the blockchain. Willy smart contract can obtain data from, send data to or request services from the enterprise application.

On the other hand, the enterprise user directory keeps user information for either supporting authorization, authentication, or profile data related to the enterprise applications while the connectivity and transformation services are controlling access to the enterprise services, enterprise network, or enterprise-specific cloud provider services.

Enterprise data comprises metadata in addition to record systems for enterprise applications that may possibly flow directly to data repositories or data integration which provide feedback loop in the blockchain systems' analytical procedure. Enterprise data correlates to blockchain consist of:

1) Transactional Data – Business interactions data that adhere to related processes whether healthcare or financial. This data is derived from reference data, distributed storage, and master data repositories.
2) Application Data – Enterprise applications functionally or operationally used or produced data. Usually, the data get enhanced or improved for adding value and driving insight.

3) Log Data – Data aggregated from enterprise applications' log files, infrastructure, systems, governance, security, etc.

E. TIER 5: NETWORK GOVERNANCE

The Network Governance tier interacts with all levels that allow its services and functionalities globally; it's composed of three main specialized layers: the Security service layer, system management service layer, DevOps services layer, and Governance services layer. Each service specializes in a critical role that provides the framework with the required functionalities.

1) SECURITY SERVICES LAYER

The security service layer will be an overall authentication and authorization using a container-based security model. The layer provides a standard security model for securing framework components and users. The layer comes with a variety of security components. Some of the standard options available are E Certificate Component, Certificate Authority Component, and System Wallet.

2) SYSTEM MANAGEMENT SERVICES LAYER

Systems management services refer to the centralized management of a framework infrastructure. It is an umbrella term and includes several components needed to manage and monitor framework system components. It's composed of the following main components Load Balancing & Routing Component, Interservice Communication Component, and Dashboards Component.

3) DEVOPS SERVICES LAYER

DevOps capabilities consist of analytics, monitoring, and automation tools used for responding to framework platform as well as environment changes including system capacity and error analytics. It's composed of Collaborative Development Component, Continuous Development Component, Configuration Management Component, and Continuous Testing Component.

4) GOVERNANCE SERVICES LAYER

The policies and procedures governing the blockchain network operations that network participants agree upon are recognized as governance. It's composed of the following components Logging Component, Service Discovery Component, and Monitoring Component.

VI. IMPLEMENTATION

A proof of concept (POC) implementation of decentralized access control is presented for sharing EHRs that focuses on the interoperability between the existing healthcare systems and the proposed method evaluation. Later, subsections showing the implementation details along with system configurations. Achieving semantic interoperability allows providers to exchange patient summary information with other caregivers and authorized parties using different I systems to improve care quality, safety, and efficiency.

A. HEALTHCARE INDUSTRY STANDARDS

PCH Framework achieves semantic interoperability by allowing providers to exchange patient summary information with other authorized parties using different I systems to improve care quality, safety, and efficiency. This level of interoperability allows healthcare organizations to seamlessly share patient information to reduce duplicative testing, enable better-informed clinical decision-making, and avoid adverse health events. Effective health data exchange can also help to improve care coordination, reduce hospital readmissions, and ultimately save hospitals money.

The HL7 (www.hl7.org) organization is an Standards Developing Organizations (SDO) accredited by the American National Standards Institute (ANSI) with the purpose of developing and publishing healthcare-specific standards. It publishes messaging standards for healthcare interoperability that aim to enhance care delivery, knowledge transfer and optimize workflow. HL7 products that PCH uses are HL7 version 3 (v3) messaging standard, Clinical Document Architecture (CDA).

The HL7 v3 messaging standard uses an information model called the Reference Information Model (RIM) and a formal methodology called the HL7 Development Framework (HDF) to increase the detail, clarity and precision of the message specification. The HL7 v3 Reference Information Model (RIM) provides a conceptual shared generic model that facilitates interoperability by standardizing all data models to a norm. CDA is a suite of HL7 v3 standards for representing clinical documents such as a referral form or a discharge summary.

B. SYSTEM SETTINGS

As shown in the architecture section, an interoperability EHRs framework on mobile, IoT, and hybrid cloud is considered. A Hyperledger Fabric blockchain network is deployed on Amazon cloud computing and the on-premises servers. The Cloud infrastructure is composed of two layers of the Core Network Layer. The Blockchain Application layer includes two virtual machines, AWS EC2, built based on the two virtual machines. Ubuntu 20.04 LTS was used as the application layer component. Detailed system setting and topology and illustrated in Fig. 10 below and elaborated in the below section.

Blockchain Network layer utilizes the Blockchain Application layer using a Linux computer through accessing the VPC resources for serving as Hyperledger Fabric client, thus AWS CLI version 1.16.149 or later is installed on computer. As AWS CLI prior versions do not have the managed-blockchain command. Thus, the latest version of the available AWS CLI is recommended to be used.

VPC must have an Ipv4 CIDR block, with enableDnsHostnames and enableDnsSupport options set to true. In case of connecting to the Hyperledger Fabric client utilizing SSH,

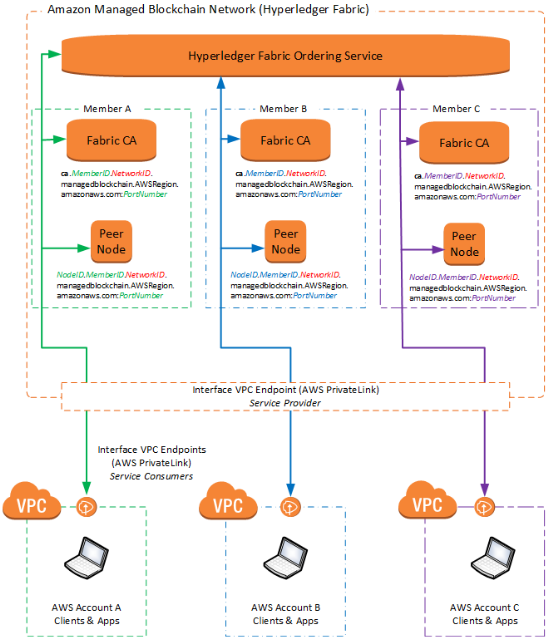

FIGURE 10. **PCH Framework AWS blockchain topology.**

VPC required to have an internet gateway, with security group configuration accompanied with the Hyperledger Framework client allowing inbound SSH access from SSH client.

The EC2 security groups accompanying with the Hyperledger Fabric client Amazon EC2 instance and VPC endpoint interface created must have rules allowing traffic between them for neededHyperledger Fabric services. EC2 security groups are restrictive by default, so that security group rules are needed to be made for enabling necessary access. Additionally, the security group linked with the Hyperledger Fabric client Amazon EC2 instance obligated to have an inbound rule allowing SSH traffic (Port 22) from clients of trusted SSH.

On Managed Blockchain, Blockchain Network layer utilizes the AWS Hyperledger Fabric network so, for changing to Hyperledger Fabric network on Amazon Managed Blockchain it needs consensus between network members who make proposals. Amazon Managed Blockchain is a totally managed service that create and manage the blockchain networks besides their resources by using open-source frameworks. Blockchain permits building applications where several parties can run transactions transparently and securely as well as sharing data without the necessity for a trusted central authority.

For creating scalable blockchain resources and networks quickly, Managed Blockchain is used in addition to using AWS Management Console, AWS CLI, or the SDK of the Managed Blockchain efficiently. Managed Blockchain scales to meet various applications demands that is running millions of transactions. Also Managed Blockchain simplifies the managing blockchain networks and its resources after they are up and running. Additionally, it manages certificates, easily allows creating proposals for voting among network members, and helps tracking operational metrics associated with requests, data storage, memory usage, and computational load.

C. ARCHITECTURE AND CONFIGURATION PARAMETER

Fabric network involves various entities, ordering service nodes, peer nodes, and clients belong to other organizations. On the network, each one holds his own an identity, offered by a Membership Service Provider (MSP), that typically correlated with an organization. The whole network entities have visibility of all organizations' identities as well as the ability to verify them. The fabric consists of a variety of components such as endorsers, ordering services, and committers, which constitutes different steps in transaction processing, for instance, an endorsement, ordering, validation, and commit. As a result of components and stages variety, Fabric offers several configurable parameters for instance endorsement policy, channels, block size, as well as state database. Thus, one of the major challenges faced during setting up an effective blockchain network is finding the correct set of values used for these parameters.

D. MICROSERVICES IMPLEMENTATION

This section describes the microservices-based system that we implemented with smart contracts. To validate our approach's feasibility and simplicity, the method of this case study is composed of only three microservices. The exact implementation approach could be extended to more complex designs by adding more microservices. In this case study, we adopted a simple microservice-based application consisting of three microservices. The method comprises three microservices written in JavaScript: Doctor, Patient, and Diagnosis. The system's goal is to allow doctors to keep track of diagnoses for their patients' diseases. The microservices are accessed from the web user interfaces through an API-Gateway that routes the requests and forward the messages. Besides its simplicity, the system implemented includes several characteristics of accurate and more extensive procedures. It exposes APIs to connect to the graphical user interface, enables microservices to communicate, and stores the data in independent non-SQL databases.

E. SMART CONTRACT

In this subsection, A smart contract is designed for formulating an access control model. As well, an access protocol is created that presenting EHRs workflow sharing scheme. The smart contract was written in NodeJS programming language then deployed on AWS Lambda functions that work together with the cloud blockchain through the web3.js API. Interaction between users and smart contracts can be achieved through client that create an account to communicate with the blockchain network to gain access to data.

First, the data-sharing contract controlled by the admin is created for monitoring transaction operations within the blockchain network, where the user's public key is denoted as PK, the user's role is denoted asuserRole, and the patient's address is denoted as Addr. The following are five functions that are provided mainly by the contract.

1) AddUser(PK, userRole): function executed by Admin, used for adding a new user to the main contract. First the user is identified by his public key then added to the contract using a matching role based on his request, also the user information is stored on cloud storage that is considered as part of the data storage system.
2) DeleteUser(PK, userRole): function executed by Admin, used for removing users from the network based on the matching public key, also all personal information is deleted from cloud storage.
3) PolicyList(PK): function executed by Admin, where a peer of health provider-patient can agree on a policy expressing the relationship in medical services. For instance, a patient has a unique doctor for his health care, who is the only one that has the right for accessing his patient EHRs. The policy list encompasses the public key of all entities for identification once the smart contract processes new transactions.
4) RetrieveEHRs(PK, Addr): function executed by EHRs manager, allows retrieving medical records stored on cloud storage. A network participant provides the patient's address (including Patient ID and Area ID) to the smart contract, Then the contract verifies and sends a message to EHRs manager for extracting and returning data to the requester.
5) Penalty(PK, action): function executed by Admin, When an unauthorized request to the EHRs system isdetected, the EHRs manager inform the smart contract for issuing a penalty to the requester. In this paper, a warning message is also given as a penalty.

F. NETWORK GOVERNANCE TIER IMPLEMENTATION

On top of Amazon, Managed Blockchain Hyperledger Fabric encourages publishing peer node, chaincode, and Certificate Authority (CA) logs to Amazon CloudWatch Logs. These logs can be used for troubleshooting during chaincode development as well as monitoring network activity and errors.

Logs are enabled and viewed in the Managed Blockchain management console, CloudWatch Logs console, as well as AWS CLI commands for CloudWatch Logs. Additionally, metric filters are configured in CloudWatch Logs for turning log data into numerical CloudWatch metrics that can be graphed and the alarm is set on. For each member enabled with logging, Managed Blockchain creates a log group in CloudWatch Logs.

Peer node logs support debugging timeout errors coupled with proposals and detect the refused proposals that does not matched with the endorsement policies. They include messages used as soon as the client submits transaction proposals to peer nodes, requests to join channels, enrols an admin peer, and lists the chaincode instances on a peer node. Also, peer node logs include the chaincode installation outcomes with the facility of enabling and disabling logs on individual peer nodes.

Chaincode logs support analysing and debugging the business logic and execution of the chaincode on a peer node. They contain the results of chaincode instantiating, invoking, and querying. A peer can run many instances of chaincode, thus when chaincode logging is enabled, individual log streams are created on the peer for each chaincode.

CA logs support determining when an account member connects to the network or as new peers join with a member CA. It can be used for debugging problems concerned with certifications and enrolment. For each member CA logging can be enabled and disabled along with a separate log stream for each member.

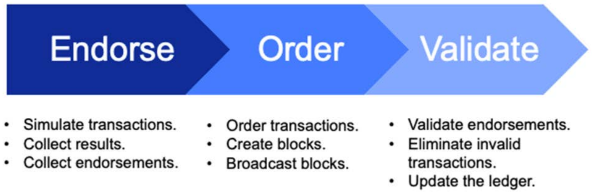

FIGURE 11. Hyperledger Fabric consensus implementation.

G. HYPERLEDGER FABRIC CONSENSUS IMPLEMENTATION

In Hyperledger Fabric, consensus involves the endorsement, Ordering, and Validation phases. The transaction flow is separated into three steps, which might be run on different system entities: As shown in Fig. 11, the first step is Endorsing a transaction: Run the transaction and check its correctness. This step corresponds to "transaction validation" in other blockchains. The second step is Ordering transactions through a consensus protocol: The ordering is done without regarding the transaction semantics. Finally, the third step is Validating transactions: Transactions are validated per application-specific trust assumptions. This step is also helpful in preventing race conditions due to concurrency.

The architecture employs an endorse-order-validate paradigm to distribute the execution of untrusted code in an untrusted environment. This design is different from the order-execute paradigm because Hyperledger Fabric runs transactions before reaching the final agreement on their order. It combines the passive and active approaches to replication.

H. HYPERLEDGER FABRIC TRANSACTION LIFECYCLE IMPLEMENTATION

This section goes through the process from submitting a transaction from a client app to creating a block on the chain and confirming consensus, as shown in Fig. 12. We see how privacy is achieved with only specific participants running

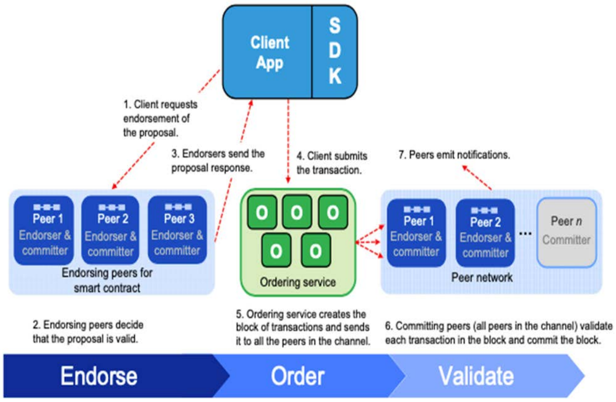
Client App
S D K
1. Client requests endorsement of the proposal.
3. Endorsers send the proposal response.
4. Client submits the transaction.
7. Peers emit notifications.
Peer 1 Endorser & committer
Peer 2 Endorser & committer
Peer 3 Endorser & committer
Endorsing peers for smart contract
O O O O O
Ordering service
Peer 1 Endorser & committer
Peer 2 Endorser & committer
...
Peer n Committer
Peer network
2. Endorsing peers decide that the proposal is valid.
5. Ordering service creates the block of transactions and sends it to all the peers in the channel.
6. Committing peers (all peers in the channel) validate each transaction in the block and commit the block.
Endorse
Order
Validate

FIGURE 12. Hyperledger Fabric transaction lifecycle implementation.

the marketing against the smart contract. Being in a private blockchain enables us to limit the compute power by using several endorsers to commit a transaction instead of the whole network solving a cryptographic puzzle.

For example, the clinician uses a mobile app to submit a request to process surgery for a patient. The clinician clicked the surgery request in the mobile app and submitted the proposal to book surgery.

The Transaction first (Endores) phase composed of three steps. Starting with the first step is an application submitting a transaction. The client (clinician) proposes a requestPatientSurgery for a patient transaction to the endorsing peers. The endorsement policy specifies that you need three endorsements from three different members (Supporters, Controllers, Providers) that specified by the endorsement policy. The second step before the actual execution is to identify the endorsement peer. Then, those peers will execute the chaincode for the proposed transaction independently. They run the transaction against the requestPatientSurgery smart contract, and they check all the rules defined by the smart contract. Finally, each peer calculates a set of outputs for the transaction. However, the peers do not update the ledger with the output of the executed transactions. The third step in the transaction flow is proposal response. All endorsement peers (legal professionals, health authorities, and hospitalpeers) sign the transaction, and R/W sets and respond to the client by sending this information.

Then the transaction second (Order) phase composed of two steps. the fourth and essential step in the transaction flow is the ordering step. The client submits the requestPatientSurgery transaction for ordering with R/W sets and signatures from the peers. The fifth step in the transaction flow is delivering the transaction itself. It starts with the requestPatientSurgery transaction is attached to a block and other transactions for specific channel. Then, the ordering service distributes the block to all the peers of the blue channel. Finally, the legal professionals, health authorities, and hospitalpeers receive the block, as do other peers on the channel (such as the insurer). After a block is distributed, each peer can distribute this block to other peers of the channel in a hierarchical way.

Finally, the transaction third (validate) phase that composed of last two steps. The sixth step in the transaction flow is the validation step. Where the requestPatientSurgery transaction is inspected for validation. If the block has the right R/W sets and signatures according to the endorsement policy and the current state of the ledger (based on the R/W set key history). committers flagged the transaction as valid and updated their world state based on the write set and surgery request. The final and seventh step in the transaction flow is the notification step where if the client registered to be notified when transactions succeed or fail, it is notified of the event.

VII. RESULT

Several research ideas have been suggested for applying blockchain to healthcare, as well as implementation are underway for attempt requests. Even now, few published studies have kept in consideration the needed software design for implementing healthcare applications based on blockchain effectively. This section evaluates the security dimensions of the system and the interoperability of the proposed healthcare framework. First, the security of a system is analyzed by studying its related properties such as data integrity, and non-repudiation of unauthorized access, after that, healthcare data interoperability is examined via theoretical analysis besides trials. Finally, Table 4 summarized the evaluation is presented through a comprehensive discussion.

A. DATA INTEGRITY

Taking part in integrity analysis, data can be categorized into; on-chain data and off-chain data. The immutability of the blockchain ensures on-chain data integrity while the off-chain data can be split up into directory and healthcare information. On the blockchain, the healthcare data integrity is validated with the digested data stored in it. Thus, because the data storage on the blockchain is tamper-proof, so in case that they pass the integrity check, then the users can trust the healthcare data.

Alternatively, the directory information could be tampered from malicious servers through an internal attack. But for two reasons it will not be a calamity. First, before storage all sensitive data is encrypted. Thus, tampering directory information will not be leaked. Probably, as a result of ID corruption or decryption malfunction caused by content corruption will led to data not found, and later users will be informed of it. Second, once data corruption happens, the patient or the healthcare provider can recover the directory information quickly, where the patient can rebuild the corrupted session using the data on their device, while the healthcare provider can rebuild a data inventory on the local legacy system.

B. NON-REPUDIATION OF UNAUTHORIZED DATA ACCESS

In one case, patient data may retrieve and abuse by an adversary without authorization. The block digest and the

TABLE 4. Comparison between PCH framework and its related works.

Metric	Jamil et al. [19]	Musamih et al. [23]	Rajput et al. [24]	P.Zhang et al. [26]	Antonio et al. [28]	A.Azaria et al. [29]	PCH
Access Control	5	1	5	1	3	5	5
Access Revocation	5	1	5	1	1	5	5
Privacy-Preserving	5	3	1	1	1	5	5
Patients Control Access	5	1	1	3	3	1	5
Different user types	5	1	1	3	3	1	5
Block Search	1	1	1	1	5	1	5
Architecture	3	3	1	5	3	1	5
Implementation	5	1	3	5	1	3	5
Interoperability	1	1	1	3	1	1	5
SCORE (45)	**35**	**13**	**19**	**23**	**21**	**23**	**45**

blockchain immutability property can provide evidence for a session that authorize data access for the adversary, does not exist, proving the behavior illegality. Also, an adversary may gain access to the data out of the approved access range and in another case deny it. Also, the blockchain immutability property can offer evidence for the degree of data sharing, proving that the data access is out of the range.

C. INTEROPERABILITY

Any technology that can securely solve the interoperability problem has the potential to become a game-changer. This is the potential of Blockchain technology. Not surprisingly, it generates an inordinate amount of interest in the industry. While organizations like Health Level Seven International (HL7) continue to provide standards for data exchange like Fast Healthcare Interoperability Resources (FHIR), blockchain could provide the right interventions.

VIII. DISCUSSION

Without compromising scalability, privacy, and security, the proposed framework reveals higher interoperability than the current designs of the communication and storage overhead discussed earlier. Moreover, an additional advantage is flexibility. Differentiating the mutable healthcare data from immutable one enables healthcare providers update the description with minimal overhead.

In order to qualify the comparison between the proposed framework and the other frameworks, a grading method was uses based on the 1,3,5 rating matrix. Also, to simplify the comparison, the same rated metrics are removed like tamper-proof, non-repudiation, and attack resistance. Moreover, the data format and blockchain platform also neglected from the ranking metrics as those are alternatives that each have its procs and cons.

Generally, the not satisfied metric scored 1, partially satisfied metric scored 3, and finally fully Satisfied metric scored 5. However, for the Interoperability metric the score will be as the following foundational interoperability will be rated as 1, structural interoperability will be rated as 3 and finally semantic interoperability will be rated as 5.

In summary, Table 5 compares the proposed PCH framework with other solutions. This comparison illustrates the advantage gained from the proposed scheme in different aspects, mainly the detailed design and architecture alongside with deep dive into the implementation strategy and challenge.

Table 5 summarizes healthcare data management mechanisms in blockchain technology from 2018 till now. Much research work was developed to design blockchain technology to secure, share, and store EHR data within and across institutions.

Only two out of ten frameworks based on Ethereum based consortium Blockchain they were developed by Musamih *et al.* [23], Nguyen *et al.* [25]; on the other hand the remaining eight frameworks were developed using Hyperledger frameworks. Dubovitskaya *et al.* [16], and Liang *et al.* [17] developed a generic Hyperledger proposal. However, Li *et al.* [18], Yang *et al.* [20], Tanwar *et al.* [22] developed Hyperledger Fabric Framework. On the other hand, the remaining frameworks developencryption, and digitaled by Jamil *et al.* [19], Sharma and Balamurugan [21], Rajput *et al.* [24] are based on the combination of Hyperledger Fabric and Hyperledger Composer.

Dubovitskaya *et al.* [16], and Nguyen *et al.* [25] get the maximum benefit of cloud adoption. On the other hand, Jamil *et al.* [19] integrate and amalgamate the IoT devices in the same framework which has its own pros and cons as discussed before.

A. SECURITY ANALYSIS FOR THE PROPOSED FRAMEWORK

PCH offers the necessary security analysis to demonstrate that the proposed framework with adopted components and the fundamental protocols has excellent security and privacy protection advantages for users in decentralized and collaborative data management. According to the security standards, some important security and privacy requirements are satisfied in our proposed framework. We summarize the significant advantages of the proposed framework in the following aspects.

1) CONFIDENTIALITY

Confidentiality of communications is protected by exploiting the standard cryptographic primitives. PCH utilize Signcryption and asymmetric key-based encryption, and digital

TABLE 5. Comparison between PCH and the existing Blockchain-based healthcare frameworks.

#	Author	Focus Area	Framework	Storage	Contribution	Remarks
1	Dubovitskaya et al. [16]	Sharing Health Information	Hyperledger	off-chain	Using Blockchain framework for business. Cloud environment.	Critical data is saved off-chain which empire the security. Very shallow proposal (idea only). Missed implementation derails for reference.
2	Liang et al. [17]	Remote care with IoT.	Hyperledger	on-chain	Have evaluation criteria. Implement the channel concept.	Missed implementation derails for reference.
3	Li et al. [18]	The supply chain for healthcare	Hyperledger Fabric	on-chain	Integrate with standard healthcare applications. Primitive definition for the healthcare entities.	Design using Hyperledger Composer while implementing done using Hyperledger Fabric. Require standard healthcare framework to integrate with.
4	Jamil et al. [19]	Remote care with IoT.	Hyperledger Fabric/ Composer	on-chain	Amalgamating the Internet of Things (IoT), Machine Learning, and Blockchain.	Shallow proposal.
5	J. Yang et al. [20]	Security and privacy	Hyperledger Fabric	on-chain	Data privacy and security issues in electronic healthcare.	Idea and implementation need more details by implementing various smart contracts to handle the advanced functionality of the EHR system.
6	Sharma et al. [21]	Security and privacy.	Hyperledger Fabric/ Compose	on -chain	Real implementation, the balance between data privacy and data accessibility.	Implementations need a further extension by implementing various smart contracts to handle the advanced functionality of the EHR system.
7	Tanwar et al. [22]	Security and privacy.	Hyperledger fabric	on-chain	Performance evaluation of the proposed system is completed using the caliper	Make the framework interactive by integrating it with a web application.
8	Musamih et al. [23]	Supply chain for healthcare.	Ethereum	off-chain	System architecture and detailed algorithms. performed testing and validation. the proposed solution is cost-efficient.	Framework itself needs more elaboration from a design and architecture perspective.
9	Rajput et al. [24]	Sharing Health Information	Hyperledger Fabric/ Hyperledger Composer	off-chain	Personal health record (PHR) data privacy	Needs more testing standard like HL7 FHIR is required to guarantee the data sharing implementation security
10	Nguyen et al. [25]	Sharing Health Information	Ethereum	off-chain	Edge-cloud computing and Ethereum blockchain. Smart contracts operation cost is low, and system security is assured.	Implementation viewpoints need to be addressed in a more detailed manner.
11	Gohar et al.	Sharing Health Information	Hyperledger Fabric	on/off-chain	Interoperability, privacy.	

signatures in our schemes. Without any entities' asymmetric keys and private keys, any potential adversaries cannot open the encrypted packets even though they may realize the existence of boxes and steal them by eavesdropping on wireless communications and illegal packet capture. We use a timestamp in all the packages during the contacts to effectively prevent replay attacks.

2) INTEGRITY AND AUTHENTICATION

In the EMR management scheme, after treatment, a doctor must sign the diagnosis record. The diagnosis record with the digital signature is sent to a patient. The patient confirms the diagnosis record and further signs it by verifying the digital signature. Thus, the diagnosis record with a dual signature is finally generated to reach a consensus. Here, without the signer's private key, any entity cannot counterfeit the digital signature of other entities. Since a specific signer only generates the digital signature, any information with a digital signature can be authenticated and verified whether the signer is the sender or not. If unauthorized parties or random errors modify one EMR during the transmission, the receivers can also discover it in verification, guaranteeing integrity and authentication.

3) TRACEABILITY

Due to the proposed dual signature, non-repudiation of designed communication protocols is ensured. In case of a round of packet transmission and receipt, neither the sender nor the receiver can deny taking part in the communication. This means that the communication protocols can avoid one of the implied entities (i.e., sender and receiver) cheating and being cheated.

4) USER-CENTRIC ACCESS CONTROL

When a doctor wants to access a patient's healthcare data, the doctor should ask permission. Otherwise, the system will prevent access caused by the doctor. Similarly, when the doctor hopes to acquire a regular access privilege from the patient, the doctor should also directly ask whether it can be granted. In short, for the patient, all the data access regarding his healthcare data should be firstly authorized by him. Moreover, the patient can independently permit temporary access and assign/revoke any access privileges for/from others in the system.

B. INTEROPERABILITY

The shift towards patient-centered interoperability brings numerous challenges around patient consent, governance, security, privacy, and patient engagement. Blockchain technology is an attractive method of addressing these challenges by creating a platform for the secure exchange of data. In essence, blockchain provides a high-level framework for how a patient could securely interact with multiple stakeholders, identify themselves across each entity, and aggregate their health data in a persistent form.

C. SCALABILITY

From the patient perspective, scalability is a common concern for the whole patient-centric solutions as patients must provide a reply for each data-sharing request in addition to adding into a session the requested data for authorizing access. This is a trade-off between patient controllability and overhead. Thus, for reducing further overhead a more elegant solution could be built by creating an attribute-based data sharing along with medical history-based data sharing, complementing the session-based scheme. Attribute-based data sharing allows patients to share their healthcare data tagged with attributes with a group of requesters, e.g., biomedical laboratories and physician. Medical history-based data sharing enables patients to gain access to all their medical data correlated to a specific disease/symptom.

IX. CONCLUSION AND FUTURE WORK

A Patient-Centric Healthcare Framework called PCH is proposed for improving patients' control over their healthcare data as well as reducing information fragmentation. The proposed framework shows higher efficiency in data interoperability with no security compromise across a proposed architecture than the existing blockchain-based approaches. However, till now finding a solution study for comprehensive EHRs sharing along with data interoperability is lacking.

This study seeks to fill up the gap considering sharing issues for EHRs along with the access control on data usage in the e-health blockchain. The major variations between this study and the current EHRs sharing schemes can be emphasized in the following points.

1) In this study, a comprehensive integrated data sharing architecture by means of blockchain, cloud, and IoT is built for better interoperability.
2) A PCH framework is proposed by leveraging Blockchain technology to protect the health data sources, particularly by implementing a smart contract design on top of Hyperledger blockchain platform on Amazon cloud, aiming at exploiting the access control capability of smart contract and blockchain for managing the required healthcare business and ensuring integrity of the system.
3) Instead of theoretical analysis shown in contemporary studies, this study focuses on detailed architectural design and actual implementation of data sharing design using Blockchain, Cloud, as well as IoT in the healthcare systems. Thus based on implementation outcomes several useful technical blockchain features are identified for EHRs sharing, resulting in significant contributions to blockchain research in multiple domains such as IoT applications, Cloud including healthcare.
4) A comprehensive evaluation of the proposed framework regarding various aspects is provided like security aspects (attack resistance, access control, access revocation, privacy-preserving, patients control EHR access, different user types), also data integrity aspects (Block Search, data format, Interoperability), and finally technical aspects (used Blockchain platform, detailed architecture, detailed implementation)

The work results are significant as efficiency, and interoperability level is considered as one of the important issues faced during the adoption of healthcare blockchain. PCH provides the comprehensive platform from an enterprise architecture viewpoint that would be implemented as a government scope of at least a mega healthcare provider chain/group. The framework provides the integration fixability to integrate with the currently existing system, either its data stored in healthcare standard format like HL7 or customized non-standard design. The transformation component plays an important role. Moreover, it provides a template for holding the healthcare information in a standard format that facilitates the interoperability between the data from different systems and the pluggable reporting engine and analytical services.

As a result, once a provider has obtained access to patient data, that data is permanently in possession of the provider. When a patient visits different providers many times throughout their lifetime, their health and other sensitive personal information are available at several sites based on the granted permission. Also, patients may wish to release their medical records to a new provider, which was not easily accomplished and became available today using PCH.

As the proposed framework is at the prototype stage, it should be tested by engaging different groups of participants and then considering their feedback during the maintenance stage. Furthermore, as the PCHs are exchanged/shared among different participants, HL7 FHIR is one of the standards needed to be adopted by newly developed healthcare systems to ensure the security, and consistency of data sharing implementation for better interoperability.

REFERENCES

[1] T. K. Mackey, T.-T. Kuo, B. Gummadi, K. A. Clauson, G. Church, D. Grishin, K. Obbad, R. Barkovich, and M. Palombini, ''Fit-for-purpose?'—Challenges and opportunities for applications of blockchain technology in the future of healthcare,'' *BMC Med.*, vol. 17, no. 1, pp. 1–17, Dec. 2019, doi: 10.1186/s12916-019-1296-7.

[2] K. Rabah, ''Challenges & opportunities for blockchain powered healthcare systems: A review,'' *Mara Res. J. Med. Heal. Sci.*, vol. 1, no. 1, pp. 45–52, 2017. [Online]. Available: http://www.mrjournals.org/

[3] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, ''Data sharing and privacy for patient IoT devices using blockchain,'' *Commun. Comput. Inf. Sci.*, vol. 1122, pp. 334–348, Oct. 2019, doi: 10.1007/978-981-15-1301-5_27.

[4] S. Schindler, S. Pfattheicher, and M.-A. Reinhard, ''Potential negative consequences of mindfulness in the moral domain,'' *Eur. J. Social Psychol.*, vol. 49, no. 5, pp. 1055–1069, Aug. 2019, doi: 10.1002/ejsp.2570.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ''An overview of blockchain technology: Architecture, consensus, and future trends,'' in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[6] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, ''Blockchain for healthcare data management: Opportunities, challenges, and future recommendations,'' *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022, doi: 10.1007/s00521-020-05519-w.

[7] S. Gaikwad, N. Kirad, S. Gayake, and D. P. Kulkarni, ''Electronic health record: Blockchain technology,'' *ASIAN J. Converg. Technol.*, vol. 5, no. 1, pp. 1–4, Apr. 2019, doi: 10.33130/ajct.2019v05i01.002.

[8] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, ''Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,'' *Cryptography*, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/cryptography3010003.

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, ''Blockchain with Internet of Things: Benefits, challenges, and future directions,'' *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, 2018, doi: 10.5815/ijisa.2018.06.05.

[10] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ''A survey on the security of blockchain systems,'' *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2017, doi: 10.1016/j.future.2017.08.020.

[11] A. P. Joshi, M. Han, and Y. Wang, ''A survey on security and privacy issues of blockchain technology,'' *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, May 2018, doi: 10.3934/mfc.2018007.

[12] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, ''Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,'' *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018, doi: 10.1016/j.scs.2018.02.014.

[13] X. Li, X. Huang, C. Li, R. Yu, and L. Shu, ''EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems,'' *IEEE Access*, vol. 7, pp. 22011–22025, 2019, doi: 10.1109/ACCESS.2019.2898265.

[14] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, ''The benefits and threats of blockchain technology in healthcare: A scoping review,'' *Int. J. Med. Informat.*, vol. 142, Oct. 2020, Art. no. 104246, doi: 10.1016/j.ijmedinf.2020.104246.

[15] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, ''Health-CPS: Healthcare cyber-physical system assisted by cloud and big data,'' *IEEE Syst. J.*, vol. 11, no. 1, pp. 88–95, Mar. 2017, doi: 10.1109/JSYST.2015.2460747.

[16] A. Dubovitskaya, Z. Xu, S. Ryu, M. I. Schumacher, and F. Wang, ''How blockchain could empower eHealth: An application for radiation oncology,'' in *Proc. VLDB Workshop Data Manage. Anal. Med. Healthcare*, Sep. 2017, pp. 3–6, doi: 10.1007/978-3-319-67186-4.

[17] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ''Integrating blockchain for data sharing and collaboration in mobile healthcare applications,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2018, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[18] P. Li, S. D. Nelson, B. A. Malin, and Y. Chen, ''DMMS: A decentralized blockchain ledger for the management of medication histories,'' *Blockchain Healthcare Today*, vol. 2, pp. 1–15, Jan. 2018, doi: 10.30953/bhty.v2.38.

[19] F. Jamil, L. Hang, K. Kim, and D. Kim, ''A novel medical blockchain model for drug supply chain integrity management in a smart hospital,'' *Electronics*, vol. 8, no. 5, pp. 1–32, 2019, doi: 10.3390/electronics8050505.

[20] J. Yang, M. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, ''Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making,'' *Appl. Sci.*, vol. 9, no. 7, p. 1370, Apr. 2019, doi: 10.3390/app9071370.

[21] Y. Sharma and B. Balamurugan, ''Preserving the privacy of electronic health records using blockchain,'' *Proc. Comput. Sci.*, vol. 173, pp. 171–180, Jan. 2020, doi: 10.1016/j.procs.2020.06.021.

[22] S. Tanwar, K. Parekh, and R. Evans, ''Blockchain-based electronic healthcare record system for healthcare 4.0 applications,'' *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407, doi: 10.1016/j.jisa.2019.102407.

[23] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, ''A blockchain-based approach for drug traceability in healthcare supply chain,'' *IEEE Access*, vol. 9, pp. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[24] A. R. Rajput, Q. Li, and M. T. Ahvanooey, ''A blockchain-based secret-data sharing framework for personal health records in emergency condition,'' *Healthcare*, vol. 9, no. 2, p. 206, Feb. 2021, doi: 10.3390/healthcare9020206.

[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ''A cooperative architecture of data offloading and sharing for smart healthcare with blockchain,'' 2021, *arXiv:2103.10186*.

[26] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, ''Design of blockchain-based apps using familiar software patterns with a healthcare focus,'' in *Proc. 24th Conf. Pattern Lang. Programs*, 2017, pp. 1–14.

[27] E. Chukwu and L. Garg, ''A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations,'' *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[28] A. Fusco, G. Dicuonzo, V. Dell'atti, and M. Tatullo, ''Blockchain in healthcare: Insights on COVID-19,'' *Int. J. Environ. Res. Public Health*, vol. 17, no. 19, pp. 1–12, 2020, doi: 10.3390/ijerph17197167.

[29] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ''MedRec: Using blockchain for medical data access and permission management,'' in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[30] P. Thakkar, S. Nathan, and B. Viswanathan, ''Performance benchmarking and optimizing hyperledger fabric blockchain platform,'' in *Proc. IEEE 26th Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst. (MASCOTS)*, Sep. 2018, pp. 264–276, doi: 10.1109/MASCOTS.2018.00034.

[31] K. Rabah, ''Convergence of AI, IoT, big data and blockchain: A review,'' *Lake Inst. J.*, vol. 1, no. 1, pp. 1–18, 2018. [Online]. Available: http://www.thelakeinstitute.org

[32] R. Urwongse and K. Culver, ''Applications of blockchain in healthcare,'' in *Patient-Centered Digital Healthcare Technology: Novel Applications for Next Generation Healthcare Systems*, Dec. 2021. [Online]. Available: https://digital-library.theiet.org/content/books/10.1049/pbhe017e_ch10, doi: 10.1049/pbhe017e_ch10.

[33] C. Lapointe and L. Fishbane, ''The blockchain ethical design framework,'' *Innov., Technol., Governance, Globalization*, vol. 12, nos. 3–4, pp. 50–71, Jan. 2019, doi: 10.1162/inov_a_00275.

[34] E. Androulaki *et al.*, ''Hyperledger fabric: A distributed operating system for permissioned blockchains,'' in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[35] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, ''Blockchain technology in healthcare: A systematic review,'' *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019, doi: 10.3390/healthcare7020056.

[36] G. Carter, D. White, A. Nalla, H. Shahriar, and S. Sneha, ''Toward application of blockchain for improved health records management and patient care,'' *Blockchain Healthcare Today*, vol. 2, pp. 1–12, Jun. 2019, doi: 10.30953/bhty.v2.37.

[37] *Hyperledger Fabric*, Readthedocs, 2021.

[38] B. Zhong, H. Wu, L. Ding, H. Luo, Y. Luo, and X. Pan, ''Hyperledger fabric-based consortium blockchain for construction quality information management,'' *Frontiers Eng. Manage.*, vol. 7, no. 4, pp. 512–527, Dec. 2020, doi: 10.1007/s42524-020-0128-y.

[39] (2021). *What is Blockchain?*. [Online]. Available: https://www.ibm.com/eg-en/blockchain/what-is-blockchain

[40] J. Al-Jaroodi and N. Mohamed, ''Blockchain in industries: A survey,'' *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[41] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, ''Blockchain's adoption in IoT: The challenges, and a way forward,'' *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019, doi: 10.1016/j.jnca.2018.10.019.

[42] O. Choudhury, N. Fairoza, I. Sylla, and A. Das, ''A blockchain framework for managing and monitoring data in multi-site clinical trials,'' 2019, *arXiv:1902.03975*.

[43] Hyperledger. (2016). *Hyperledger Project*. [Online]. Available: https://www.hyperledger.org/

[44] A. Gohar, S. AbdelGaber, and M. Salah, "A proposed patient-centric healthcare framework for better Semantic interoperability using blockchain," *Int. J. Comput. Sci. Inf. Secur.*, vol. 19, no. 11, pp. 26–35, 2021.

[45] N. Tissir, S. E. Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal," *J. Reliable Intell. Environ.*, vol. 7, no. 2, pp. 69–84, Jun. 2021, doi: 10.1007/s40860-020-00115-0.

AHMAD N. GOHAR (Senior Member, IEEE) was born in Qena, Egypt, in 1983. He received the M.S. degree in information systems from the Faculty of Computer and Artificial Science, in 2014, and the M.I.B.A. degree in global business management from ESLSCA University, France, in 2014.

He worked in multiple software companies, from 2007 to 2009, he was a Software Developer at ResalaSoft. From 2009 to 2011, he was a Senior Software Developer at United Nation. From 2012 to 2015, he was a Project Lead at eFinance. Since 2012, he has been working with the Client Innovation Centre, IBM, as a Senior Solution Architect and also leading the Technical Specialist Profession of MEA. He represents IBM in several events like Egyptian Engineering Day EED18, Judging competitions, and IBM innovation days. He is recognized as a public speaker in several conferences like JavaOne, Devoxx, Oracle CodeOne, Code Monsters, Java2Days, and Global Technology Summit. He has authored three courses and one disclosure in the blockchain field.

Mr. Gohar is a member of IBM Academy of Technology, a Java Community Process (JCP) Member, a Professional Member of British Computer Society, and a member of Association of Enterprise Architects.

SAYED ABDELGABER ABDELMAWGOUD received the Ph.D. degree in information systems. He is currently a Professor of information systems and the Vice Dean of postgraduates and research with the Faculty of Computers and Artificial Intelligence, Helwan University. He is also the Digital Transformation Manager of Helwan University. His research interests include data science, medical informatics, and software engineering.

MARWA SALAH FARHAN received the Ph.D. degree in information systems from the Faculty of Artificial Intelligent, Helwan University. She is currently an Associate Professor with the Department of Information Systems, Faculty of Informatics and Computer Science, The British University in Egypt. Her research interests include big data and data analytics, the IoT data analytics, advanced database management, and software engineering.