BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
ORIGINAL RESEARCH

Hyperledger Fabric-Powered Digital Identity Scheme: Transforming CIA—Triad Security in IoMT Integrated Healthcare Eco-System

Sanjay Jena, PhD Scholar[1]; Ram Chandra Barik, PhD[2] and Saroj Padhan, PhD[3]

[1]Department of Computer Science and Engineering, C.V. Raman Global University, Odisha, India; [2]Associate Professor, Department of Computer Science and Engineering, C.V. Raman Global University, Odisha, India; [3]Associate Professor, Department of Electrical Engineering, Parala Maharaja Engineering College, Odisha, India

Corresponding Author: Sanjay Jena: sanjayjena51@gmail.com

DOI: https://doi.org/10.30953/bhty.v8.411

Keywords: Availability, biomedical, blockchain, confidentiality, healthcare, integrity

Abstract

This study underscores blockchain technology's potential to tackle critical healthcare challenges, including data security, interoperability, and collaboration, delivering a scalable and efficient framework that enhances patient trust, operational efficiency, and compliance with global data protection standards. The advent of blockchain technology has radically altered centralized data management to adopt decentralized distributed systems with their inherent features—such as transparency, immutability, and security—that offer a promising answer for the challenges faced by modern healthcare systems. The authors introduce a smart healthcare solution for a secured digital identity of a patient by maintaining its Confidentiality, Integrity, and Availability (CIA-triad). It customizes an open-source Hyperledger Fabric-based framework for developing and utilizing the healthcare ecosystem as per the requirements of maintaining the digital identity of a patient. In addition, it uses fabrics' key components, such as privacy-preserving channels, endorsing peers, anchor peers, orderer nodes, and a secure consensus for an efficient collaboration among stakeholders that ensures data integrity and confidentiality. The decentralized storage feature allows secure Secure Hash Algorithm 256-bit (256-bit) during digital signature generation and verification algorithms across the network, and its one-way cryptographic function feature adds an advantage to maintain digital identity encryption both on-chain and off-chain during sharing and storing. This acts as a resistance to different cyberattacks as a record of the Common Vulnerability Scoring System scorecard. The efficiency of the proposed operational model tested in a closed experimental network gets a more balanced output than that of a test network, which may be chosen for an adoption.

Plain Language Summary

Modern healthcare systems are widely dependent on sensors to monitor patients, collect vital data, and share information between hospitals, doctors, and insurance providers. With this modern approach it has become more efficient for seamless movement of patients as well as their data; however, it raises concerns about privacy, data security, and trust. To address these challenges, a Secured Digital Identity system can be used. Every patient, doctor, and device get a unique digital ID, ensuring that only authorized users can access sensitive health data. This approach relies on the CIA principles: confidentiality—only authorized entities can read patient data; integrity—the data cannot be altered without detection. Availability—data are accessible when needed. By integrating blockchain technology through Hyperledger, healthcare systems can store records in a decentralized and tamper-proof ledger. This ensures that every transaction, such as a medical report update or an insurance claim, is securely recorded and verifiable.

Submitted: June 6, 2025; Accepted: August 26, 2025; Published: September 3, 2025

The transformation of traditional healthcare management to a smart ecosystem demands a secure and reliable framework for managing sensitive patient information. Blockchain technology, with its decentralized framework Hyperledger Fabric, offers this opportunity for establishing an authenticated and controlled data exchange among the stakeholders.[1] It also embeds with it the core principles of Confidentiality, Integrity, and Availability (CIA triad).

Confidentiality is preserved through its cryptographic access controls, private data channels, and encrypted storage mechanisms. Integrity is safeguarded by the feature of immutability and consensus-driven transaction validation. Availability is achieved through its distributed architecture that ensures continuous service without any network failure. At the heart of this transformation lie Internet of Medical Things (IoMT) devices that collect, monitor, and transmit this sensitive information and are uniquely authenticated and authorized.[2,3] This integration of blockchain technology with IoMT devices enhances a security system and develops a responsive healthcare ecosystem where patient trust is intrinsic to digital transformation.[4]

Although blockchain applications in healthcare have been explored extensively, most approaches concentrate on developing only a test network from the fabric framework that limits peer nodes and would focus solely on electronic health records (EHR) or Internet of Medical Things (IOMT) separately.

This research combines digital identity management with permissioned blockchain to protect continuous IoMT data streams while fully integrating the principles of the Confidentiality, Integrity, and Availability (CIA triad). The absence of an integrated, scalable, and real-time framework of IoMT in blockchain-enabled smart hospitals represents a critical gap that has been found for study.

To address this gap, this study is guided by three research questions: 1) How can Hyperledger Fabric be used to develop a smart hospital network while managing digital identities of patients? 2) What blockchain-enabled strategies will ensure confidentiality, integrity, and availability for real-time IoMT data exchange by complying with healthcare security regulations? 3) What architectural framework can integrate blockchain, digital identity, IoMT, and the CIA triad into a scalable and interoperable smart hospital model?

The structure of this article is outlined as follows: Aan extensive literature review of twenty-three selected articles. Detailing of the technical and procedural methodology, incorporating various diagrams, flowcharts, equations, and code screenshots to illustrate the proposed model. Examination of the challenges and results, supported by cited references to validate the model's credibility. Finally, there is a summary of findings and key takeaways.

System Under Study

What follows is a summary of the sources used in a descriptive format as well as in tabulated form for the readers, making the section easier to comprehend. The survey starts with the benefits of digital identification in the rapidly modernizing healthcare industry; it reveals that there are numerous online articles, journals, and conferences available. Out of those, some sixteen articles have been selected for this literature review. Yousef and colleagues[5] integrate IoMT and blockchain for secure, tamper-proof, and traceable healthcare applications.

An online post[6] by Siddharth Gandhi presents a three-point rationale, the first of which is regarding exclusive ownership of the patient's healthcare data. Whereas the availability of a clear image of the patient's healthcare is discussed in the second point, and error-free treatment and safety in healthcare are referred to in the third point.

The deployment of digital identification will result in the demise of the current username and password system. Natarajan and colleagues[7] demonstrate how decentralization enhances traceability, security, and transparency, which are critical in medical logistics. Internet of Things (IoT) technology may help with these tasks, as is detailed in the aforementioned review paper.[8] With the installation of IoT sensors, also known as body sensing devices, in the patients, the system would function as a Save Our Souls (SOS) signal in the event of an emergency.[9]

It is also feasible to diagnose patients remotely, which is a benefit for isolated rural locations. Whether it was monitoring temperature or wheelchair management, monitoring asthma, or monitoring glucose levels, everything was recorded and saved in the fabric chain to simplify treatment that could be simplified.[10] This was done to make it easier to provide care. Implementation of IoT, which uses a lot of body-sensing devices, can be the solution to physical visits and save time, with a simultaneous advantage for the doctor to attend to more patients at the same time.[11] The current healthcare system continues to use the conventional mode of physically visiting a doctor and diagnosing the diseases before any treatment procedure starts, and when it comes to some critical situations, the patient needs to visit the doctor regularly.[12,13]

Agbo and Mahmoud[15,16] provided a table that summarizes the key differences between the various blockchain frameworks. As a result, Hyperledger is superior to all competing frameworks in terms of performance, scalability, latency, and security. The results of the comparison show that fabric can significantly impact any industry that chooses to embrace it because the framework's contents are freely accessible on GitHub. To fully realize the technology's potential, the Linux Foundation had, of course,

Citation: Blockchain in Healthcare Today 2025, 8: 411 - https://doi.org/10.30953/bhty.v8.411

released the code as open source. The open-source code facility of Hyperledger provides several benefits.

First, the openness facility of Hyperledger Fabric refers to its open-source nature that provides accessibility, flexibility, and community-driven development. The developers can view, modify, and contribute to the Hyperledger Fabric's full source code on GitHub, which lets them participate in a transparent development process with community development for their specific enterprise needs.[17]

Next, related to cooperation and creativity, Hyperledger Fabric, as an open-source enterprise blockchain framework, fosters cooperation and creativity through its community-driven development, modular design, and open collaboration. These facilities allow developers, academics, and businesses to all benefit from working together, thanks to open source. Individuals are invited to introduce changes to the project or suggest improvements.[18]

Regarding personalization and flexibility, Hyperledger Fabric is designed to provide high levels of personalization and flexibility, making it an ideal enterprise blockchain solution. Unlike rigid, public blockchains, Hyperledger Fabric allows organizations to customize their networks, consensus mechanisms, and smart contracts to fit their unique business needs. The open-source nature makes it easy for businesses to customize it to their requirements. They are adaptable and can introduce changes to the code, implement new features, and combine them with other systems.[19]

Next, lessened vendor involvement is one of the key advantages of Hyperledger Fabric, and organizations can pick service providers or create their expertise, reducing vendor lock-in and providing greater support, customization, and deployment alternatives.[20]

This facility guarantees data integrity, privacy, security, and trustworthiness for businesses. Its robust security controls, consensus mechanisms, identity management, and regulatory compliance features are the trusted solutions to develop a system with a secured network architecture. The broad use of peer review of the code enhances the likelihood that any potential security flaws will be found and fixed promptly.[21]

Finally, to permit affordability, the high licensing costs that are often associated with proprietary software solutions are not required when using open-source software. As a result of being able to exploit the open-source code of Hyperledger Fabric without having to spend major up-front fees, businesses will be able to manage their resources more effectively.[22]

Now, after covering digital identity and the application of the IoT in the healthcare sector, the next consideration is to move on to healthcare data management utilizing an immutable decentralized database system, which is something that can only be made feasible by a blockchain platform built on top of the Hyperledger architecture.[23,24,25] As a result, several publications have been discovered that could explain the aforementioned aspects. Concerned about maintaining patients' confidentiality while maintaining the integrity of their medical data, several nations have begun to implement electronic healthcare systems. The decentralized technology offers a mechanism for storing and distributing e-health data remotely, making it useful for remote healthcare.[26]

The articles reviewed here were chosen because they discussed different ways of looking at perspectives. A comprehensive evaluation of the references used in this section is presented in Table 1 for clarity and a better understanding of their relevance and credibility.

Technical and Procedural Approach

Procedural Design

The article presents a new idea of application to blockchain technology cascading with the Hyperledger Fabric project of the Linux Foundation for developing a production network in the field of healthcare. The pieces of the architecture are used to describe the making model's fundamental transaction process. The concise diagram in Figure 1 describes the hierarchical model of different nodes in the architecture, where it provides an in-depth idea to the reader's mind via distributed technology so that it can be adopted by any real-world place to get upgraded and establish a secure milieu by the CIA plan that would eliminate current challenges experienced by the organizations and the users (patients). This will be an overall network configuration that is described in the article. Moving forward in the section, it goes much deeper into the model, with several more figures to put a clear picture in the minds of the readers. The network contains the setting up of Certificate Authorities (CAs) and Membership Service Providers (MSPs), roles of Ordering Nodes, Endorsing Peers, Anchor Peers, Committing Peers.

By setting up the contents of the network, it is possible to establish a decentralized network using the Hyperledger Fabric, which consists of several nodes that can interact with one another. The blockchain stores the chaincode, the ledger data, and the transactions that are executed over it. In addition to this, it will manage the identities by using MSPs. Identity and membership, which enable permission and access control for many kinds of activities, are the most important components for making use of the fabric.

The members of a network may be identified from inside the network by their distinct digital fingerprints, which are known as their identities. These kinds of identities may be preserved using Hyperledger via the use of certificates, which can include digital certificates in the X.509 standard, which is very similar to a secure

Table 1. Comprehensive description of the references used in this literature review.

Journal/year/reference/publisher	Methodology used in article	Comments
Results in Engineering, 2025[5], Elsevier	GM-SSO is integrated to enhance authentication security in a lightweight encryption of data protection.	Decentralized storage strengthens privacy preservation, optimizing healthcare blockchain applications for scalability and reliability.
ET HealthWorld. 2023[6], The Economic Times	Highlighted the value of digital identities in healthcare	Future healthcare will rely heavily on digital identification verification.
Results in Engineering. 2025[7], Elsevier	Ethereum blockchain and smart contracts enhance security, traceability, and decentralization in cord blood procurement, improving transparency, efficiency, and accountability in healthcare supply chains.	It presents an innovative approach to transforming cord blood procurement in healthcare supply chains using Ethereum blockchain and smart contracts.
Journal of Healthcare Engineering. 2021[7], Hindawi	Various healthcare IoT devices with their architecture have been discussed.	Several challenges and limitations like standardization, power consumption, self-configuration, data privacy, and the security and environmental impact of HIoT devices, need to be addressed.
Journal of Clinical Orthopedics and Trauma. 2020[10], Elsevier	Orthopedic patients in pandemics benefit from IoMT.	Security and interoperability are key issues, and orthopedic IoMT requires deeper research.
IEEE Access. 2020,[11] IEEE	BAKMP-IoMT was tested using the popular AVISPA program to show its resistance to various assaults.	Decentralization helps protect IoMT communication from different threats.
Journal of Information Security and Applications. 2020,[12] Elsevier	The author tested the system's performance and settings using Hyperledger Caliper.	Blockchain technology improves health record management.
IEEE Access. 2020,[13] IEEE	Aims to check blockchain technology's applicability in patient data and identity management with EHR and PHR implementations.	Distributed ledger technology is a potential solution for patient data management and self-sovereignty.
Internet Technology Letters. 2019,[14] Wiley	Compared Bitcoin, Ethereum, and Hyperledger Fabric for healthcare.	Hyperledger Fabric has greater healthcare application development abilities.
Conference IEEE Explore. 2022,[15] IEEE	Ethereum vs. Hyperledger Fabric success rate, average latency, throughput, and resource usage.	Ethereum is a public blockchain, therefore all data is public, whereas Hyperledger Fabric is for private use cases.
IEEE Transactions on Network Science and Engineering. 2024,[18] IEEE	Ethereum and Hyperledger have been combined to develop a hybrid model by using SQLite. They also integrate IoMT devices in their model.	Hyperledger Fabric is a permissioned decentralized framework. It is not a centralized architecture.
IEEE Transactions on Industrial Informatics. 2020,[19] IEEE	An architecture based on blockchain technology by using hyperledger framework has been designed.	The authors had designed the architecture on the test network.
IEEE Transactions on Emerging Topics in Computing. 2019,[20] IEEE	A 360 degree review of the Applications, Benefits, Challenges and future roadmap.	Authors had done a deep review on the applications of blockchain in healthcare sector.
IEEE Access. 2022,[21] IEEE	Developed a patient data exchange model using Hyperledger platform	Utilized the advantages of Blockchain technology for patient information sharing.
Conference IEEE Explore. 2023,[25] IEEE	Discussed Hyperledger fabric's healthcare data management process.	Hyperledger Fabric is distributed, reliable, and immutable, it is able to use for sharing a patient's medical history.
IEEE Journal of Biomedical and Health Informatics. 2022,[26] IEEE	Proxy re-encryption on semi-trusted cloud storage allows for trackable, anonymous, aloof healthcare data storage and exchange through decentralized consortium blockchain.	The report has addressed all technical issues and in an efficient system via simulation and analytical theory.

AVISPA: Automated Validation of Internet Security Protocols and Applications; BAKMP-IoMT: blockchain-based authentication and key management scheme for the internet of medical things; EHR: electronic health records; GM-SSO: Genetically Modified Salp Swarm Optimization; HIoT: Health Internet of Things; IEEE: Institute of Electrical and Electronics Engineers; IoT: Internet of Things; PHR: Professional in Human Resources; SQLite: Structured Query Language of lightweight nature.

socket layer. Certificates, including public and private key pairs, may be found in the aforementioned GitHub repository, labelled fabric-ca-client, fabric-ca-server, or peer. These certificates provide the information needed to decrypt both the private and public keys. The permits granted to the actor are based on the actions that are carried out by the actor and are determined by the certificate. These certificates in the Hyperledger are managed by the MSP, and they adhere to a specific standard called X.509. This level of security to the identity makes blockchain technology desirable for many organizations.

Hyperledger Fabric uses team members who are legally separate entities to join the blockchain network. Figure 2 uses an example of a hospital named Allied Care Experts (ACE) Hospitals as a member organization, where more than one branch acts as the nodes. Each of the host nodes

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

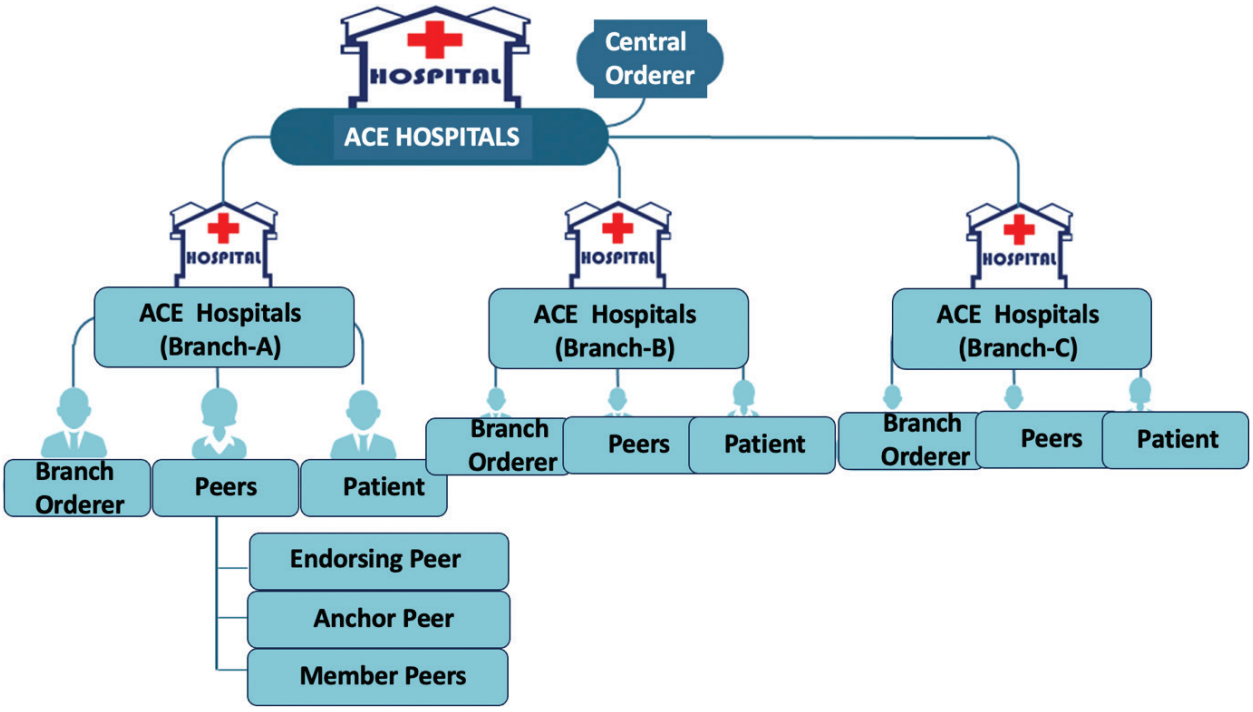

Fig. 1. Hierarchical model of a smart hospital using Hyperledger Fabri.

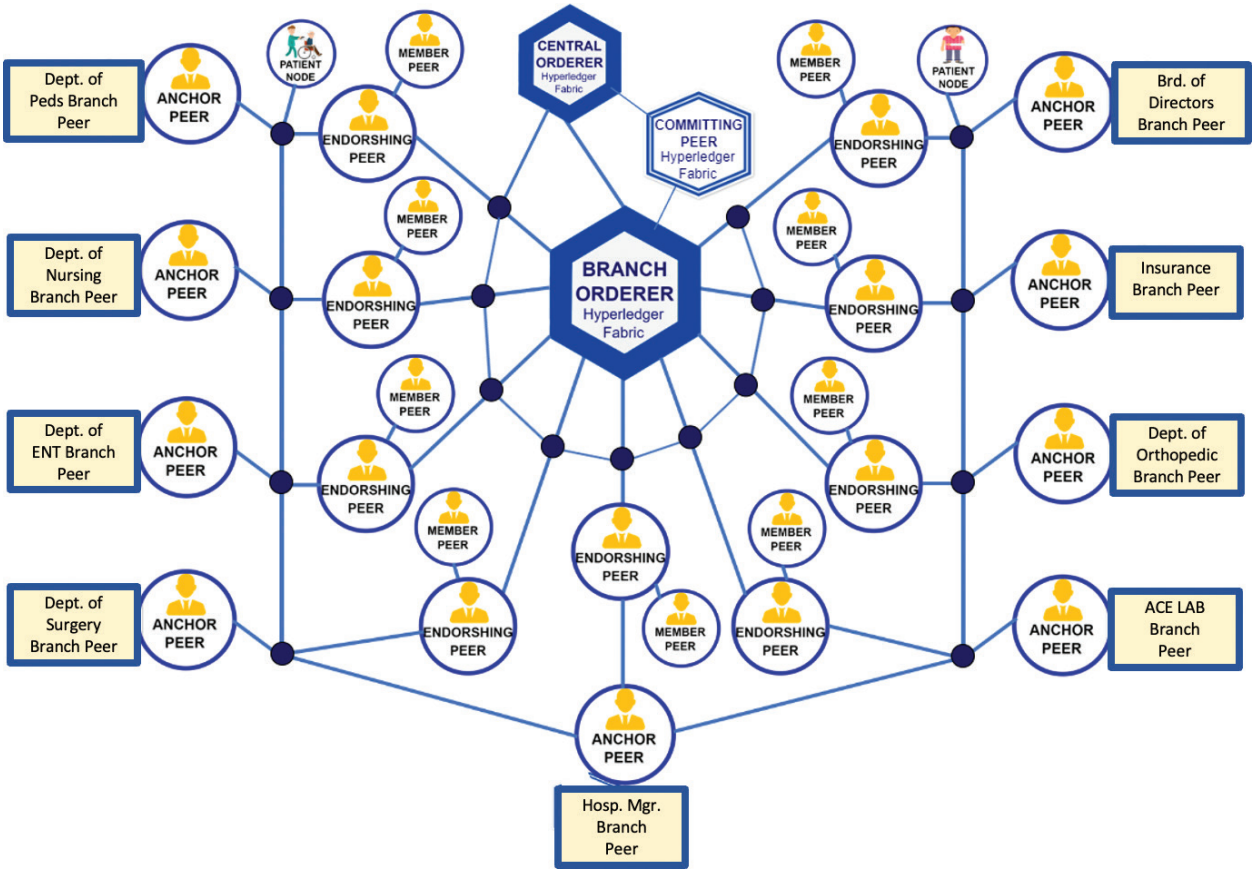

Fig. 2. Smart healthcare ecosystem using Hyperledger Fabric.

provided by each of the member entities shares one or more distributed ledgers. These nodes are used to manage the ledger status inside the organization and to submit transactions. All the data generated by the ordering service are recorded in the ledgers. It records all the events in chronological order and organizes them in a timeline. Users can access the information, and any request may be fulfilled for an authentic individual.

The orderer node creation is one of the initialization steps followed during the deployment and is responsible for the creation of new blocks for the transaction by forming an ordering service, which may implement centralized or distributed protocols. The central orderer node acts as a primary coordinator for the network, managing critical consensus tasks across branches. Its ordering service acts as a central hub where patients and peers may exchange diagnostic reports via IoT and prescribe treatment for speedy recovery. Each branch has its own local orderer node used for local transactions and ensuring data availability even if the central orderer is temporarily unreachable. It also uses cryptographic services with software or hardware cryptographic service providers on the platform and exposes cryptographic features such as encryption, decryption, keypair creation, private key message digest, and many other things. This orderer is one of the several binaries that have been cloned from the GitHub link of the Hyperledger community repository using the client URL command during the setup of prerequisites and installation of Fabric and Fabric Samples.

Raft is used for cluster formation, through which the orderer will be able to communicate with any other organization or peer. It requires the genesis block for initialization and the runtime properties. The ledger data for the blocks is written to the file system by the orderer during execution. According to the settings, the orderer is given the location of the ledger data. The orderer.yaml file is configured, and before that, the orderer binary is initialized using the genesis block.

The peer node is the physical body in any Hyperledger framework implemented. There might be many peer nodes in any organization. As in the model, the organization is in a healthcare center, so the peers are also placed. Each peer may consist of several Endorsing peers, one Anchor peers, and several Member peers. The transaction is processed once the endorsing peers validate the signature. Hence, the peers are created to establish a network structure. To effectively endorse a transaction, these peers must adhere to the endorsement rules in place.

When deploying transactions, certain rules and regulations must be followed to ensure both security and performance. These policies can be found in the Configuration Transaction Generator (i.e., configtxgen) binary. Organizational participants in a channel are the legal owners of the peers they use. They are the nodes that house the ledgers, link to the ordering service and other peers, and run the smart contracts. As the fundamental parts of the network, these peers perform a crucial role.

Like the Orderer node, the peer node contains a *core.yaml* file. As seen from the Github link, the *core.yaml* has multiple sections, such as the peer section, which contains networking, MSP, and storage paths; the ledger section, which contains the state database in *CouchDB*; and the chaincode section, which contains the logs. A specific naming scheme is followed by creating specific folders with paths for the new peers created. Ledger and channel data are distributed in a scalable manner using the gossip protocol used by peers. Using this gossip messaging protocol, each peer may exchange ledger data with several other peers in real-time. There may be only one anchor peer in a peer group. The anchor peer is the only peer that can communicate with another anchor peer group. In a similar vein, the endorser peers may take the form of one or more individuals and can communicate both ways with the patients.

Patients are the end users who utilize the software development kit to propose a transaction to the endorsing peer. Then only the endorsing peers will validate the transaction by simulating the *chaincodeID* and *txPayload* with a copy of the ledger. The member peers become part of the peer group with limited credentials, as they can only communicate with other peers through the anchor peers. The patients are the client nodes that use software development kits made by Golang to make any transaction by broadcasting a message that can only be received and validated by the endorsing peers. All the transactions that are started in the channel are kept private, meaning that only the members of the channel can access them.

Figure 2 shows the organogram that might be followed by hospital management, where the three types of peers were given charge distribution as per the policy made in the chain code. You can establish a decentralized network using the Hyperledger Fabric, which consists of several nodes that can interact with one another. In addition, the system keeps track of users' identities by employing an MSP.

The blockchain contains the chain code, the ledger data, and the transactions that are executed across it. Nodes in a blockchain network are referred to as peers inside the network. When it is talked about the nodes in this context, it is about the computers that are responsible for executing the apps that make up the blockchain. Each peer can store a copy of the ledger and any smart contracts. It is possible to create new peers in Hyperledger, start them, stop them, reconfigure them, and remove them. They make available a collection of application programming interfaces (APIs), which make it possible for administrators and applications to communicate with hyperledger services such as ledgers and chaincode.

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

Advantageously, a peer may host more than one ledger and chaincode since this provides for greater flexibility in the system. Like the staff nurse-1, she can be part of the orthopedic channel as well as the surgery channel. The staff nurse-1 who is running a computer is a node that stores the information on ledgers for both channels, and it will also have both the orthopedic chain and surgery chain.

Although this article speaks to the broader use of blockchain in Hyperledger Fabric in the healthcare industry, its primary concern is with the digital identity of a patient. It is safe to assume that in today's world, having an identity is one of the most fundamental needs for every living being to exist, and to demonstrate one's identity, several organizations provide a wide variety of identification cards that have been vetted by recognized organizations or government entities.

Similarly, the safety of an individual's identity, even though it is robust enough to be broken, continues to be the target of multiple attempts by unauthorized individuals in the hopes of achieving success in identity theft. Additionally, there are instances in which the theft of an individual's identity was successful, which raises the question of whether there is any other strategy or awareness that can keep an individual's identity from being tampered with. As if some instances could be picked to talk about, if an accident takes place, then in this urgent circumstance, it becomes extremely tough to identify the patient until and unless his or her close family arrives to identify them. This is the case that implies that the second person who arrives to identify the patient or corpse becomes the first and main option.

This choice has several drawbacks, such as the fact that the relative might be fake or that it could skip the patient's true relative. A circumstance quite similar to this one occurred after the recent railway catastrophe in India, which sent shockwaves across the whole globe. When it comes to determining someone's identification, it is a legitimate challenge that the administration of the hospital, as well as any government agency or other organization, must confront. Similar cases of identifying identities occur in every sector of the area, and solutions must be found for them all. However, in this particular instance, the sector in question is the medical field, which is one in which identity is the primary concern. This is because the life of a human being is a precious commodity, and as such, its identity should be protected from being altered and made available to whom it belongs at the appropriate time. Only by adhering to the CIA scheme, which is proven and discussed in the latter part of this article, is it possible to keep one's identity secure. In addition, this article demonstrates how the model is ready for production and adheres to the highest level for maintaining one's confidentiality, integrity, and availability at the right time and to the right person.

Because it was stated earlier that this study is concerned with a patient's digital identity, the suggested larger model has just the digital identity of a patient as its primary emphasis, and it has been explained in detail. The network topology of a smart hospital is laid out in Figure 3. Several bodies that are engaged in the process of diagnosis and treatment are all documented in the ledgers that are made of fabric. Using IoT in the network causes the process to become automated. In this automated process, the patient's information and tracking are captured by IoT wearable devices, which has the advantage of allowing for speedier treatment at the needed time. One patient could have multiple diseases, which could be treated at the same hospital organization or a different organization like (Hospital Laboratory, Medico Insurance, Orthopedic Dept., Surgery Dept., Ear Nose and Throat Dept. etc.). However, as described in Figure 3, all the organizations are interlinked in the hyperledger chain, and and one patient is a node in several channels. Additionally, the staff nurse who is the endorsing peer, as mentioned in the previous paragraph, could also be a node point in any other channel. Therefore, it can be said that all the node points are attached in some fashion, depending on the range of permissions that each node point was granted by the organization's orderer.

Hyperledger Fabric is one of the platforms that blockchain uses, and it is being developed by open source. Blockchain is a technology, and some of its applications have already achieved the height of popularity in the realm of the cryptocurrency world. Despite this, Hyperledger Fabric is one of the platforms that blockchain uses. Fabric is designed to be extremely modular and adaptable, making it suitable for applications in the banking, finance, insurance, healthcare, human resources, supply chain, and even digital music distribution sectors. And here the healthcare industry has been selected to receive an enterprise-grade, permissioned distributed ledger technology platform. This platform delivers many key differentiating capabilities compared to other popular distributed platforms, which may be best in some areas. However, the fabric is taking advantage of and overcoming the disadvantages of those decentralized platforms.

The core workflow of the deployed Hyperledger Fabric for the production network of the hospital organization is displayed in Figure 4. In it, the transactional mechanics that occur during a patient's enrollment or registration at the appropriate hospital department are laid out in detail. For patients already registered, they may use a software development kit to have their registration identification recognized in the application by supplying their biometrics using body sensing equipment to identify themselves, or they can use a software development kit (SDK) to become registered by filling out the needed data of the SDK themselves.

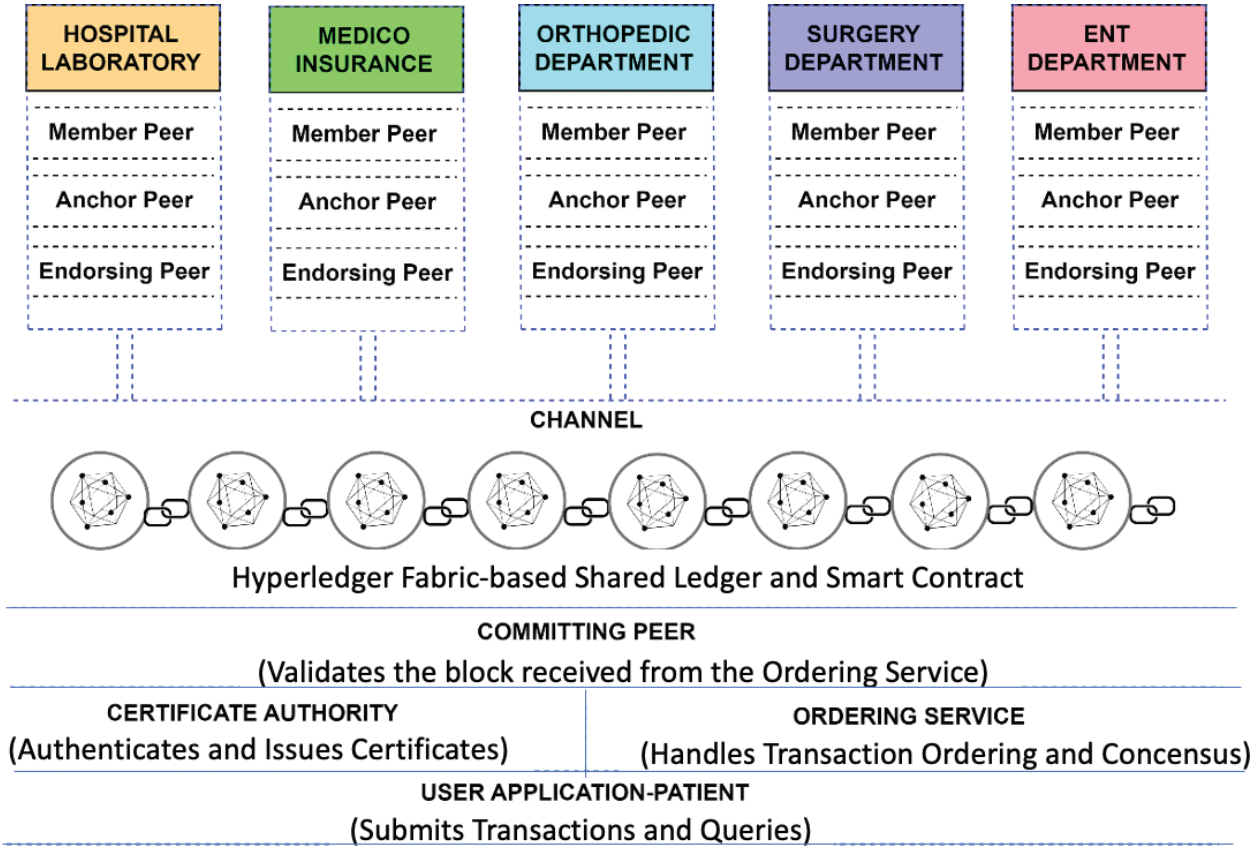

Fig. 3. Hyperledger Fabric Network Topology for Smart Healthcare Solution.

A transaction proposal is generated when an application written in one of the supported SDKs (Node, Java, or Python) makes use of one of the APIs. To read from or write to the ledger, the proposal asks for the execution of a chaincode function. The SDK acts as a bridge, transforming the patient's cryptographic credentials into a one-of-a-kind signature for the transaction proposal and packaging it in the correct architectural format. This workflow, explained further below, begins with the initiation of the first message a patient sends to the endorser peer node, which then follows the endorsement policy specified by the orderer node for making a transaction in the channel.

The patient will initially broadcast the message, which is received by the endorsing peer, who acts as the assistant nurse and may simulate the *chaincodeID* and *txPayload* from the message.

Here, the format of the message may be <*PROPOSE, tx, [anchor]*>, where *tx* is mandatory and anchor is optional. Again, *tx*=<*cliendID, txPayload, timestamp, clientSig*> and the entire message format is explained in the readme file at the included GitHub link. The endorsing peer checks that the transaction proposal is correctly formatted and that the signature is legitimate by using this method. The transaction results, which include a response value, read set, and write set, are produced when the endorsing peers provide the transaction proposal inputs as arguments to the function of the called chaincode. This function is then performed against the existing database.

One thing to keep in mind is that the ledger is not undergoing any modifications at this time. This is subsequently forwarded along as a 'proposal response,' which is examined by the ordering service after being received by the orderer node. The ordering service takes in all the transactions from the various channels in the network, sorts them in order of their occurrence in time, and then creates blocks of transactions for each channel. These blocks of transactions are then sent to all the peers in the relevant channel. And then the ledger is eventually updated across all the nodes. In all, the endorsing peer sends the transaction-endorsed messages to the patient, which will then be sent to the orderer peer, who will assign the patient to the required channel with a particular endorsing peer and anchor peer. In a broader sense, it can be said that finally, the patient is allotted to a particular peer node, which is where the therapy process will proceed.

Now, if the question arises as to how digital identity is incorporated into the overall procedure, the answer is

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

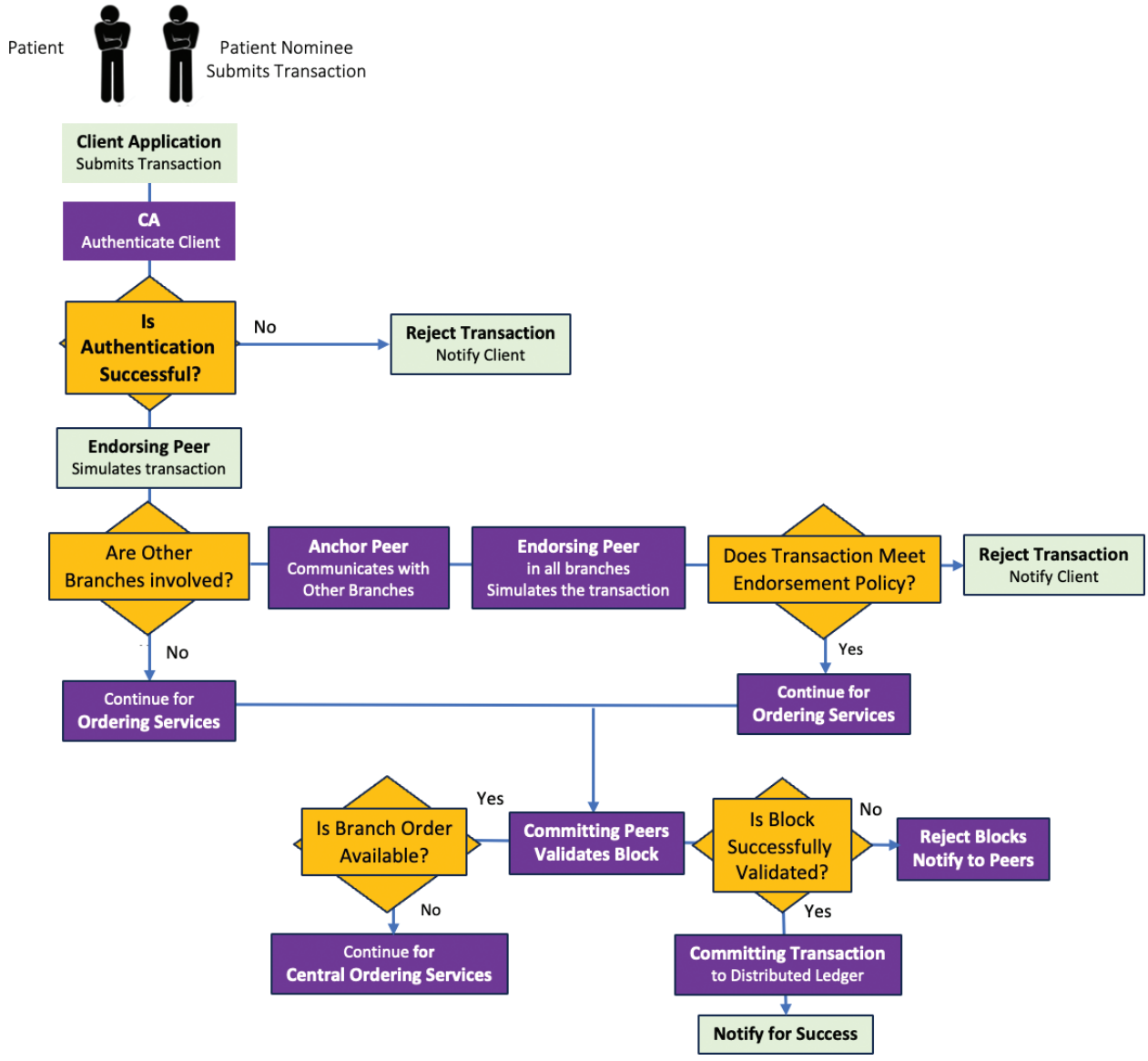

Fig. 4. Process Flow of Transaction Lifecycle in Hyperledger Fabric for Smart Healthcare. CA: certificate authority.

straightforward: Hyperledger is a massive chain of blocks that incorporates a number of organizations into it. Alternatively, it could say that it is an interconnection of all the organizations, in which case various sets of policies are in place for the nodes to act upon, and a single node may have varying roles in various channels. Policies are also maintained by the orderer of the organization. Patients will invariably have linked themselves, either directly or indirectly, to the chain of networks, which will have individually given them an identity as well as caused them to be stored and recognized with ease.

Tools and Methods Used

The Hyperledger Fabric framework is provided by the Linux Foundation in the open-source market to make research and innovations with much more developmental work. It requires becoming acquainted with the key concepts of Hyperledger Fabric and then installing the prerequisites depending on the platform (here it is for Windows: Docker, WSL2, VS Code, Git to run the software). Thereafter, it is needed to clone the Hyperledger Fabric with the Git repository, or else you can download the fabric binaries from Git to the system and deploy it by using the curl command. It could also be downloaded and opened up with VS Code directly in the Windows platform.

All these were tested on a test network first of fabric samples and then implemented on the fabric main to make a production network. The network is started by executing the network.sh command; also, Vagrant can be used.

Thereafter, it is needed to set up the network by creating Channels, Peers, Orgs, Orderer, Patient nodes and policies for the nodes, and the CAs are set up to create the MSPs.

A screenshot of a patient identity structure is shown in Figure 4. Similarly, Figure 5 shows the screenshot of peer nodes created using Ain't Markup Language (YAML). The policies assigned for different peer nodes in the model are displayed in a screenshot of Figure 6. These dictate who can endorse transactions, access data, manage the network, and make administrative changes. The database is CouchDB, while LevelDB can potentially be utilized similarly. Golang is used for chaincode development. All these need to be done by a network administrator. The strong network creation is very much required to defend against the vulnerabilities that are played by the network administrator in a very efficiently. The hardware used for the implementation of the fabric kit is as follows: Dell AMD Ryzen-5 Hexa Core Processor-5515 with

```go
type PatientIdentity struct {
    ID            string `json:"id"`
    Name          string `json:"name"`
    DOB           string `json:"dob"`
    Gender        string `json:"gender"`
    MedicalRecords []string `json:"medicalRecords"`
    AccessControl map[string]bool `json:"accessControl"` // Who can access the record
}
```

Fig. 5. A screenshot of a patient identity structure.

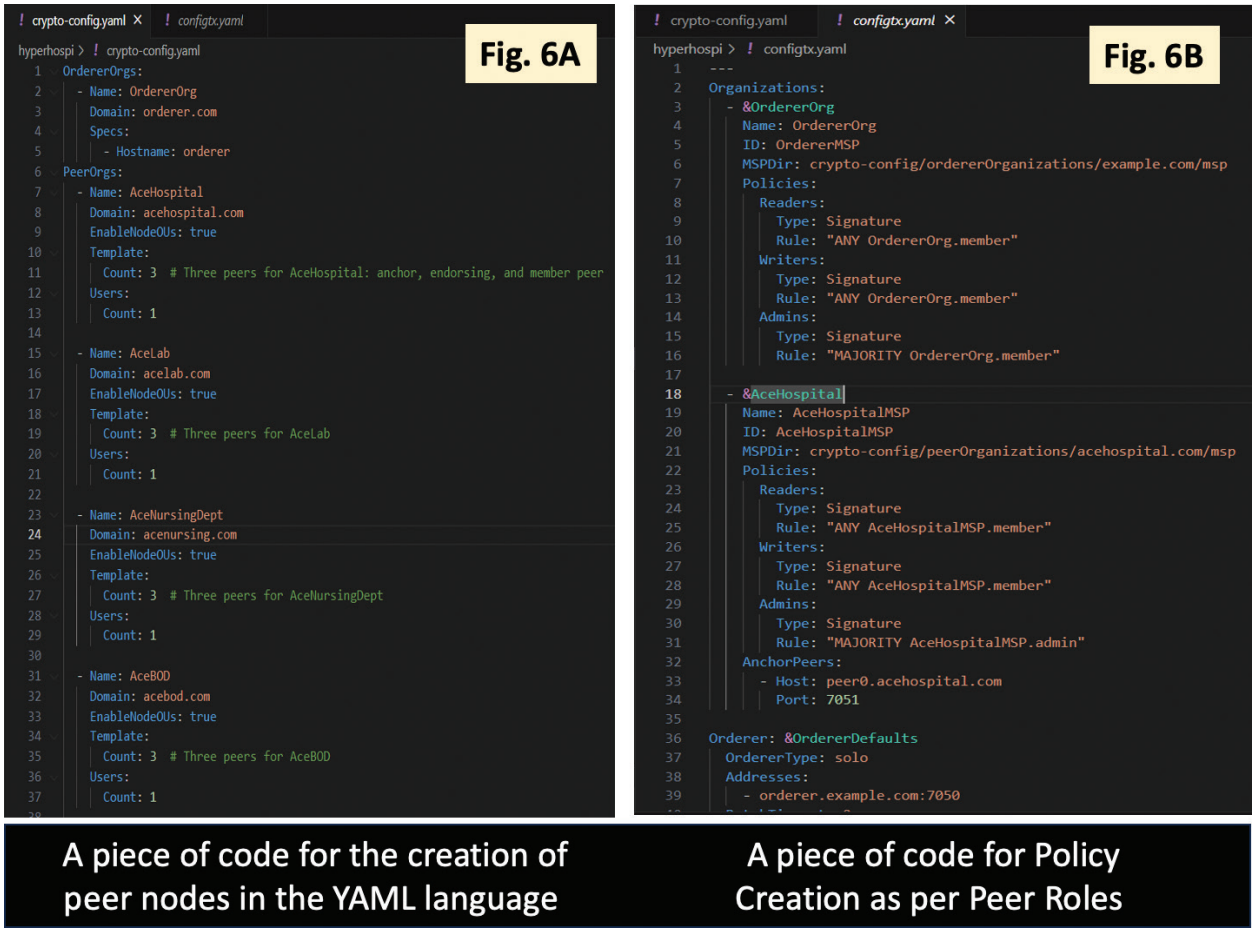

Fig. 6. A piece of code for patient identity structure in the GO language. Figure 6A shows the screenshot of peer nodes created using Ain't Markup Language (YAML). The policies assigned for different peer nodes in the model are displayed in a screenshot of Figure 6B.

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

16 GB of RAM and 4 GB of NVDIA RTX-3050/120Hz Discrete Graphics.

Crypto Hash Techniques Used

To guarantee the security, confidentiality, and reliability of sensitive medical data, the article's cryptographic hash algorithms are essential for an increasingly linked healthcare setting. These methods form the basis for establishing a secure communication between IoT devices by maintaining data integrity and producing tamper-proof digital identities. Healthcare systems can create distinct digital fingerprints for patient records and IoT device data by utilizing cryptographic hash functions like SHA-256 and SHA-3 as well as lightweight substitutes like BLAKE2, guaranteeing that any alteration is identifiable. While hash-based digital signatures safeguard the secrecy and legitimacy of data transferred across networks, blockchain hash chaining further ensures the integrity of medical records.

Cryptographic hash generator, $H(x)$ is a single direction mathematical function that transforms an input x with an arbitrary length into an output with a specific length h. This result is known as the hash value or digest. x is the unique biometric data of a patient, which is hashed to create a secured digital identity h. A hash function is formally defined as:

$$H: \{0,1\}^* \rightarrow \{0,1\}^n \quad (1)$$

Where:

- $\{0,1\}^*$denotes an input arbitrary length.
- $\{0,1\}^n$ denotes a fixed-length output of n bits.

The function $H(x)$ must satisfy the following properties:

1. For same input x the function always produces same hash value h.
2. Given h, finding x such that $H(x) = h$ is computationally impossible.
3. It is computationally impossible to obtain two separate inputs, x_1 and x_2, such that $H(x_1) = H(x_2)$
4. A small change in x significantly affects h.

Cryptographic hash functions are generated and used to link blocks of transactions or data (such as patient records). This ensures data integrity because tampering with any block changes the hash values of subsequent blocks, disclosing the tampering. The hash of the most recent block $H(B_1)$ is obtained as follows:

$$H(B_i) = H(D_i \| H(B_{i-1}) \| T_i \quad (2)$$

- D_i denotes recorded IoT sensor data.
- $\|$ denotes concatenation of values.
- $H(B_{i-1})$ is the hash of previous block.
- T_i denotes timestamp.

Digital signatures use cryptographic hash functions and asymmetric encryption to assure data secrecy and authenticity, which legitimates patient data or medical reports that are transferred across devices. This ensures confidentiality and authenticity of digital signatures in an IoT-enabled healthcare system.

Mathematically, the digital signature of a message m is created as follows:

Step 1: Compute hash of the message $h = H(m)$

Step 2: Encrypt hash by using the sender's private key K_{priv}

Where:

$$\sigma = E_{priv}(h) \quad (3)$$

And σ is the signature that is sent alongside the message.

Step 3: Verification of signature by decrypting it using sender's public key K_{puv}, if $h_1 = h_2$

By,

$$h_1 = D_{puv}(\sigma) \quad (4)$$

$$h_2 = D_{puv}(\sigma) \quad (5)$$

Merkle trees are used in blockchain-enabled healthcare systems to efficiently validate big datasets, such as patient information, while keeping the full dataset private. The structure of a Merkle Tree is as follows:

Step 1: The hashes h_1, h_2,……..h_n of each individual piece of data are calculated.

$$h_i = H(D_i) \; for \; i = 1, 2, \ldots .n \quad (6)$$

Step 2: Parent nodes are formed by concatenating pairwise hashes and hashing them once more.

$$h_{ij} = H(h_i \| h_j) \quad (7)$$

Step 3: This procedure keeps going until the Merkle root is obtained.

SHA-256 is a key technique in blockchain-based systems that maintains the security and integrity of critical patient data. It is a one-way cryptographic hash function that outputs a constant 256-bit (32-byte) value regardless of input size. This means that the original input cannot be deduced from the output, and it is collision-resistant, ensuring that no two distinct inputs yield the same hash value. Each block in blockchain-based healthcare systems includes a timestamp, patient data, and a reference to the preceding block's hash.

Mathematically:

$$h = SHA - 256\,(x) \tag{8}$$

Where:

- x denotes the input message.
- h denotes the fixed output of 256-bit hash.

And,

$$H(B_i) = SHA - 256\,(D_i \| T_i \| H(B_{i-1})) \tag{9}$$

Where:

- $H(B_i)$ denotes the hash of current block i.
- D_i denotes the data in a block.
- T_i denotes the timestamp of block.
- $H(B_{i-1})$ denotes the hash of previous block.
- || denotes the concatenation operator.

Algorithm for Digital Identity Encryption

Algorithm 1 & Algorithm 2 are used for digital signature generation and verification that ensures data authenticity, integrity, and confidentiality in secure systems. After creating a digital signature, the sender first uses a cryptographic hash function, SHA-256 to hash the original message into a fixed-length digest, which is then encrypted using their private key. The original message gets forwarded to the recipient along with this signature. To verify the message, the recipient computes the hash of the received message after decrypting the signature with the sender's public key. The validity of the signature is next verified by comparing the two hashes; if they match, the message's authenticity and integrity are confirmed.

Algorithm 1. Digital Signature Generation.

For, m = message and K_{priv} = private key
Compute the hash of the message
$h \leftarrow H(m)$
For, h = hash and $H(m)$ = cryptographic hash function
Encrypt the hash with the sender's private key
$\sigma \leftarrow Encrypt(K_{priv}, h)$
Return Digital Signature σ
End

Algorithm 2. Digital Signature Verification.

For, m = message and K_{pub} = public key
Decrypt the digital signature with public key
$h' \leftarrow Decrypt\ (K_{pub}, \sigma)$
Compute the hash of the message received
$h'' \leftarrow H(m')$
Compare the hashes
If $h' = h''$
Return Valid Digital Signature (σ)
Return invalid Digital Signature (σ)
Elseif
End

Result Analysis

Security Challenges

Hyperledger Fabric has numerous safeguards to ensure a network operates in accordance with the CIA scheme. Immutability and decentralization of data are both preserved in the Hyperledger Fabric ledger, which is a distributed network of peer nodes.[27] Many businesses are adapting other popular blockchain platforms for enterprise use right now, but hyperledger fabric is still ahead of the pack because it was built specifically with permissioned distributed ledger technology to deliver key differentiating capabilities over other popular distributed technologies and also the open-source availability of codes allows many developers to apply their intellectual abilities in making fabric bug-free[28,29] It is the first distributed ledger platform to allow smart contracts/chaincode to be written in general-purpose programming languages like Java, Go, and node.js, providing a highly modular and editable architecture that promotes innovation, versatility, and efficiency across a wide variety of industry use cases. And also, no cryptocurrency is needed to incentivize mining or power the execution of smart contracts. Despite Hyperledger Fabric's versatility and a number of useful high-level capabilities, certain organizations might have difficulties during implementation and use.[30]

Identification and Authentication

It is the crucial part of Hyperledger Fabric to establish a robust identity management system. Any failure in managing the identity may lead to unauthorized access with malicious activities.

Risks in chaincodes

The chaincodes written in Go, Node.js may have some vulnerabilities that can be exploited. So, organization need to have through code reviews, security audits, and testing to identify the vulnerabilities.

Information Security

The private channels which carry sensitive data within the network of authorized nodes. But this could be a challenging factor for the organization, so it is needed to carefully implement encryption techniques, write policies to protect the data from unauthorized disclosure.

Protecting Dispersed Networks

As Hyperledger rests on distributed network technology, hence the organizations should implement advanced encryption algorithms, firewalls, intrusion detection

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

systems to protect against network level attacks using unauthorized access.

Consensus-Based Attacks

When many parties have agreed upon a transaction, it is stored in a distributed ledger, which is a shared database among various nodes. The consensus algorithm used in Hyperledger Fabric can have malicious actors that attempt to manipulate the order of content of transactions. And another point would be the nodes struggle for control during the consensus process; the branching event could happen.

Resistance to Cyber Attacks

The distributed ledger technology provides certain mechanisms and best practices that contribute to the resistance against different cyberattacks, including brute force attacks, Distributed Denial of Service attacks (DDoS), Denial of Service Attacks (DoS) and 51% attack. The organization should maintain best security practices, conduct regular security audits, and stay updated with the latest security patches to get a secured Hyperledger network. The main risk to security that must be fixed to acquire the trust of Hyperledger members and new clients. It is very much necessary to understand the attacks to defend them. Here is the analysis of how the newer technology mitigates these types of attacks. The references[31,32,33] give a broader idea to understand and make strategic plans to prepare resistance methodologies for the possible security issues. Similarly, in regard to[34] i.e., Table 2, four vulnerabilities have been discovered to date.

Brute Force Attacks

The attacker might use the brute force method on a website that requires a user ID and password. It may use any automated program to make a hit-and-trial method of several password combinations to find the correct one. Or, as the article describes about biometric identification methods, the attacker may collect several biometric identification samples and apply them in a brute force method to collect patient health information. Keeping in view these types of attacking techniques, there are several features and mechanisms that help resist the brute force attacks. Some of them, such as the robust access control and authentication mechanism ensures that only authorized entities can access the network. By applying the best cryptographic techniques for encryption of data, an extra layer of protection makes it extremely difficult to decrypt it without encryption, such that even if the attacker intercepts the encrypted data, it becomes more difficult for attackers to make brute force attacks possible.

DoS Attacks

A DOS attack is a type of attack that prohibits the legitimate users from reaching a network, host, or other pieces of the architecture. It often targets banks, credit card gateways, and other financial institutions to temporarily disrupt the host. It is always a key source of worry in any cybersecurity infrastructure. Due to a DoS attack, a load is created on the web server, making it overload with a large number of request packets. The persona of an endorsing peer is known to all members of a channel, opens the door for DoS attacks. So, maintaining the anonymity of the endorsing peers can be the prevention against the attack.

DDoS Attacks

The DDOS attacks are a significant variant of the DOS threat with many categories that affect the network bandwidth, RAM and CPU resources and slow the processing power. The solution can be a strong network and policy-making. It can be a risk via profiling load.It might not be direct, but could one of them be on port 6060, which has been resolved in the upgraded versions. So, it is needed to use the updated SDK of fabric.

51% Attack

It can also be termed a majority attack, as the attacker owns more than half the power of decision-making in the blockchain network. Hyperledger Fabric is a private, permissioned network, so the risk of a 51% attack is very low. However, it cannot be disregarded because a scenario might emerge if the network is not properly configured. The network can be designed in such a way that the consortium group, rather than being part of the internal members of the organization, can be a group of other organizations also, and any transaction would need approval of all the participants rather than a few selected

Table 2. Discovered vulnerabilities of Hyperledger Fabric, recorded in CVSS scorecard.[34]

CVE ID	Affected product name	Type of attack	CVSS score	EPSS score
CVE-2022-45196	Hyperledger Fabric	Denial of service	7.5	0.05%
CVE-2022-36023	Hyperledger Fabric	Input validation	7.0	0.12%
CVE-2022-31121	Hyperledger Fabric	Input validation	7.5	0.15%
CVE-2022-3756	Hyperledger Fabric	Security vulnerability	7.5	0.08%

CVE: Common Vulnerabilities and Exposures, CVSS: Common Vulnerability Scoring System, EPSS: Exploit Prediction Scoring System, ID: identification.

members. This differs from the traditional centralized network where the administrator has the full permission that may become malicious at any time.

Empirical Findings

The efficiency of the model is compared with the cited references in Table 3, which results in a highly efficient model with unique architecture that can be implemented for operations. Which are then analyzed through resource utilization of various nodes are evaluated using Hyperledger Caliper of the model, which has been displayed in Table 4. Organizations can better deal with fabric's challenges by following secure network design, which includes things like implementing the CIA scheme, performing regular security audits and testing, and using the most recent security patches and updates provided by the Hyperledger Community. To further strengthen the safety of their Hyperledger Fabric deployments, businesses may also seek the advice of security professionals and consultants versed in blockchain and distributed ledger technology.

Thus, a networked CIA architecture is essential. Hyperledger Fabric has the following important safety measures.

Immutability

Any decentralized ledger is known for its immutability. And this ensures data integrity, trust, and security within the network. Once a transaction is recorded on blockchain, then it cannot be altered, deleted, or tampered with. This safety measure of data integrity,

Table 3. Comparison of efficiency of the cited references.

Reference	Consensus mechanism	Performance indicators	Scalability	Privacy & security	Latency	Throughput	Remarks
Cyran[5]	PoA	Identity verification speed, level of security	Moderate	Strong	High	Low	Highly suitable and lightweight design with enhanced security and authentication.
Natarajan, et al.[7]	PoS, PoW	Authentication time, access control, cryptographic strength	Moderate	Strong	Moderate	High	The study is for application in healthcare supply chains and is scalable for streamlining medical asset logistics.
Tanwar, et al.[12]	POW	Data privacy, processing efficiency	Limited	Strong	High	Low	Despite having high security, huge networks suffer from performance overhead.
Rehman, et al.[18]	Hybrid (PoS + Consortium Consensus)	Resource efficiency, data processing speed	High	Strong	Low	High	Recommended for IoMT and making effective use of resources.
Barbaria, et al.[21]	RAFT	Data sharing speed, network reliability	Moderate	Strong	Moderate	Moderate	Robust security but limited scalability for large-scale healthcare systems.
Gohar[23]	PBFT	Semantic data interoperability, access speed	High	Moderate	Low	High	Strong semantic interoperability but potential privacy issues.
Saranya and Murugan[25]	RAFT	Transaction speed, data integrity	High	Strong	Low	High	High efficiency with strong data integrity, best suited for private networks.
Proposed	PBFT	Confidentiality, integrity, availability	High	Strong	Moderate	High	It is developed for an operational model rather than a test network.

PBFT: Practical Byzantine Fault Tolerance, PoA: Proof of Authority, PoS: Proof of Stake, PoW: Proof of Work, RAFT: Crash Fault Tolerant Consensus.

Table 4. Performance Indicators Across Different Parameters of the Tested Model.

Type Avg.	Name	Avg. Memory	CPU Usage	Traffic In	Traffic Out	Disc Write
Docker	admin@orderer.com	59.3 MB	2.11%	3.4 MB	16.0 MB	4.8 MB
Docker	peer0.acehospital.com	274.4 MB	6.55%	4.5 MB	440.9 KB	6.3 MB
Docker	admin@acesurgery.com	206.4 MB	6.53%	4.8 MB	435.7 KB	6.2 MB
Docker	user1@acesurgery.com	223.9 MB	5.98%	3.2 MB	480.3 KB	6.7 MB
Docker	admin@aceortho.com	207.4 MB	7.33%	5.2 MB	432.5 KB	5.3 MB
Docker	admin@medicinsurance.com	274.4 MB	12.3%	4.6 MB	430.0KB	6.8 MB

CPU: central processing unit, KB: kilobyte, MB: megabyte.

Citation: Blockchain in Healthcare Today 2025, **8**: 411 - https://doi.org/10.30953/bhty.v8.411

security, and trustworthiness that makes Fabric an ideal choice for enterprise applications. So it can be said that all the transactions are guaranteed tamperproof with a tracking facility.

Data Isolation

It is the ability to restrict access to certain data so that only authorized participants in the network can view or interact with it. Data stored or exchanged on the blockchain platform is isolated using advanced encryption algorithms. This is a key feature in permissioned blockchain networks, where organizations may need to maintain privacy and confidentiality within a shared ecosystem. This proves the confidentiality feature of fabric.

Permissioned Network

Hyperledger maintains a permissioned network where all the nodes are identified and authenticated. Each participant has a role-based permission (Peer, Orderer, Client) where the Access Control Lists (ACLs) define who can read, write, and execute transactions. Only authorized participants can join and transact on the channel, ensuring that the network is secured and protected from unauthorized access.

Identity Management

The fabric supports various identity frameworks including X.509 certificates, MSPs, and CAs, which ensure that only trusted participants can engage in transactions on the network.

Access Control

It is a mechanism that defines who can perform specific actions within the block network. A fine grade access control mechanism is maintained, that enforces access policies for network resources. There are also ACLs configured to regulate channels, chaincodes, and any other specific data within the ledger. This proves the authorization policy.

Endorsement Policies

The endorsement policies determine the required number of endorsements from specific participants to validate transactions, which proves the validation and integrity of the network. An endorsing peer simulates the transaction and signs the result, and if it complies with the policy, it is sent back to the client.

Consensus Mechanisms

Consensus Algorithms like Practical Byzantine Fault Tolerance (PBFT) and Raft were used. The consensus mechanism is offered by Hyperledger fabric allows to choose the most suitable consensus algorithm for a specific requirement.

Efficient chaincode operation

In Hyperledger Fabric, chaincode is a smart contract that specifies business logic for carrying out transactions. Organizations can develop and deploy their own chaincodes in the channels that can run in a secure and isolated execution environment with controlled access to resources preventing unauthorized access.

Conclusion

The use of Hyperledger Fabric-based architecture to manage patient identification in smart healthcare systems demonstrates blockchain's capability to transform data security, interoperability, and stakeholder engagement. Using Fabric's modular architecture, the solution ensures confidentiality, real-time access, and decentralized storage, enabling both healthcare providers and patients. Through detailed testing and debugging, the system displays scalability and efficiency, addressing critical difficulties in healthcare data management. This work highlights blockchain's disruptive potential by improving trust, operational effectiveness, and compliance with global data protection regulations, opening the path for a more secure and linked healthcare ecosystem.

Funding

None of the authors of this article has received by any funding for doing any experimentation work.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Author Contributions

Sanjay Kumar Jena: Writing original draft, investigation, conceptualization, formal analysis. Ram Chandra Barik: Project administration, visualization, supervision. Saroj Padhan: data curation, methodology, validation.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

Data may be made available on request. No AI-generated text was used.

Application of AI-Generated Text or Related Technology

No AI-generated text was used.

Acknowledgments

Dr. Jenna would like to express my gratitude to my primary supervisor, who guided me through this paper. I would also like to thank our madam, Head of the Department of Computer Science and Engineering at C. V. Raman Global University, Bhubaneswar, for her extensive guidance. Thanks are also due to the library staff and research participants who provided invaluable

assistance and inspiration, without whom this article never would have been written.

References

1. Goldberg R, Pitts PJ, Hinkel J. Healthcare Futures: Opportunities, Challenges and Risks in a Blockchain-Driven Environment. Blockchain in Healthcare Today. 2024 Dec 30;7:10-30953.
2. Feroz I, Ahmad N. Systematic Review of Usability Factors, Models, and Frameworks with Blockchain Integration for Secure Mobile Health (mHealth) Applications. Blockchain in Healthcare Today. 2024 Dec 16;7:10-30953.
3. Cyran MA. Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today. 2018 Mar 23.
4. Sharif R. Accelerating the Worldwide Adoption of Blockchain Technology. BHTY [Internet]. 2023 Aug. 18 [cited 2025 Aug. 14];6(2). Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/278
5. Yousef N, Sata A, Shukla M, Jarboui S, Mobarsa D. Blockchain-integrated IoT device for advanced inspection of casting defects. Scientific Reports. 2025;15:5300.
6. The role of digital identity in modernising healthcare [Internet]. ET HealthWorld. 2023. Available from: https://health.economictimes.indiatimes.com/news/health-it/the-role-of-digital-identity-in-modernising-healthcare/99391030
7. Natarajan M, Bharathi A, Sai VC, Selvarajan S. Quantum secure patient login credential system using blockchain for electronic health record sharing framework. Scientific Reports. 2025;15:4023.
8. Pradhan B, Bhattacharyya S, Pal K. IoT-based applications in healthcare devices. Journal of healthcare engineering. 2021;2021:6632599.
9. Qureshi F, Krishnan S. Wearable hardware design for the internet of medical things (IoMT). Sensors. 2018;18:3812.
10. Singh RP, Javaid M, Haleem A, Vaishya R, Ali S. Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. Journal of clinical orthopaedics and trauma. 2020;11:713–7.
11. Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJ, Park Y. BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE access. 2020;8:95956–77.
12. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020;50:102407.
13. Houtan B, Hafid, Abdelhakim Senhaji, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access. 2020;8:90478–94.
14. Agbo CC, Mahmoud QH. Comparison of blockchain frameworks for healthcare applications. Internet Technology Letters. 2019;2:e122.
15. Zhao Z. Comparison of hyperledger fabric and ethereum blockchain. In: IEEE. 2022. p. 584–7.
16. Leng Z, Tan Z, Wang K. Application of hyperledger in the hospital information systems: A survey. IEEE Access. 2021;9:128965–87.
17. ANA ANW, Zahary, Ammar T, Al-Shargabi, Asma A. Blockchain-IoT healthcare applications and trends: a review. IEEE Access. IEEE; 2024.
18. Rehman AU, Tariq N, Jan MA, Khan F, Song H, Ibrahim M. A blockchain-based hybrid model for IoMT-Enabled intelligent healthcare system. IEEE Transactions on Network Science and Engineering. IEEE; 2024.
19. Singh AP, Pradhan NR, Luhach, Ashish K, Agnihotri S, Zaman JN, Verma S, et al. A novel patient-centric architectural framework for blockchain-enabled healthcare applications. IEEE Transactions on Industrial Informatics. 2020;17:5779–89.
20. Kassab M, DeFranco J, Malas T, Laplante P, Destefanis G, Graciano V. Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing. 2019;9:1835–52.
21. Barbaria S, Mont MC, Ghadafi E, Machraoui, Halima Mahjoubi, Rahmouni, Hanene Boussi. Leveraging patient information sharing using blockchain-based distributed networks. IEEE Access. 2022;10:106334–51.
22. Antwi M, Adnane A, Ahmad F, Hussain R, ur, Abdelaziz KC. The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications. 2021;2:100012.
23. Gohar AN, Abdelmawgoud, Sayed Abdelgaber, Farhan MS. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. IEEE access. 2022;10:92137–57.
24. Syed TA, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, Alghamdi T. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE access. 2019;7:176838–69.
25. Saranya R, Murugan A. A hyperledger fabric-based system framework for healthcare data management. In: IEEE. 2023. p. 552–6.
26. Liu J, Jiang W, Sun R, Bashir AK, Alshehri MD, Hua Q, et al. Conditional anonymous remote healthcare data sharing over blockchain. IEEE journal of biomedical and health informatics. 2022;27:2231–42.
27. Khan FA, Asif M, Ahmad A, Alharbi M, Aljuaid H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustainable Cities and Society. 2020;55:102018.
28. Jena SK, Kumar B, Mohanty B, Singhal A, Chandra BR. An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. Decision Analytics Journal. 2024;10:100411.
29. Wenhua Z, Qamar F, Abdali TAN, Hassan R, Jafri, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023;12:546.
30. Ruan Z. Blockchain technology for security issues and challenges in IoT. In: IEEE. 2023. p. 572–80.
31. Andola N, Gogoi M, Venkatesan S, Verma S. Vulnerabilities on hyperledger fabric. Pervasive and Mobile Computing. 2019;59:101050.
32. Chaganti R, Boppana, Rajendra V, Ravi V, Munir K, Almutairi M, Rustam F, et al. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. IEEE Access. 2022;10:96538–55.
33. Tevora. Tevora: Cybersecurity, risk, and compliance services [Internet]. 2025. Available from: https://www.tevora.com
34. CVEDetails.com. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Internet]. 2025. Available from: https://www.cvedetails.com