Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic

Mahender Kumar a,b,*, Satish Chand a,b

a School of Computer and Systems Sciences, India
b Jawharlal Nehru University, New Delhi, India

ARTICLE INFO

Keywords:
- Hyperledger fabric
- COVID-19
- Internet of medical things
- Blockchain
- Security and privacy

ABSTRACT

Recently, an infectious disease, coronavirus disease 2019 (COVID-19), has been reported in Wuhan, China, and spread worldwide within a couple of months. There have been seen an outbreak of COVID-19 in many countries, where the infected patients’ rate overwhelmed the inadequate medical services. The push of patient-centered interoperability (PCI) from medical institution-centered interoperability may defeat the current and post resultant disease of the COVID-19 pandemic. This paper proposes a state-of-the-art privacy-preserving medical data sharing system based on Hyperledger Fabric (MedHypChain), where each transaction is secured via an Identity-based broadcast group signcryption scheme. We proved that MedHypChain achieves confidentiality, anonymity, traceability, and unforgeability. Besides, we regularize the MedHypChain to implement the PCI healthcare system, where the patient manages its health-related information in the blockchain that can be accessible to the authorized entity. We also use the Hyperledger caliber as a benchmark tool to analyze the performance of MedHypChain in three metrics (latency time, execution time, and throughput) for up to 20 permissioned nodes. Finally, we compare MedHypChain with related blockchain-based healthcare systems and found that the proposed scheme needs the least computation cost and communication cost and achieves all security features, such as authenticity, scalability, and access control.

1. Introduction

In late 2019, the first case of the coronavirus disease (COVID-19) has been detected in Wuhan, China. The virus disseminated in the population and exponentially spread globally (Mehta et al., 2020). After China, Italy became the second hotspot of most significant infected cases of COVID-19, with a very high fatality rate of 7.2% (1625 deaths/22512 cases), which was substantially higher on comparing in China (2.3%) on March 17, 2020 (Remuzzi and Remuzzi, 2020). On May 11, 2020, the virus had affected around 118,000 people in 114 countries, and more than four thousand people have lost their lives.1 Accordingly, the WHO characterized the virus as a pandemic (W. H. Organization, 2020). On May 27, 2020, the USA was the first to reach 100,000 cases, which doubled in every five days, and reached 1 million with a 5.8% fatality rate in the next 31 days.2 More than ten months into 2020, the world is still suffering from an extreme health crisis. Many countries extrapolated the various measures to combat the COVID-19 pandemic, which ranges from strict quarantine measures (e.g., in China and India) to painstakingly detailed contact tracing with thousands of contact tracers (e.g., South Korea and Singapore) (Lau, 2020). Today, the healthcare industry has been revolutionized from healthcare 1.0 to healthcare 4.0. Healthcare 1.0 allows hospitals to manually maintain patient medical records, leading to data duplicity and maintenance problems. In COVID-19 alike pandemic, patients may be uncertain for their diagnosis. Hospitals cannot entertain them due to the overwhelming of the patients. Thus, Healthcare 1.0 could not diagnose a large number of infected patients timely and hence inefficient. Healthcare 2.0 addresses manual data duplicity issues by replacing it with electronic data and gives doctors accessibility. However, it is more institution-centric. Several countries adopted

1 Worldometers, https://www.worldometers.info/coronavirus/ [Accessed: 11-May-2020].
2 Worldometers, https://www.worldometers.info/coronavirus/ [Accessed: 27-May-2020].
3 Worldometers, https://www.worldometers.info/coronavirus/ [Accessed: 16-June-2020].

https://doi.org/10.1016/j.jnca.2021.102975

Received 24 June 2020; Received in revised form 14 December 2020; Accepted 1 January 2021
Available online 13 January 2021
1084-8045/© 2021 Published by Elsevier Ltd.
institution-centric solutions and considered measures (such as national quarantines, lockdown, and curfew) to slow the coronavirus spread, but these measures could not control it. Despite, other drawbacks like national economic degradation has been observed. Many countries handled this burden by adopting the triage-type hierarchy to diagnose and treat the patient based on the severity (Ayebare et al., 2020).

Healthcare 3.0 was patient-centric using wearable sensors. Adopting Healthcare 3.0 industry revolution was an excellent option to tackle such a flooded problem, but it is inadequate in managing a large volume of the real-time medical record. In this crisis, we need a modern healthcare system that covers the triad of patient-centered care, public-centered care, and minimizing per capita medication costs. Favorably, with the recent emerging technologies such as wireless body area network (WBAN), cloud storage, and biomedical sensors, healthcare 4.0 about to achieve all such requirements, including tracking, diagnosing, and treatment remotely. It implements WBAN around the patient’s body, creating a communication network between biomedical wearable and/or implanted sensor and the network coordinator via a prescribed protocol (Kumar and Chand, 2020). It also addressed the large number of big-data by connecting everyone to the wearable sensors, monitors patients remotely, and detects early illness. The real-time data collected from the sensors are stored in the centralized cloud server. This centralized system is susceptible to various attacks such as single point failure, integrity, confidentiality, and availability attacks.

Blockchain is an emerging technology that has grabbed attention in industrial and academic research as its potential to enhance interoperability. Blockchain provides a trusted and immutable transaction with a distributed decentralized system, where each node holds the same functionality with an equal measure of certainty. Some blockchain techniques allows trusted third party services to store data and synchronize them in the database. However, the decentralized and efficient non-deniable system have been achieved, but both security and synchronization consideration affects the anonymity and network scalability. In healthcare, the patient has sensitive medical data, which must be secure during the transaction and only access to qualified recipients. The current healthcare system is shifted from the institution-centric to patient-centric interoperability, which is more customizable (private).

Hyperledger Fabric is one of the example of permissioned blockchain that could have a role in implementing a patient-centric interoperability healthcare system. It is an open-source distributed ledger technology (DTL) platform that endorses strong security and privacy features. Hyperledger Fabric has a novel architectural model and especially design for industrial applications such as Healthcare system. Hyperledger Fabric allows certain qualified participants to access the specific data. In order to enhance the security and privacy, numerous cryptographic methods can be utilized on the top of the layer of Hyperledger Fabric. This includes broadcast group signcryption (BGSC) (Li et al., 2018), (Huang et al., 2020) that allows any member of a group to sign and encrypt data on behalf of the group using a set of public keys and broadcast in the network without revealing the identity of the signer. Adopting BGSC in interoperability healthcare for signcryption is a better substitute to achieve authentication, integrity, and confidentiality of data simultaneously.

Contribution. In this paper, we present state-of-the-art privacy preserving patient-centered interoperability (PCI) medical data sharing system based on Hyperledger Fabric (MedHypChain). MedHypChain can be used by the patient or any healthcare entity who want to store EHR in an immutable distributed ledger to ensure data privacy and beneficial in post corona diseases also.

Our contributions can be summarized as follows.

- We propose an identity-based broadcast group signcryption (IDBGSC) scheme that guarantees to simultaneously achieve authenticity, confidentiality, unforgeability, and access control. The proposed MedHypChain uses IDBGSC that signcrypts each transaction with the client’s private key and identity of the permissioned recipient to enhance the security.
- We regularize the proposed MedHypChain to implement patient-centered interoperability (PCI) data sharing between two entities: patient and medical server, where both entities maintain two distributed ledgers: patient-proposal blockchain (created by the patient) and patient-prescription blockchain (created by the medical server).
- We define the security attack model for proposed MedHypChain and prove that the proposed MedHypChain in confidentiality secured, unforgeable, anonymous, and traceable. Besides, it achieves access control, authenticity, interoperability, and node scalability.
- Finally, we evaluate the performance of MedHypChain in three metrics: average latency time (seconds), execution time (seconds), and throughput (transaction per second) for one permissioned peer up to 10,000 transactions. We demonstrate the performance of the proposed MedHypChain by scaling the permissioned nodes up to 20. Further, we compare the MedHypChain with related blockchain-based healthcare systems in terms of time cost and communication cost.

| Characteristics of blockchain | Description | Potential to COVID-19 |
|-------------------------------|-------------|-----------------------|
| **Immutability**              | The recorded data cannot be altered or changed due to the cryptographic hash function. | During COVID-19, the medical institutions in the whole world have been flooded with many infected patients. Thus, visiting a hospital for diagnosis is very time-consuming, costly, and risky for the patient. Presently, the healthcare industry has been revolutionized from healthcare 1.0 to healthcare 4.0. In healthcare 1.0, patient medical records were maintained manually by the hospital, which leads to the data duplicacy and maintenance problem. Healthcare 2.0 addressed manual data duplicacy issues by replacing it with an electronic record and giving doctors accessibility. However, it is more institution-centric, which was later considered in healthcare 3.0. Healthcare 3.0 was patient-centric using wearable sensors, but it is inadequate in managing a large volume of the real-time medical record. Healthcare 4.0 connects everyone to the wearable sensors, monitors patients remotely, and detects early illness. To quickly access the patient’s electronic records remotely at any time, the records are stored may be located in centralized or distributed locations. As the data is accessed from the repository using a public medium, security and privacy are significant challenges. One of the concrete solutions is to adopt the blockchain. The characteristics of blockchain making it possible to overcome such security and privacy issues. |
| **Decentralized**             | It does not have any central authority for governing the network. A group of entities manages the network making it decentralized. | |
| **Distributed Ledgers**       | A shared ledger is a consensus of replicated, shared, and synchronized data distributed across multiple entities. | |
| **Consensus**                 | The consensus algorithm ensures that an agreement is achieved with minimal cost, holding transparency and integrity in the decision it makes. | |
| **Transparency**              | Due to decentralized nature, it maintains the transparent profile of every entity. Every change in the transaction is viewable. | |
| **Self-autonomy**             | Every node in the blockchain network can make transactions, store, update, and access data securely. | |
| **Anonymity**                 | Data is communicated peer to peer in a network, the node’s identity remain anonymous. | |
Table 2
Comparison of the proposed system with the existing recent blockchain based health-care systems.

| Schemes                        | Year       | Objectives                                                                 | Advantages                                                                                           | Disadvantage                                                                 |
|--------------------------------|------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Mettler et al. (Mettler, 2016) | 2016       | First adoption of blockchain in the healthcare sector                       | Explore possible goals, influences and potentials connected to healthcare technology                   | Not provide any practical architecture.                                      |
| Yue et al. (Yue et al., 2016)  | 2016       | Proposed a Healthcare Data Gateway (HGD) framework based on blockchain technology, | Allow patient to access, control, and share their data simply and securely without any risk of attack. | All types of attacks were not explored                                        |
| Azaria et al. (Azaria et al., 2016) | 2016       | Proposed blockchain-assisted medical data access and permission management system (MedRec). | Ensure confidentiality, authenticity, and data sharing                                                |                                                                             |
| Kuo et al. (Kuo et al., 2017)  | 2017       | Design secure eHealthcare system based on blockchain ledger technology       | Explore the potential challenges in biomedical/health care domains.                                   |                                                                             |
| Esposito et al. (Esposito et al., 2018) | 2018       | Discussed the efficacy of blockchain technology to ensure medical data security hosted on the cloud. | Consider the challenges in adopting blockchain in healthcare systems.                                 |                                                                             |
| Griggs et al. (Griggs et al., 2018) | 2018       | Design blockchain-based smart contracts for biomedical sensors in a WBAN.    | Offer real-time analysis and log transactions                                                         |                                                                             |
| Gordon et al. (Gordon and Catalini, 2016) | 2018       | State that blockchain can be used to transit the institution-driven to patient-driven data sharing. | Consider data access rules, data aggregation, patient identity, data liquidity and immutability.     |                                                                             |
| Wang et al. (Wang and Song, 2018) | 2018      | Proposed an attribute and identity-based encryption method to propose a health data sharing system | Ensure the traceability and integrity of data, they use smart contracts.                             | Due to complex architecture, the complexity of system is high.               |
| Guo et al. (Guo et al., 2018)  | 2018       | Presented a multi-user eHealth record management system using an attribute-based signature scheme and blockchain. | Avoids key escrow problem and collusion attacks                                                      | All types of attacks were not explored                                         |
| Vora et al. (Vora et al., 2018) | 2018       | Propose an authentication protocol using blind signature                    | Enhance the patient’s anonymity and safeguard the interests of all stakeholders.                     |                                                                             |
| Hathaliya et al. (Hathaliya et al., 2019a) | 2019      | Propose a biometric-based authentication scheme                             | Ensure secure access of the patients EHR from any location                                            | Not provide the scalability and forward secrecy                               |
| Bhattacharya et al. (Bhattacharya et al., 2019b) | 2019      | Proposed a blockchain based deep learning as a service for sharing EHR records | privacy, confidentiality, and data consistency                                                      | Not provide the scalability and forward secrecy                               |
| Hathaliya et al. (Hathaliya et al., 2019b) | 2019       | Presented a Permissioned blockchain-based healthcare architecture           | Enhance the security and privacy of the patient medical data                                         | Not resist Privileged insider attack, and scalability                         |
| Omar et al. (Al Omar et al., 2019) | 2019       | Proposed a privacy-preserving patient-centric healthcare system based on blockchain technology | Ensure pseudonymity and access control of the data to the patients                                   | Not explore the interoperability between distinct entities.                  |
| Wang et al. (Wang et al., 2019)  | 2019       | Presented a blockchain-based eHealthcare system                             | Least hardware resource utilization and high level of security protection                            | Not exploited Network scalability                                            |
| Chen et al. (Chen et al., 2019) | 2019       | Proposed a searchable encryption scheme for eHealthcare data via blockchain | Preserve integrity, traceability and anti-tampering of EHRs’ index                                   | Not analyze the scalability of the network                                    |
| Kumar et al. (Kumar and Chand, 2020) | 2020      | Proposed identity-based authenticated key agreement protocol for healthcare data in the cloud. | Under random oracle model, it achieves mutual authentication and user anonymity.                     | did not provide the scalability and forward secrecy                          |
| Tanwar et al. (Tanwar et al., 2020) | 2020       | Design an access control policy mechanism by implementing a Hyperledger-based electronic healthcare data system | Improve data accessibility between various medical service providers                                 | Not suitable for COVID-19 environment                                         |
| Kumar et al. (Kumar and Chand) | 2020       | Proposed an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme to secure data transmission | Achieve secure and efficient cloud-centric IoMT-enabled smart healthcare with public verifiability. | Not resist against privileged insider attack                                   |
| Fekih et al. (Ben Fekih and Lahami, 2020) | 2020       | Survey of the application of blockchain in healthcare domain                | Discuss the security attacks                                                                          | But did not give any practical secure model.                                 |
| Hathaliya et al. (Hathaliya and Tanwar, 2020) | 2020      | Discuss the concrete survey and analysis of state-of-the-art schemes for secure Healthcare 4.0 | Explored limitations of various secure techniques and existing challenges and future research direction | Did not give any practical secure architecture.                              |
| Hathaliya et al. (Hathaliya et al., 2020) | 2020       | Proposed a self-authenticated mobile-based healthcare system               | Achieve mutual authentication and user verification                                                  | Did not achieve access control and scalability.                             |
| Park et al. (Park et al., 2020) | 2020       | Design an efficient and secure mutual authenticated scheme for medical IoT | Preserve user privacy and secure communication                                                       | Not provide sensor stolen, privileged insider, and data masquerading attacks |
| Saha et al. (Saha et al., 2020) | 2020       | Proposed a control access mechanism for healthcare system via private blockchain | Preserve access control                                                                               | Not provide scalability and forward secrecy.                                  |
| Proposed scheme                | –          | Proposed a privacy-preserving data sharing system based on Hyperledger Fabric for the medical health care system | Easily resilient to various kind of attacks, achieve PCI solution for COVID-19 like pandemic.        | –                                                                             |

Organization. The rest of the paper is organized as follows. Section 2 provides related blockchain-based healthcare systems. Section 3 gives the background, including the internet of medical things (IoMT), blockchain, Hyperledger Fabric, and identity-based broadcast group signcryption scheme. In section 4, we provide the system definition, system architecture, and security definition. The proposed MedHypChain and its regulation in the healthcare system to overcome the COVID-19 crisis is given in Section 5. A real-time use case is demonstrated in Section 6. Section 7 provides the security proofs, performance analysis, and comparison analysis. Finally, the conclusion is given in Section 8.

2. Related work

The IoT is a network of interconnected devices where they can share
data and interact with each other, making it possible to develop a wide variety of smart applications, such as wearable devices, smart homes, healthcare, etc. IoT solutions are being deployed in healthcare industries, where it integrates with wearable devices to develop an emerging and advanced technology, known as the Internet of Medical Things (IoMT). However, it is challenged with existing heterogeneity that led to vertical silos and humiliated IoT exploration. Besides, data trustworthiness is also an essential factor to bear in mind while integrating with IoMT. In IoMT, ensuring trust, security, and privacy of the patient’s physiological data is challenging for the eHealthcare system, causing a severe health issue if data is compromised. One of the most advanced technology is the blockchain that addresses these problems by distributing data management for eHealthcare systems, which guarantees that the data remains immutable. Table 1 summarizes the characteristics of blockchain and its potential in the COVID-19 pandemic.

In this section, we discussed the existing blockchain-based healthcare schemes to secure medical data. There have been various pieces of research to strengthen the security of healthcare data. For example, in 2016, Mettler (2016) first adopted blockchain technology in the healthcare sector. However, he facilitated achievable goals, influences, and potential healthcare technology challenges but did not provide the implementation. In the same year, Yue et al. (2016) designed a blockchain-based eHealthcare system and constructed the Healthcare Data Gateway (HGD) framework based on blockchain technology that allows a patient to access, control, and share their data without any risk of attack. Azaria et al. (2016) proposed blockchain-assisted medical data access and permissioned management system (MedRec) that promises confidentiality, authenticity, and data sharing due to blockchain’s distributed nature. Kuo et al. (2017) discuss the secure eHealthcare system based on blockchain ledger technology, but they did not provide the detailed implementation.

Esposito et al. (2018) studied blockchain’s efficacy to ensure cloud-assisted medical data security. Griggs et al. (2018) proposed blockchain-based smart contracts that attempt real-time analysis and log transactions for biomedical sensors in a WBAN. The system is based on the Ethereum protocol that appropriates a permissioned blockchain to execute smart contracts, but it failed to ensure patient-centric systems’ privacy. Gordon et al. (2018) considered the medical data interoperability that demonstrates how blockchain can transit institution-driven to patient-driven data sharing. They studied the data access rules, data aggregation, patient identity, data liquidity, and immutability while integrating the blockchain in the healthcare system. Wang et al. (2018) employed an attribute-based encryption method to propose a health data sharing system. To ensure the traceability and integrity of data, they use smart contracts. Guo et al. (2018) proposed a multi-user e-health record management system using an attribute-based signature scheme and blockchain secured against key escrow problem and collusion attacks. Vora et al. (2018) proposed an authenticated key agreement protocol using a blind signature scheme that ensures the patient’s anonymity and protects all entities’ privacy. However, all kinds of attacks were not discussed. Hathaliya et al. (2019a) proposed an attribute-based authenticated protocol that guarantees secure access to patients’ EHR remotely. Nevertheless, it did not provide forward secrecy and network scalability issues. Battacharya et al. (2019) presented a blockchain-based deep learning-as-a-service for sharing medical data. However, it ensured privacy, confidentiality, and data consistency and did not provide the network scalability. Hathaliya et al. (2019b) proposed a permissioned blockchain-based healthcare architecture, which enhances the security and privacy of the patient’s EHR records. However, it is vulnerable to a privileged insider attack.

Om et al. (2019) presented a privacy-preserving patient-centric healthcare system based on blockchain technology, where they employ blockchain as storage to manage patient’s medical data. In 2019, Wang et al. (2019) presented a blockchain-based eHealthcare system employing WBAN with blockchain technology to achieve a secure and efficient solution. Chen et al. (2019) proposed a searchable encryption scheme for eHealthcare data via blockchain. They constructed a healthcare data indexing algorithm using complex logic expressions and kept it in the blockchain so that the data owner could use it to search the index. In 2020, Tanwar et al. (2020) presented an access control policy mechanism and implemented a Hyperledger-based electronic healthcare data system. These systems improve data accessibility between various medical service providers.

Recently, Kumar et al. (2020) discussed an identity-based authenticated key agreement protocol for healthcare data in the cloud, secured in a random oracle model, and achieves mutual authentication and user anonymity. In 2020, Kumar et al. (2020) proposed an escrow-free identity-based aggregated signcryption scheme for a secure and efficient cloud-centric IoT-enabled smart healthcare system with the public verifiability. Fekih et al. (2020) studied the blockchain adoption in eHealthcare, where they discussed various security attacks and challenges but did not give a practical model. Hathaliya et al. (2020) gave the concrete literature review and analysis of state-of-the-art schemes for secure Healthcare 4.0. They explored the drawbacks of various secure techniques and future research directions. Hathaliya et al. (2020) presented a self-authenticated mobile-based healthcare system. The proposed system ensures mutual authentication and user verification but not resilient to access control and network scalability. Park et al. (2020) et al. design an efficient and secure mutual authenticated scheme for medical IoT. The system preserves privacy and ensures secure data communication and but did not discuss the sensor’s stolen, insider attack, and data masquerading attacks. Saha et al. (2020) proposed an access control mechanism for the healthcare system using private blockchain but is susceptible to network scalability and forward secrecy.

This paper proposes a privacy-preserving data sharing system based on Hyperledger Fabric (permissioned blockchain) for the medical health care system. Each transaction is signcrypted via the patient’s private key and authorized entity’s public key. We adopt PBFT with an execute-order-validate mechanism for the consensus. We then regularize the proposed system to implement a patient-centered interoperability data sharing between two industrial entities: patient and Medical server. Each entity manages two ledgers: patient-proposed blockchain (created by the patient) and patient-prescripted blockchain (created by the medical server). Table 2 discussed the comparison of the proposed system with existing state-of-the-art solutions for healthcare systems.

3. Background

3.1. Internet of medical things

The eHealthcare system includes two kinds of communication protocols. The first protocol works around the human body, generally known as the wireless body area network (WBAN). It serves communication between the sensors and personal digital assistant (PDA). The second protocol serves communication between other members of the system, including internet and cloud storage. Integrating WBAN with IoT constitutes an emerging and advanced technology, the Internet of Medical Things (IoMT) (Limaye and Adegbiye, 2018). In the IoMT framework, various sensors (wearable, implanted, or off-body sensor nodes) sense the patient body and send electronic health record (EHR) to the PDA periodically. The data is passed to the cloud, medical server may be allowed to access and process the data and suggest a prescription based on the patient’s health. The widely used communication protocol in the WBAN system is IEEE 802.15.6 that is appropriate for the healthcare system. The WBAN system is sensitive due to the low-power supply. Simultaneously, it needs the least data rate, bandwidth, and frequency as data collection is quite simple, and the data transmission period is significant. The widely used communication protocol in the
WBAN system is IEEE 802.15.6 that is appropriate for the healthcare system. Also, the IEEE 802.15.6 standard supports a lightweight security scheme for the WBAN system.

### 3.2. Blockchain

Blockchain is a distributed database of records shared among all participants in the network (Crosby et al., 2016). It is a chain of blocks, each linked to the previous one, and has a set of ordered-transactions. Each transaction is verified by the consensus of a majority of the participants in the network. (Pilkington, 2016). There are different consensus protocols, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), for different types of the blockchain (i.e., public, permissioned and private) (De Angelis et al., 2018). Public blockchain allows a participant to freely involve or terminate the generation of blocks based on classical consensus protocols (e.g., PoW and PoS). The permissioned and private blockchains are maintained by a set of reliable participants (also referred to as permissioned nodes) based on traditional protocols (e.g., PBFT). Once the data is stored, it can never be modified/deleted, and so easily tracked. Bitcoin, a cryptocurrency, is one of the applications in practice that uses blockchain. Blockchain has a wide range of applications in several areas, including peer-to-peer insurance, online voting, smart contracts, and its adoption in the healthcare system is also being discussed.

### 3.3. Hyperledger fabric

Hyperledger is a permissioned distributed ledger technology designed as a supplementary security concern, as it provides the access control mechanism to individual authorized participants for specific actions (Androulakiet al., 2018). It can be accessed in multiple ways that need special permission to read, write, and access information. The fabric has a highly configurable and modular structure, versatility, and optimization for implementing a broad range of industrial applications, such as finance, healthcare, insurance, banking, and supply chain. It is implemented on modular consensus protocols, PBFT, that does not need to incentivize mining or smart contract execution. The ordering of appearing transactions ensures the consistency of each transaction. The fabric has the following components.

- **Ordering service.** It creates a consensus on given transaction orders and broadcasts block to peer.
- **Membership service provider.** It binds each entity in the network with its cryptographic identities.
- **Peer-to-peer gossip service.** It distributes the blocks, committing from ordering service to the other peers in the networks.
- **Chaincode (smart contract).** It is a smart contract (program) that runs on peers to create transactions. More precisely, it allowed users to create transactions in the network’s shared ledger and update the asset’s world state. It divides the ledger into two parts: world state and transaction log. The world state holds the current state of data, and transaction log stores the logs of transactions.
- **Consensus protocol.** Fabric uses a PBFT consensus protocol to work effectively in an asynchronous manner. In a decentralized network, PBFT achieves the consensus for the blockchain, even if some nodes are malicious, i.e., some nodes do not approve the transaction. Some faults can be tolerated without affecting the integrity of the network.
- **Channel.** A channel is a private sub-network to communicate with two or more peers for conducting private and confidential transactions.
- **Endorsement and validation policy.** It enables users to define policies for executing a chaincode. Every chaincode has an endorsement policy that defines the set of peers on a channel to execute chaincode and approve the execution response in order for the valid transaction.

### Table 3

| Notations/abbreviation | Description |
|------------------------|-------------|
| NA                     | Network administrator |
| PDA                    | Personal digital assistant |
| PP                     | Permissioned peer |
| E6CP                   | Endorsement and committing peer |
| OP                     | Ordering peer |
| TA                     | Traicking agent |
| EHR                    | Electronic health record |
| PCI                    | Patient-centered interoperability |
| MSP                    | Membership service provider |
| PBFT                   | Practical Byzantine fault tolerance |
| PoW                    | Proof-of-work |
| msk and pp             | NA’s master key and public parameters |
| add_i and pow_i        | Account address and account password of ith participants |
| RS                     | Registered identities set |
| gsk_i                  | Group private key of ith participant corresponding to RS |
| RS                    | Set identities of registered participant |
| CID                    | Channel identity |
| RW                    | Read/write policy |
| skpp                  | Private key of tracing agent |
| vrs                    | Value of version in current world state |
| sigi                  | Signature generated by ith E6CP |
| TxB                    | Transaction proposal |
| CS                    | Signcrypted transaction proposal |
| TxCR                  | Chaincrypted resulted transaction |
| TXK                   | Transaction response |

- **Commitment.** The transaction-ordered blocks must be validated by all peers on a channel and committed in channel ledger. After commitment, each transaction is either valid or invalid.

### 3.4. Identity-based group broadcast signcryption

Broadcast encryption (Li et al., 2018) enables users to encrypt the data using many public keys and distributed in the network. The only qualifier winners can decrypt the encrypted data. Group signature (Huang et al., 2020) allows any group member to sign on data on behalf of the group without revealing the signer’s identity. Identity-based broadcast group signcryption (IDBGSC) scheme achieves the advantage of both simultaneously in an identity-based environment. More precisely, the IDBGSC scheme achieves authentication, integrity, and confidentiality of data simultaneously that avoids certificate management, pre-distribution of a key, and public key management. IDBGSC scheme consists of five phases: BGSSetup, BGSReg, BGSSignc, BGSUnsignc, and BGSTrace, defined as follows.

- \((\text{pp}, \text{msk}, \text{tsk}) \rightarrow \text{BGSSetup}(1^k)\). For a security parameter \(k\), it outputs the master private key \(\text{msk}\), tracing key \(\text{tsk}\) and public parameter \(\text{pp}\), where \(\text{msk}\) and \(\text{tsk}\) is kept secret to \(\text{PKG}\) and \(\text{pp}\) is made public.
- \(\text{sk} \rightarrow \text{BGSReg}(\text{ID}_i, \text{msk}, \text{pp})\). For an identity \(\text{ID}_i\), \(\text{msk}\) and \(\text{pp}\), it outputs the group private key \(\text{sk}\) corresponding to identity \(\text{ID}_i\) and send it to user via secure channel.
- \(\text{CT} \rightarrow \text{BGSUnsignc}(m, \text{RS}, \text{sk}_{\text{pp}})\). It takes a message \(m\), public parameter \(\text{pp}\), user \(A\)’s private key \(\text{sk}_A\) and identity \(\text{ID}_A\), and a set of receiver identities set \(\text{RS} = \{\text{ID}_1, \ldots, \text{ID}_n\}\), and outputs the signcrypted text \(\text{CT}\). Now, user \(A\) will broadcast \(\text{CT}\) to the users in \(\text{RS}\).
- \(\bot / m \rightarrow \text{BGSUnsignc}(\text{CT}, \text{sk}_{\text{pp}})\). User \(B\) with identity \(\text{ID}_B \in \{\text{ID}_1, \ldots, \text{ID}_n\}\) receives the signcrypted text \(\text{CT}\), and unsigncrypts with private key \(\text{sk}_B\) to obtain message \(m\) if the received signcrypted is valid otherwise \(\bot\).
- \(\bot / \text{ID}_A \rightarrow \text{BGSTrace}(\text{CT}, \text{sk}_{\text{pp}})\). On given public parameter \(\text{pp}\), signcrypted text \(\text{CT}\), and a tracing key \(\text{sk}_{\text{ta}}\), if \(\bot \rightarrow \text{BGSUnsignc}(\text{CT}, \text{sk}_{\text{pp}})\), it return \(\bot\), otherwise, it retunes corresponding identity \(\text{ID}_A\).
4. System definitions

4.1. Abbreviations and notations

Table 3 provides the description of abbreviations and notations, which we will use throughout the paper.

4.2. Network model

The proposed system has four participants: Network Administrator (NA), Client, Personal Digital Assistant (PDA), Permissioned peer (PP), and Tracing Agent (TA).

- **NA**: It is a trusted entity registering other participants in the network. Before joining the proposed network, the Client, PDA, and PP obtains credentials (key information) from NA. Similar to MSP in Hyperledger, NA plays a sole role without managing identities of peers.
- **Client**: A client can be a user or organization who wish to use the ledger service, which owns the credential, obtained from NA for secure, anonymous, and traceable data.
- **PDA**: It is a centralized device (e.g., smartphone) that has adequate large computation power and storage but not trustworthy as it is easy for any adversary to retrieve the patient’s sensitive data by physically stealing the phone or statistically attacking on it. It can collect the data from one or more clients in a secure way, verifies it without knowing anything about data, and aggregates in its storage. Besides, it has fabric software development kit (SDK) that allows to interact with the Fabric blockchain and provides a simple API to query a data from ledger and submit transaction to a ledger.
- **PP**: It is responsible for managing, processing, and maintaining transactions. We adopt execute-order-validate architecture and the Fabric blockchain and provides a simple API to query a data from ledger and submit transaction to a ledger.
- **TA**: It is a trusted entity and is accountable for tracking the malicious behavior and revoked users. It possesses the address’s account and password (add, psw), and the private key sk corresponding to its identity ID. Also, it has an extra tracing key to accomplish its responsibility.

4.3. System component

The proposed MedHypChain model mainly consists of following algorithms: Initialization, Registration, Transaction, and Tracing, as defined below.

1. \((msk, pp)\)→**Initialization**(`1`). This algorithm will respond a public parameter pp and master key msk on given the input security parameter k.
2. \((add, psw, sk)\)→**Registration**(`msk, pp, IDi`). It gives the account address add, and account password psw, and generates a private key sk corresponding to the participant’s IDi.
3. **Transaction**: It includes five sub-algorithms:
   - \(\{\sigma, Cx, add\}\)→**TransPrl**(`data, psw, sk, RS`). It signcrypts data using the sender’s private key sk, and set of recipient identities \(RS = \{ID_1, ID_2, ..., ID_n\}\) and outputs the signcrypted data Cx.
   - \(\{0.1\}→**Endorsement**(`\sigma, Cx, add, psw`). It allows PP to unsigncrypt the transaction Cx using his private key sk, corresponding to identity IDi∈RS, validate the transaction Tx using add, sign it with its private key psw.
   - **Inspection** (`Tx`). It compares the transactions response and submit the transaction for ordering if same.
   - \(\{0.1\}\)→**Ordering**(`\sigma, Tx, add`). It verifies the signature \(\sigma\) using add, and validates the transaction using the PBFT consensus mechanism and ordering the valid transaction Tx.
   - **CommitUpdate**(`Tx`). It validate each transaction in block, update the blocks in ledger and notifying the sender.
4. **ID→****Tracing**(`sk_i, Tx`). It allows TA to trace the actual identity of any malicious transaction. It takes TA private key sk, malicious transaction Tx and outputs the user’s actual identity IDi.

4.4. Security model

We formalize the definition of security models, such as confidentiality, unforgeability, traceability, and anonymity. These are described as follows.

**Confidentiality.** The confidentiality of data ensures that the transaction and ledger cannot reveal any information about data. The proposed MedHypChain system holds confidentiality if the probabilistic polynomial time (PPT) adversary \(A = (A_1, A_2)\) has a negligible advantage in the game, defined as

\[
\text{Pr}(A) - \frac{1}{2} \leq \epsilon
\]

The game is played between the adversary A and challenger C. A runs the following queries.

- \(pp\)→**Initialization**(`1`).
- \(H_{Reg}(i, pp)\). It generates the address and private key `add, psw`) for any given query i. Additionally, it computes private key sk for any identity IDi. At last, it adds the tuple \(i, add, psw, gsk_i >\) into the list Lr and respond \(< ps, gsk_i >\).
- \(H_{Reg}(data, psw, sk, RS)\). It invoke `Tx→transaction(data, psw, gsk, RS)` on given data, sender’s group private key and account password (gsk, psw), received from Hreg queries, and identities set RS.
- \(H_{Reg}(i)\). For given a query i \(L_r\), it extract the list Lr and respond \(< add, psw, sk_i >\).
- \(H_{Reg}(i)\). For given transaction Tx and TA tracing key sk_i, it responds the signer actual identity of transaction.

**Challenge.** For given pp, Adversary A1 outputs the tuple \(< data_1, data_2, add, add, >. Picks a bit b \(\in\{0, 1\}\), execute Cx→**TransPrl**(`data_1, psw, gsk, RS`). Second adversary A2 runs above queries on given pp and Cx, and outputs b’. The adversary A wins the game if its guess is correct, that is, \(b = b’\).

**Unforgeability.** The unforgeability ensures that a forger could not forge a given signature. The proposed MedHypChain system is unforgeable, if the forger F has non-negligible advantage \(\epsilon\) to win the following game, played between forger F and challenger C.

\[
\text{Pr}(A) - \frac{1}{2} \leq \epsilon
\]

The forger runs \(H_{Reg}, H_{Reg}, H_{Reg}, H_{Reg}\) and Hq queries similar to queries given in confidentiality.

**Challenge.** After successful queries, forger F response with tuple \(< ID_2; data, Cx >\) with following restrictions:

- F does not allowed to query BGSReg on ID’ previously in IDBGS scheme.
- F does not allowed to query BGSSignc on \(< ID’; data >\) previously in IDBGS scheme.

If \(C_x\) is successfully verified on \(ID’\) then F wins the game.

**Anonymity.** The anonymity ensures that no actual identity of issuer can be revealed to the adversary. The proposed MedHypChain system is anonymous if distinguisher \(D = (D_1, D_2)\) has non-negligible \(\epsilon\) advantage in the game, defined as
Hyperledger Fabric in the following phases. Our MedHypChain is different from a machine, which starts with genesis state and incrementally runs the transaction to the final state. Our MedHypChain is different from a hyperledger blockchain system.

5.1. Overview of architecture

We propose an architecture for proposed hyperledger-based EHR sharing system.

5. MedHypChain: proposed medical healthcare based hyperledger blockchain

This section introduces the proposed system for electronic health record sharing based on the Hyperledger Fabric architecture. We first propose an architecture for proposed hyperledger-based EHR sharing system.

5.1. Overview of architecture

The proposed MedHypChain can be viewed as a transaction-based state machine, which starts with genesis state and incrementally runs the transaction to the final state. Our MedHypChain is different from Hyperledger Fabric in the following phases.

- **Consensus.** Hyperledger Fabric is a private blockchain, where network peers ensure a guaranteed ordering of transactions and validate the blocks of transactions that need to be committed to the ledger. In the proposed MedHypChain, the ledger is managed by permissioned peers: E&CP and OP. We adopt PBFT to consensus the ledger, which ensures the consistency of the set and transaction throughout the network.

- **Transaction.** In MedHypChain, each transaction is cryptographically signed using an ECDSA signature scheme. Each transaction is also secured using an identity-based broadcast group signcryption (IDBGSC) scheme. The collected data is signed by any group client’s member and only by the set of the network’s authorized nodes. The MedHypChain avoid the transaction fee but utilize gas to manage the use of resources.

- **World State.** The MedHypChain adopts a world state of Hyperledger Fabric that consists of two states. The first state has simple values: key-value and the second state has complicated values: Key-key-value. Each state has a version number, which is incremented every time the state changes. Whenever the state is updated, the version is verified to ensure that the version at the time of endorsement matched with the current states.

- **Membership service provider.** The MedHypChain adopts a Membership service provider (MSP) of Hyperledger that manages the peer’s account address, which is then used to validate the signature attached to the transaction. It allows that identity to be trusted and recognized by the rest of the network without peers’ account passwords. The NA in MedHypChain is accountable for doing this. Besides, NA also authenticates each participant and issues a private group key to the peer for group signcryption.

Our MedHypChain adopts the functionality of chaincode (smart contract) supported by Hyperledger Fabric. This chain code is programmed in a standard language such as Java and Go, running on a ledger, to encode data and the transaction instruction for modifying the data. We can use a chaincode to deploy the privacy-preserving application in MedHypChain. There are two kinds of transactions in MedHypChain, “deploy transaction” that creates a new chaincode and

\[
\Pr (A) = 1
\]

\[
\Pr (D) - \frac{1}{2} < \epsilon
\]

**Challenge.** D₁ runs H₁, H₂, H₃, H₄, and H₅ queries similar to queries given in Definition 1 except H₅. Here H₅ responds one more tracing key sk₅ and responds C₀, where \( i \in \{0, 1\} \). D₁ picks \( b \in \{0, 1\} \) and executes Trace(sk₅, C₀) that outputs ID₅. On given pp and ID₅, distinguisher D₂ runs H₀, H₁, H₂, H₃, H₄ and H₅ and outputs b. The adversary D wins the game if his guess is correct, that is, \( b = b' \).

**Traceability.** The traceability ensures that the sender’s original identity of malicious communication can be traced. The proposed MedHypChain system holds the confidentiality if there exist a traceability algorithm for tracing such that

- **pp:** Initialize(1^k)
- \( \langle \text{add}_0, \text{pw}_0, \text{sk}_0 \rangle \rightarrow \text{Register}(\text{pp}, \text{ID}_0) \)
- \( \langle \text{add}_i, \text{pw}_i, \text{sk}_i \rangle \rightarrow \text{Register}(\text{pp}, \text{ID}_i) \) where \( i \in \mathbb{L}_r \)
- \( \text{C₀} \rightarrow \text{TransPrsl}(\text{data}_0, \text{ask}_0, \text{sk}_0, \text{RS}) \) where \( \text{al}, \text{bl} \in \mathbb{L}_r \)
- \( \text{Trace}(\text{pp}, \text{C₀}) = \text{ID}_0 \)

![Fig. 1. Architecture of proposed MedHypChain system.](image-url)
“invoke transaction” that invokes an operation in the context of previously deployed chaincode.

5.2. System architecture

Here, we discuss the architecture of the proposed hyperledger-based data sharing system for healing COVID-19 situation. The proposed system consists of five participants as given in Fig. 1: Client, Personal Digital Assistant (PDA), Network Administrator (NA), Tracing Agent (TA), and Permissioned Peer. A participant with an identity ID requests NA for credentials via a membership service provider (MSP). NA registers the participant by validating his ID and issues a password to him. Each transaction is implemented on the hyperledger fabric blockchain. Each participant in the network has a distinct role and allows access to those records that they have been granted permission. A patient uses PDA, which has a client application or SDK to add records that commits the participant by validating his ID and issues a password to him.

5.3. MedHypChain: proposed hyperledger-based patient-centric medical healthcare system

Here, we construct the proposed MedHypChain system, which consists of four phases: Initialization, Registration, Transaction, and Tracing. We invoke ECDSA as the cryptographic scheme, which includes ESsetup, ERreg, ESign, and EVER, and Identity-based broadcast group signcryption, which includes BGSsetup, BGSReg, BGSSignc, BGSUnsignc, and BGSttrace.

5.3.1. Initialization

This phase first initializes the system by designing system architecture. The system to obtain the credentials, including an account address and password key (addI, pwdI) using ERreg. Given his original identity IDI and a random value rI, the participant signs them using its account password via EVER, and sends the signature σI, address addI, and identity IDI together with a random value rI to NM. On receiving a registration request (addI, IDI, rI) from the participant, NA first authenticates the user after verifying the request (σI, addI, IDI, rI) using EVER. NA then generates the user’s private key skI using BGSReg of IDBGSC and signs it to the participant. Similarly, TA and PPs obtain their private key skI and skB after registering themselves from NA, shown in Fig. 2 and Algorithm 2.

Algorithm 1

**Initialization**

| Input: security parameter k | Output: system master key msk and public parameter pp |
|-----------------------------|------------------------------------------------------|
| 1: On given security parameter k, NA runs ESsetup(k) and BGSsetup(k) to give public parameter pp and master secret key msk. | 2: NA kept secret msk. |
| 3: The public parameter pp is stored in the genesis block in order to distribute it publicly. |

Algorithm 2

**Participant’s Registration**

| Input: public parameter pp and participant’s identity IDI | Output: participant private key gskI and tracing key skI |
|-----------------------------------------------------------|-------------------------------------------------------|
| 1: Participants extract pp from genesis block | 2: (addI, pwdI) < − ERreg(pp) |
| 3: Choose random number rI and IDI | (continued on next column) |

Algorithm 2 (continued)

| 4: σI < − ESign(rI, IDI) | 5: Sends (σI, addI, IDI, rI) to NA |
|--------------------------|----------------------------------|
| 6: NA checks the parameter | |
| 7: If σI < − EVER(σI, addI, IDI, rI) | 8: gskI < − BGSRegmk((IDI, pp) |
| 9: skI < − BGSRegmk((IDI, pp) |
| 10: Sends gskI to the participant and skI to tracing agent |

5.3.2. Registration

Whenever new participants join the network, it must first register with the NM. The participant extracts the pp from the genesis block of the system to obtain the credentials, including an account address and password key (addI, pwdI) using ERreg. Given his original identity IDI and a random value rI, the participant signs them using its account password via EVER, and sends the signature σI, account address addI, and identity IDI together with a random value rI to NM. On receiving a registration request (addI, IDI, rI) from the participant, NA first authenticates the user after verifying the request (σI, addI, IDI, rI) using EVER. NA then generates the user’s private key skI using BGSReg of IDBGSC and signs it to the participant. Similarly, TA and PPs obtain their private key skI and skB after registering themselves from NA, shown in Fig. 2 and Algorithm 2.

Algorithm 3

**Transaction**

| Input: Security parameter k | Output: participant private key and tracing key |
|-----------------------------|--------------------------------------------------|
| 1: (σI, Cx.addI)←TransPrl(data, psk, skI, RS), where RS = {IDI, ID2, …, IDn} | 2: Call Endorsement() |
| 3: If 1 < − Endorsement(σI, Cx.addI, pskI) | 4: PP unsigncrypt and gives σI.Tx.addI |
| 5: Otherwise | 6: abort the process |
| 7: Call Inspection(Tx) | 8: If two transaction response are same |
| 9: Call Ordering() | 10: If 1 = − Ordering(σI, Tx.addI) |
| 11: validate Tx using PBFT | 12: ordering Tx |
| 13: Otherwise | 14: abort |
| 15: Call Commit&Update(Tx) to update the blocks in ledger | 16: notifying the sender. |

5.3.3. Transaction

Fig. 3 and Algorithm 3 show the transaction mechanism that takes place during the exchange of the patient’s EHR defined as follows.
• **Transaction Proposal.** Client is associated with multiple sensors that obtain data. The any sensor (leader) aggregates data $= \sum data_i$ and retrieves the current value of vs from the world state that is maintained by its PDA and proposes a transaction $Tx_P$ as $Tx_P = (vs + 1)\mid(data)\mid(RS)\mid(RW)\mid(CID)\midESign_{pw}(data, vs + 1)\mid(add)$. The transaction proposal $Tx_P$ is signed as a set of registered identities $RS$ and the (leader) sensor’s group private key $gsk$ via BSGCSignc and generates the signcrypted transaction proposal $Cx_P$, which is sent to PDA. The PDA sign transaction $Cx_P$ using its account password via $ESign$, and broadcasts the transaction $Cx_P$ to the E&CP for endorsing each transactions.

• **Endorsement:** The PDA receives the transaction $Cx_P$ and verifies the following requirements. E&CP with identity $ID_e \in RS$ can access signcrypted transaction $Cx_P$ by invoking the BGSUnsignc of the BSGSC scheme and check whether the transaction is valid or not. If not, it discards the transaction; otherwise, it uses its private key $gsk_e$ and set of identifier $RS$’s to unsigncrypt the signcrypted $Cx_P$ via $BSGCSignc$ and obtains the transaction $Tx_P$. It also checks the validation of the ECDSA signature via $EVerr_{add}(\sigma_i)$ and compares all transaction proposals’ responses $Tx_Ri$ to check whether they are the same. The PDA submits the transaction to the OP to update the ledger if endorsement policies have been fulfilled before submitting it. Now, the PDA broadcasts the signcrypted transaction proposals $Cx_Pi$ and responses $Tx_Ri$ with the transaction message to OP.

• **Ordering.** OP received transactions from the channels and adopts the PBFT consensus protocol for validating the transaction. To be more precise, the current leader in the protocol aggregates enough legitimate transactions for a pending block. The consensus of the block can be achieved if and only if the maximum number of malicious nodes is not greater than or equal to one-third of all the nodes in the system. Now, OP ordered them chronologically by channel by checking that the value of version is incremented by one and creates blocks of transaction per channel. OP is then passed it to the E&CP for committing the transaction.

• **Commit and Ledger Update.** The E&CP makes sure that the RW sets match the world state to validate the transactions. The validated transactions in the block ensure that the endorsement policy is fulfilled, and no modification has been done in the ledger state. Each transaction in blocks is either tagged valid or invalid. Now, E&CP appends the block to the channel’s blockchain, and the write sets are committed to the current state database for each valid transaction. Each peer passes a notification to PDA that the transaction has been committed to the current state database for each valid transaction. OP appends the block to the channel.

Fig. 3. Transaction flow of proposed MedHyPC.
append to the chain without any modification. After validation, the transaction is written to the ledger, and the world state is updated via write data from the RW set.

5.3.4. Tracing

TA, in the MedHypChain system, is accountable for tracing the user’s original identity for malicious transactions. For any illegal transaction, TA invokes BGSTrace to trace the participant and its personal information using its tracing key sk_{TA} and find the actual identity with the help of NA. Additionally, TA can further decrypt the transaction by collaboration with PP.

6. MedHypChain: real-time use case demonstration

Here, we discuss how the proposed MedHypChain regularizes the construction of a private patient-centered care blockchain network, in which, data as a transaction is accessible to authorized MS. The proposed patient-centered interoperability healthcare system consists of four participants: NA, Patient, and medical server (MS) implemented under the framework of proposed MedHypChain. The NA is the same in MedHypChain, and the patient and MS are the two organizations that maintain interoperability manages the patient EHR, record in the ledger, and shared over MedHypChain. A patient is a person who has been seen a symptom of coronavirus or a quarantined person who has a chance of disease. Each patient is surrounded by WBAN that comprises of various tiny sensors with limited battery life and storage space, installed either on or outside the patient’s body (wearable sensors) or deployed in the patient’s tissues (implanted sensors). It collects the patient’s EHR data, and due to a limited broadcast range, it stores EHR to a personal assisted device (PDA). For simplicity, we use smartphones as PDA with the same functionality as given PDA in MedHypChain, which as a network coordinator that helps WBAN to communicate with the blockchain network. The MS is a device on the medical institution, which can access the patient’s EHR and diagnose the patient’s diseases based on their resulting EHR. We provide the real-time use case of proposed MedHypChain by demonstrating three practical use-cases.

6.1. Remote diagnosis of patient in COVID-19 alike pandemic

In the first scenario, we assume that a patient is surrounded with WBAN, which includes various kinds of wearable, implanted, or off-body sensors, each of which is capable of sensing, processing, sampling, and communicating the medical signal to the recipient. Few serious symptoms found in COVID patient are breathing shortness, fever and dry cough. We consider that a patient is surrounded with the respiratory sensor, pulse oximeter and thermometer, which sense the patient’s body and obtain data, related to the breathing, oxygen level and temperature of patient on different time intervals. Any sensor (leader) aggregates the data = Σ data, and retrieves the current value of vrs from the world state that is maintained by its PDA and proposes a transaction T_{SP} as T_{SP} = (vrs + 1)||data||RS||BW||CID||ESign_{pwd}(data, vrs + 1)||addm, via Transaction proposal. The sensor sends the transaction C_{X} to the PDA, where the PDA verified the data via EVer and kept the health data in encrypted form, such that PDA could not access the data. PDA broadcasts C_{X} to E&CP for endorsing Endorsement. Now, E&CP runs Inspection and ordering algorithm to validate and ordering the transaction, if the transaction is valid, E&CP forwards the transaction to the PDA. The PDA passes the transaction to E&CP for validating the transaction via Committing transaction. After commitment, E&CP appends the block to the blockchain and notify the PDA. In this way, patient EHR is stored in the channel blockchain.

If the patient permits, MS will access the transaction from the patient-created permissioned blockchain, MS will access data and examine the EHR data based on their experience. MS will suggest a prescription Pr (which includes the instruction to the sensor to actuate as per their command) and create a transaction C_{X} using the Transaction algorithm. Similar to patients, MS will make their permissioned blockchain that is blocks of transactions. Each transaction C_{X} = (vrs + 1)||Pr||data||RS||BW||CID||ESign_{pwd}(data, vrs + 1)||addm is created under MS’s private key sk_{MS}, similar to the patient side, which consists of prescription Pr and patient’s EHR data. Accordingly, the transaction is endorsed by E&CP via Endorsement, ordered by OP via Inspection and ordering, and updated by CP via Committing in the blockchain.

6.2. Interoperability with other healthcare entity

In the scenario, a patient with corona symptoms needs to share their EHR data to the MS to diagnose remotely. MS is only allowed to access the data and suggested a prescription after analyzing the data. To maintain interoperability, each patient manages two permissioned blockchains: patient-data blockchain B_{1}, and patient-prescription blockchain B_{2}. The first blockchain B_{1} is created by the patient that contains the patient’s health-related information, such as a patient’s EHR, his identity, and the name of the physician. The blockchain B_{2} is created by the MS that contains the patient’s diagnosis-related information such as the assigned physician’s identity, EHR, and details of the prescription. Similarly, MS maintains the blockchains B_{1} and B_{2} for each patient. The MS will access the patient’s EHR if the patient allows MS to access blockchain B_{1}. It will process the data on their server and diagnose a patient remotely. On the flip side, patients via PDA will access the blockchain B_{2} and read the prescription Pr if they are allowed to access blockchain B_{1}.

6.3. Tracing of malicious transaction

In the third scenario, we suppose an adversary is attacked on any sensor, say respiratory sensor wearable on the patient body, and this malicious sensor makes an illegal transaction in the network. In order to trace such malicious participants, the patient requests the TA. TA runs the Tracing algorithm using its tracing key sk_{TA} to trace the personal information of the malicious participant.

7. Security and performance evaluation

Here, we will give the security and privacy discussion of proposed MedHypChain, and analyze the performance evaluation.

7.1. Security proof

Theorem 1. Under the assumption that the adopted IDBGSC scheme is anonymous, the proposed MedHypChain satisfies the traceability and anonymity.

Proof. Suppose there exists a PPT distinguisher D who wants to distinguish two transactions on two different identities (e.g., ID_{0}, ID_{1}) with non-negligible advantage _ε_, then there exists a B that helps D to break the anonymity of the proposed scheme. For given BGSReg and BGSSignc, B simulates the following queries run by D.

• H_{req}(i, pp). On given i^{th} query, it runs EReg to generate the account address and password (add_{i}, pwd_{i}). Additionally, it runs BGSReg to compute the private key gsk for any identity ID. At last, it adds the tuple < i, add_{i}, pwd_{i}, gsk_{i} > into the list L_{i} and respond < pwd_{i}, gsk_{i} > to D.

• H_{req}(data, pwd, sk_{i}, RS). On given transaction data, sender and receiver account address (add, addr), B runs ESign using his account password pwd_{i}, and invokes transaction (data, ps_{i}, gsk_{i}, RS) to give signcrypted transaction proposal C_{X_{i}}, signcrypted under its private key gsk_{i} and identities set RS and responds C_{X_{i}} to D.

• H_{req}(i). For given a query i<_{L_{i}}, it extract the list L_{i} and respond < add_{i}, pwd_{i}, gsk_{i} > to D.
The proposed MedHypChain scheme with advantage $\epsilon$, is with confidentiality. Therefore, the proposed MedHypChain scheme is CCA secure, the proposed MedHypChain is anonymous. Therefore, the proposed MedHypChain satisfies the confidentiality property.

Theorem 2. Under the assumption that the adopted IDBGS is IND-ID-CCA secure, the proposed MedHypChain satisfies the confidentiality property.

Proof. Suppose there exists a PPT adversary $A$ who wishes to distinguish two transactions of different data (i.e., $data_0, data_1$) with a non-negligible advantage $\epsilon$, then there must be an algorithm $B$ that helps $A$ to break the unforgeability of IDBGS scheme. On given a set of public keys, $Key$ generation queries, and unsigncryption queries, $B$ simulates the following queries by $A$.

- $H_{\text{req}}(i, pp)$. On given $i^{th}$ query, it runs $B\text{Reg}$ to generate the account address and password $(add, pwd)$. Additionally, it runs $BG\text{Reg}$ to compute the private key $gsk_i$ for any identity $ID_i$. At last, it adds the tuple $<i, add, pwd, gsk_i>$ into the list $L_i$ and respond $<pwd, gsk_i>$ to $D$.
- $H_{\text{req}}(data, psw, sk, RS)$. On given transaction data, sender and receiver account address $(add, add_r)$, $B$ runs $E\text{sign}$ using his account password $pwd$, and invokes transaction $(data, psw, gsk_i, RS)$ to sign signcrypted transaction proposal $C_{xp}$, signcrypted under its private key $gsk_i$ and identities set $RS$ and responds $C_{xp}$ to $D$.
- $H_{\text{add}}(i, L_r)$. For given a query $i \in L_r$, it extract the list $L_r$ and respond $<add, pwd, gsk_i>$ to $D$.
- $H_{\text{add}}(i, L_r)$. For given transaction $C_{xp}$ and TA tracing key $sk_{ta}$, it queries the BGSSignc to respond the actual transaction information.

After running these queries, $A$ gives the challenged to $B$ with two transferred value $(data, data_1)$ and two uncorrupted accounts $(add, add_r)$. $B$ uses the account passsword $pwd$ to obtain transaction information $C_{xp}$, where $i = \{0, 1\}$. The $B$ will get a challenge $C_{xp}$ signed under private key $gsk_i$ and it to $A$ ad obtain $A$’s guess $b_0$. Finally, $B$ consider the $b_0$ as its answer to challenge of BGSSignc scheme.

That means, $B$ has a potential to forge signature in BGSSignc scheme with advantage $\epsilon$, which contradicts that our adopted BGSSignc is forgeable. Therefore, the proposed MedHypChain scheme is unforgeable.

7.2. Security analysis

In addition to owning the above proved properties, our MedHyp-Chain also achieves some security properties.

Authenticity. Each transaction in the proposed MedHypChain is signcrypted with the sender’s Private key $sk_i$ and set of recipient identities $RS$. Further, signcrypted transaction is signed with the sender’s account password $pwd_{\text{sys}}$, ensuring the authenticity of the transaction in the blockchain.

Interoperability. In the proposed MedHypChain, the patient creates patient-data blockchain $B_1$, and MS creates patient-prescription blockchain $B_2$ on their ends. The first blockchain $B_1$ contains the patient’s health-related information, such as a patient’s EHR, identity, and physician name. The blockchain $B_2$ contains the patient’s diagnosis-related information, such as the identity of the physician assigned, EHR, and details of the prescription. Similarly, MS maintains the blockchains $B_1$ and $B_2$ for each patient. The $MS$ will access the patient EHR data if the patient allows MS to access the blockchain $B_1$.

Access control. Hyperledger fabric is a permissioned blockchain that allows only authorized participants to access the blockchain. It adopts access control in the chaincode logic that allows specific roles in an organization to access it. The proposed MedHypChain is based on the Hyperledger Fabric model. Therefore, by adopting access control in chaincode logic, the MedHypChain achieves access control.

Scalability. The consensus, in our MedHypChain, is done at the Inspection and ordering phase. The proposed system achieves better concurrency by adding more peers. The Inspection ordering phase is designed in a modular way as it supports pluggable functionality. Our proposed MedHypChain selects scalable consensus protocol, which is PBFT for the application use case.

7.3. Performance evaluation

The proposed MedHypChain architecture is supported by any identity-based broadcast group signcryption to ensure data privacy and security. Different consideration leads to variant performance results, and we consider the integration of broadcast encryption (Li et al., 2018)

Table 4

| Name         | Specifications          |
|--------------|-------------------------|
| Operating system | Window 10 Pro operating system |
| CPU          | Intel® Core™ i5-5200U  |
| Frequency    | 2.20 GHz                |
| RAM          | 8 GB                    |
| Memory       | 1 TB                    |
| Blockchain   | Hyperledger fabric v1.0 |
and group signature (Huang et al., 2020) in the identity-based environment. We realize these considerations in our laptop on a pairing-based cryptography library. We consider the Fabric v1.0 blockchain platform to implement the proposed MedHypChain and simulate the proposed MedHypChain on the personal computer with following specification, defined in Table 4. The authors have used type A pairing on elliptic curves whose length of the group order as 256 and the order of base field as 512 bits long.

The performance evaluation of MedHypChain is measured in terms of average latency time (time taken to respond to each transaction), execution time (time required to add and execute a transaction successfully), and throughput (number of successful transaction per second), by changing the transactions up to 10,000. Besides, we evaluate the scalability of proposed MedHypChain by changing the number of permissioned nodes up to 20 to measure the same metrics. We utilized the Hyperledger caliper as a benchmark tool to analyze the performance for the MedHypChain.

### Single peer performance analysis

We analyze the execution cost (seconds), latency cost (seconds), and throughput (transaction per second) for distinct functions such as query and invoke functions. The execution time of MedHypChain on distinct number of transactions has been demonstrated in Fig. 4. It has been seen that the execution time for query and invoke function increases with a large number of transactions. Likewise, the latency time for query and invoke functions for varying numbers for transactions are given in Fig. 4, where we see a noticeable change in latency, especially when the number of transactions increases from 1000 to 10,000. Besides, the throughput (tps) is illustrated in Fig. 4, where it is observed that the throughput of the invoke function is almost the same (higher) to the throughput of query function for 100 transactions.

### Scalable experiment

Now, we evaluate the node-scalability performance on the different number of permissioned peers (up to 20 nodes). We consider evaluating the node-scalability performance on the same metrics (execution cost, latency cost, and throughput) on transactions (1000 and 10,000). The results proposed MedHypChain with 20 permissioned peers can easily handle the workload of 1000 simultaneous transactions in the three metrics, while the MedHypChain with 10,000 concurrent transactions could not serve for more than 4 permissioned peers, as shown in Fig. 5.

### Cost comparison

Using the above implementation, we compare our MedHypChain with MedRec (Azaria et al., 2016), (Tanwar et al., 2020), and (Guo et al., 2018), for simply we call them MedRec, 4.0Chain, and ABSChain, respectively, in terms of time (total of execution and latency time in ms) and communication cost (in bits). We practice the realistic hypothesis from the widely used Ethereum to determine the latency time using PoW consensus is around 15 s and execute around 8 transactions per second, and Fabric (Androulaki et al., 2018) that PBFT consensus can 3500 transactions per second with clock average time is less than 1 s. We
realize to combine the consensus time into the time of cryptographic protocols, that is, ECDSA in the related scheme, and ECDSA and IDBGSC in MedHypChain. We consider a single permissioned peer, and accordingly, we get the comparative results, as shown in Fig. 6. It has been seen that the computational cost of MedRec is less than the MedRec and ABSChain, and comparable to 4.0Chain. The communication cost of MedHypChain is less than ABSChain but higher than that of MedRec and 4.0Chain. This high communication cost is due to the integration of the new IDBGSC scheme in MedHypChain, which could be optimized by selecting IDBGSC with shorter signcryption length, shown in Fig. 7.

Security comparison. We provide a high-level comparison between MedHypChain and MedRec, 4.0Chain, and ABSChain, in terms of some essential blockchain-based healthcare properties. Here, we estimate the following properties: name of blockchain, type of blockchain, node-scalability (e.g., number of permissioned peers), transaction fee, mining-reward, consensus protocol, performance-scalability (including execution, latency, and throughput), authenticity, confidentiality, unforgeability, access control, anonymity, concurrency and interoperability. We assume “Y” and “N” to mean the property achieved or not, and represent Low, Medium and High as “L,” “M” and “H,” respectively. Table 5 gives a comparison of MedHypChain with MedRec, 4.0Chain, and ABSChain, where it can be observed that the MedHypChain achieves these properties.

8. Conclusion

This paper proposed a privacy-preserving patient-centric medical healthcare data sharing system (MedHypChain) to defeat the current outbreak and post resultant disease of the COVID-19 pandemic. The proposed MedHypChain scheme is implemented over the permissioned blockchain, i.e., Hyperledger Fabric. We proposed an identity-based broadcast group signcryption to enhance the security of the proposed MedHypChain system. The signcrypted transaction is updated on the blockchain after successful ordering via PBFT as consensus protocol. The proposed MedHypChain achieves confidentiality, anonymity, traceability, and unforgeability. We implement a PCI healthcare system, where the patient’s health data is recorded in the blockchain, and only authorized node will be permitted to access. Based on the proposed MedHypChain, we have provided a real-time use case by demonstrating three practical use-cases in the COVID-19 scenario: remote diagnosis of a patient, interoperability, and malicious participant tracing. We have also analyzed its performance in three metrics and scaled up to 20 permissioned nodes. We have observed that MedHypChain can handle up to 20 permissioned nodes for concurrent 1000 transactions and 4 permissioned nodes for concurrent 10,000 transactions.

Credit author statement

Mahender Kumar: Methodology, Visualization, conceptualization writing, implementation and security analysis. Satish Chand: Supervisor, reviewing and editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Ali Omar, A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S., Rahman, M.S., 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generat. Comput. Syst. 95, 511–521.
Androulaki, E., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, pp. 1–15.
Auyebare, R.R., Flick, R., Okware, S., Bodo, B., Lamorde, M., 2020. Adoption of COVID-19 triage strategies for low-income settings. Lancet Respir. Med. 8 (4), e22.
Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30.
Ben Fekih, R., Lahami, M., 2020. Application of blockchain technology in healthcare: a comprehensive study. In: International Conference on Smart Homes and Health Telematics, pp. 268–276.
Bhattacharya, P., Tanwar, S., Bodke, U., Tyagi, S., Kumar, N., 2019. BiDaas: blockchain-based deep-learning as-a-Service in healthcare 4.0 applications. In: IEEE Trans. Netw. Sci. Eng., pp. 420–429.
Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K.R., Zhang, N., 2019. Blockchain based searchable encryption for electronic health record sharing. Future Generat. Comput. Syst. 95, 420–429.
Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., 2016. Blockchain technology: beyond bitcoin. Appl. Innov. 2 (6–10), 71.
De Angelis, S., Ainello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V., 2018. PBFT vs Proof-Of-Authority: Applying the CAP Theorem to Permissioned Blockchain. Esposti, C., De Santis, A., Tognolli, G., Chang, H., Choo, K.-K.R., Blockchain, ~2018. A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1), 31–37.
Gordon, W.J., Catalini, C., 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. 16, 224–230.
Griggs, K.N., Osipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T., 2018. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. 42 (7), 130.
Guo, R., Shi, H., Zhao, Q., Zheng, D., 2018. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records system. IEEE Access 6, 11676–11686.
Hathaliya, J.J., Tanwar, S., 2020. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput. Commun. 153, 311–335.
Hathaliya, J.J., Tanwar, S., Tyagi, S., Kumar, N., 2019a. Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. Comput. Electr. Eng. 76, 398–416.
Hathaliya, J., Sharma, P., Tanwar, S., Gupta, R., 2019b. Blockchain-based remote patient monitoring in healthcare 4.0. In: 2019 IEEE 9th International Conference on Advanced Computing (IACC), pp. 87–91.
Hathaliya, J.J., Tanwar, S., Evans, R., 2020. Securing electronic healthcare records: a mobile-based biometric authentication approach. J. Inf. Secur. Appl. 53, 102528.

Huang, J., Huang, Q., Susilo, W., 2020. Leakage-resilient group signature: definitions and constructions. Inf. Sci. 509, 119–132.

Hathaliya, J.J., Tanwar, S., Evans, R., 2020. Securing electronic healthcare records: a mobile-based biometric authentication approach. J. Inf. Secur. Appl. 53, 102528.

Huang, J., Huang, Q., Susilo, W., 2020. Leakage-resilient group signature: definitions and constructions. Inf. Sci. 509, 119–132.

M. Kumar and S. Chand, “A secure and efficient cloud-centric internet of medical things-enabled smart healthcare system with public verifiability,” IEEE Internet Things J. 2020.

Kuo, T.-T., Kim, H.-E., Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inf. Assoc. 24 (6), 1211–1220.

Kuo, T.-T., Kim, H.-E., Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inf. Assoc. 24 (6), 1211–1220.

Lau, H., et al., 2020. The positive impact of lockdown in Wuhan on containing the COVID-19 outbreak in China. J. Trans. Med. 27 (3).

Li, J., Yu, Q., Zhang, Y., 2018. Identity-based broadcast encryption with continuous leakage resilience. Inf. Sci. 429, 177–193.

Limaye, A., Adegbija, T., 2018. HERMIT: a benchmark suite for the internet of medical things. IEEE Internet Things J. 5 (5), 4212–4222.

Mehra, P., et al., 2020. COVID-19: consider cytokine storm syndromes and immunosuppression. Lancet (London, England) 395, 1033, 10229.

Mettler, M., 2016. Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), pp. 1–3.

Park, K., et al., 2020. LAKS-VNT: Provably secure and lightweight Authentication and key agreement scheme without verification table in medical internet of things. IEEE Access 8, 119387–119404.

Pilkington, M., 2016. Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations. Edward Elgar Publishing.

Remuzzi, A., Remuzzi, G., 2020. COVID-19 and Italy: what next? Lancet.

Saha, S., Sutrala, A.K., Das, A.K., Kumar, N., Rodrigues, J.I.P.C., 2020. On the design of blockchain-based access control protocol for IoT-enabled healthcare applications. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6.