Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3813841, 14 pages
https://doi.org/10.1155/2022/3813841

Research Article

BIoMT Modular Infrastructure: The Recent Challenges, Issues, and Limitations in Blockchain Hyperledger-Enabled E-Healthcare Application

Zaffar Ahmed Shaikh,[1] **Abdullah Ayub Khan**,[1,2] **Lin Teng**,[3] **Asif Ali Wagan**,[2] **and Asif Ali Laghari**[2]

[1]*Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, 75660 Sindh, Pakistan*
[2]*Department of Computer Science, Sindh Madressatul Islam University, Karachi, 74000 Sindh, Pakistan*
[3]*Department of Software Engineering, Software College, Shenyang Normal University, Shenyang, China*

Correspondence should be addressed to Abdullah Ayub Khan; abdullah.ayub@bbsul.edu.pk and Lin Teng; 1532554069@qq.com

Received 9 June 2022; Revised 18 August 2022; Accepted 30 August 2022; Published 21 September 2022

Academic Editor: Cong Pu

This paper presents a layered hierarchy that depicts the progressive relationship between data, information, knowledge, and wisdom. To begin with, data is gathered and organized into information. Information is gathered, filtered, refined, and put through an investigation process to create knowledge. Wisdom is attained after knowledge discovery through the process of filtration and aggregation through experience. The layered hierarchy in the domain of e-healthcare necessitates higher scheduling costs for data collection, processing wisdom, and management, which is also an insecure and untrustworthy process for progressive medical service. The medical industry faces a difficult problem in providing collected data integrity, information reliability, and knowledge trustworthiness for the service of progressive medical relationships in the face of an increasing number of day-to-day records. The blockchain consortium hyperledger (fabric) has been used in this paper to act as a bridge that bridges the gap between electronic data, information, knowledge, and wisdom (DIKW) movement and processes by enabling the process of the layered hierarchy of schedule information and management and providing security and transparency. For e-healthcare information management and privacy, the DIKW-ledger, such as patients' consultancy information, availing medical services, personal records, appointments, treatment details, and other health-related transactions, a consortium hyperledger fabric-enabled efficient architecture is proposed. This proposed architecture creates two networks: a public network for medical stakeholders to exchange and agree on specific medical activities before being preserved on distributed storage (read-only after record registration) and a private network for complete DIKW process scheduling and management. We designed and created smart contracts for this purpose, as well as use-case diagrams to describe the overall execution process. The proposed architectural solution provides more efficient information integrity, provenance, and storage procedures to immutably preserve the medical ledger in a permissioned hash-encrypted structure.

1. Introduction

Data is one of the fundamental elements. It could be a common denominator in which all the constraints are connected and are preserved in the centralized storage. This data is derived from information and positioned through a continuum that exactly moves towards knowledge and then wisdom [1]. Representation of data is knowledge-driven and provides distinct attributes, for example, patient name, tracking id, gender, age, cause, symptoms, and prescription. The meaning of data attributes is semantic and drives proper information and knowledge. In the next step, this contextualized information is implied. Then, it is interpreted by the interpreter from the perspective of the information receivers.

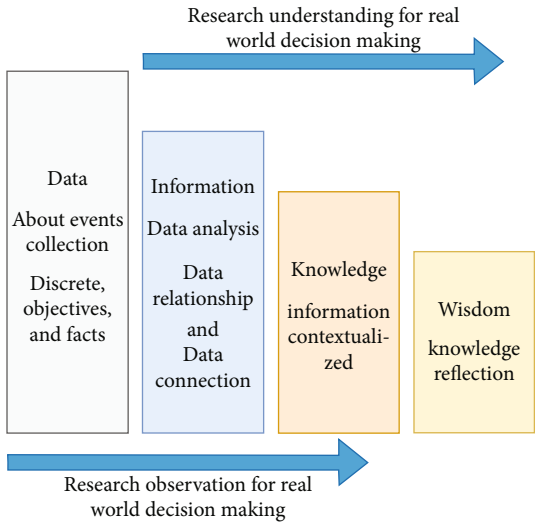

Figure 1: Current process of DIKW analysis.

After this process, the high-level knowledge states that are pertinent to wisdom are shown in Figure 1. When knowledge is truly refined and sublimated, the receiver has the potential to minimize and maximize interaction with the medical environment [2, 3].

In many cases, there is an emerging ambiguity between the definitions of information and knowledge, especially in the medical DIKW domain. The distinctness between information and knowledge may be the interpretation of users; few of them call data "information," while others call it "knowledge" [4]. To reduce equivocation, several information systems use centralized storage to preserve metadata. This recorded metadata, on the other hand, aids in the process of interpreting and transforming data into well-formed information [5]. Giant enterprises often preserve the same data in different storage structures, which creates redundancy. For instance, the process of storing information requires more time and computational power to schedule, process, organize, and store the record in the file system (storage). Moreover, this complete scenario is insecure because of the procedure of records preserved in the centralized server-based storage structure.

For every information system, the individual entity must take metadata into account when attempting to interpret data [6]. Most of the time, these additional data entities must be considered together, such as records of patients by name recorded in three different data fields in terms of first name, last name, and middle name, before the information is driven from the data. However, from the perspective of healthcare organizations, the complexity involved in accessing sensitive patient information across distinct central server-based applications and organizational boundaries is most important, yet does affect the potential cost and generate errors [7, 8].

Recently, healthcare industries have utilized different mechanisms, procedural domains, criteria of facilities, and systems that are used for processing patient data [9]. Some patients may receive healthcare services at more than one physician's consultancy affiliated with the same hospital. For instance, sometimes, patients receive medical treatment by random occurrence and sometimes as part of the medical management process [10]. Further, this happens when there is no data exchange between the connected systems (nodes), and incomplete data occurs during data exchange from different disjoint nodes because the same patients end up with two different medical records within the same e-healthcare applications [11, 12]. However, these patients' identity redundancy creates another challenging aspect in terms of data management. Moreover, data management also requires record cleanup before organizing medical processed ledgers. Additionally, record cleanup involves medical duplication data detection, examination, removal, analysis of incomplete data, correction, tuning the format of records, and preservation.

There are numerous methods and techniques proposed for e-healthcare application integration, organization, and security practitioners. To ensure the validity, authentication, and reliability of e-healthcare systems and information processing and the overall management of records [9], it is imperatively significant to maintain the transparency and privacy of the complete process of medical data, information, knowledge, and wisdom over the network. To ascertain this, the identification of shreds of sensitive medical records is critical for the record-keeping purpose of an individual transaction that occurred while analyzing the medical data [10, 11]. The complexity of hiding innumerable kinds of medical information in a carrier channel (through signals) over wireless network-based connected edge devices to exchange information. The remote medical data acquisition mechanism itself is highly vulnerable while capturing digital medical data from distinct domains of the healthcare network [12]. These medical data node transactions and information exchange layered mechanisms are deemed insecure.

For further investigation, blockchain technology has been envisioned and utilized by several industrial production systems and supply chain management to achieve provenance, integrity, and tracking to enable record storage for further investigation [13]. Most medical analysts are planning to shift from centralized to decentralized care; for this purpose, blockchain distributed technology used as a decentralized secure infrastructure protects against network attacks [14]. Usually, it is intended for server-based central systems and structures. Blockchain also enables the robust performance of distributed nodes' defense ability during the process of sharing information from one to another [15]. Security is possible because of cryptographic hash-encryption (SHA-256) functions with the installation of intrusion detection and restricted solutions. Moreover, the technology can deploy a firewall with antidisclosure techniques to guarantee the medical ledger integrity, transparency, provenance, immutability, and trustworthiness of the stored records under examination.

However, this paper discusses a secure blockchain hyperledger fabric that enables a novel medical architecture for e-healthcare information management and privacy. For this purpose, we have designed a private network infrastructure for exchanging sensitive medical information among different nodes in a protected manner (encrypted ledger)

over P2P network connectivity. This proposed medical-ledger provides overall data, information, knowledge, and wisdom of medical record provenance, track and trace, two-way protected communication, and assurance for performing all the medical-related operations. These working operations are (i) patients' registration, (ii) online medical services availing, (iii) medical alerts, (iv) physician consultancy and registration, (v) cost scheduling, (vi) payment criteria, (vii) wallet, etc. This scenario creates trust between the events while receiving the patient's medical data and preserving, examining, and interpreting the medical information. The main contributions of this paper are as follows:

(i) A blockchain consortium hyperledger network-enabled structure for medical information management and privacy is proposed

(ii) In this paper, we propose a secure process hierarchy of medical data, information, knowledge, and wisdom using blockchain-enabled serverless peer-to-peer (P2P) consortium (hybrid) network infrastructure

(iii) To automate transactions of e-healthcare, the pseudosmart contracts are designed and simulated to manage e-healthcare-related events and medical node transactions in a protected manner using the cryptographic hash-encryption (SHA-256) method. For this purpose, we create three distinct chaincodes, such as patients' device registration, new transactions and adding medical nodes, and updating the ledger

(iv) The proposed BIoMT modular medical-ledger architectural operation is simulated using an activity diagram in a permissioned private and permissionless public blockchain network

(v) Finally, we evaluate and examine the current e-healthcare applications and discuss the challenges and limitations of the proposed distributed applicational (DApp) architecture. The blockchain hyperledger fabric-enabled implementation's open issues and future directions are discussed

The remaining sections of this paper are organized as follows. In Section 2, we studied medical-related information management and privacy protection-based literature review and examine the radical impact on the previously proposed e-healthcare applications. The existing procedure of medical DIKW analysis and the communication between layered hierarchy is discussed in Section 3. In Section 4, we have presented a blockchain hyperledger fabric-enabled proposed architecture for medical DIKW management and privacy. The working operations of the proposed architecture are discussed in Section 5. Moreover, we have evaluated and analyzed the current implementation and involving challenges and limitations are addressed in the subsection (Section 5). Finally, we conclude this paper in Section 6.

2. Related Work

Blockchain technology is a decentralized database associated with the distribution chain of chronological order, the underlying system of cryptographic security. Essentially, a sequence of aligned data nodes is associated with the hash-encrypted (SHA-256) method. The individual node contains a chain of information about a specific blockchain batch of transactions over the peer-to-peer network [16]. The batch transaction is used to verify and validate the information and move to the next node (or generate a node). In the domain of medical information, each data unit can be encapsulated into a shell called a node, which creates the information-data chain-of-unit according to the defined consensus policy. However, various problems remain in the content of blockchain e-healthcare at present due to the different emphasis and development of DApp, a new way of blockchain distributed engineering in the medical environment [17].

Due to the popularity and wide use of cloud computing, medical information can be regarded as a collection. The application of distinct medical resources at different time frames in a decentralized domain reduces the cost of load [18]. The whole scenario ensures that each individual resource is independent and unique. Therefore, the distributed technology team medical resources and provides data, information, knowledge, and wisdom management with privacy. Blockchain-medical information is a new paradigm that ensures record preservation, transmission, and distributed connectivity, blockchain consensus policies, hash protection, and other information systems in the field of medical sciences [19].

Smart medical data examination and information recommendation and management based on blockchain, when combined with diverse medical data resources in different storage domains, provides organizations and data analysts with efficient identification, analysis, detection, and classification of a large number of medical records [16, 20]. The learning preferences and other activities related to medical data and wisdom are designed and recent e-healthcare assumptions are discussed in Table 1.

3. Current Process of DIKW and Clinical-Distributed Aware Technology for Usability

In this context, the concept DIKW is presented in the form of a scale that elaborates the process of moving towards increased understanding [27], as shown in Figure 2. For this reason, the process of DIKW usability in the medical domain is expressed through the applications of e-healthcare, where clinical associates with patients who are dissatisfied with the system utilization and evaluations of electronic health records. International medical standards categorize clinical trials into three main portions for the sake of usability: efficiency, effectiveness, and increased satisfaction level in terms of medical data processing, scheduling, and management [28, 29]. Include the patients' experience, historical ledger, and incorporated principles for designing clinical applications [29]. To protect patients' records' safety

Table 1: Management of medical data, information, knowledge, and wisdom, as well as blockchain security related literature reviews.

Research method	Research description	Research gaps	Similarity/difference with the proposed BIoMT
From trustworthy data to trustworthy IoT: a data collection methodology based on blockchain [21]	A data collection method based on blockchain-IoT is proposed for creating a trustworthy environment. A hyperledger fabric-enabled smart contract is designed and implemented to balance trust and privacy during the process of collection.	(i) Preprocessing issue (ii) Hybrid and complex systems' computational limitations (iii) Micro provider (iv) Data similarity-related challenges	(i) Hyperledger fabric (ii) Hash encryption (SHA-256) (iii) Permissioned, private network
MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption [22]	The authors of MedSBA presented a secure and efficient blockchain-enabled share medical records and attribute-based encryption system proposed to record and store medical data. This proposed system protects patients' privacy and allows fine-grain access control of medical services in the e-healthcare environment.	(i) PBFT consensus method (ii) Hybrid blockchain (iii) Communication and security related protocols issue (IoT/edge-enabled protocol) (iv) Patient's device registration limitation	(i) General data protection regulation (ii) Private blockchain (iii) OPNET software tool used (iv) BAN logic
A blockchain-based scheme for privacy-preserving and secure sharing of medical data [23]	The authors of this paper presented a blockchain-enabled privacy preservation scheme that enabled the secure exchange of sensitive medical information between participating stakeholders in a semitrusted cloud server. In addition, this proposed system achieves data availability between stakeholders where zero-authentication proof is employed.	(i) Hybrid communication channel (ii) Two-way authentication (iii) Cloud storage used	(i) Proxy-reencryption (ii) PBFT algorithm for transactions delivery and acknowledgement (iii) Zero-knowledge proof mechanism
Medical data sharing scheme based on attribute cryptosystem and blockchain technology [24]	A medical data sharing model based on attribute-hash-encrypted and blockchain is proposed. In this paper, the data is validated first and then preserved on an efficient storage medium (distributed). And so, reduce the possibility of irreversible modification. For this reason, the authors designed a many-to-many communication mechanism for sharing sensitive medical data between stakeholders.	(i) Data duplication issue (ii) ABS protocol (iii) Identity privacy for preservation (iv) Chosen cypher-text attack	(i) Attribute-based signature (ii) Attribute-based encryption (iii) Many-to-many communication channel
Design of a Secure Medical Data Sharing Scheme Based on Blockchain [25]	The authors of this paper proposed a blockchain-enabled authentication process for a network model of a medical cyber-physical system. This model is designed to ensure the data cannot be forged, tampered with, or untrackable.	(i) Sharing of medical big data (ii) Credibility problem (iii) Intractable challenges (iv) Bilinear mapping	(i) BAN logic (ii) Two-way authentication (iii) Permissionless network (iv) Consortium chain (v) Formal verification authentication
MEdge-chain: leveraging edge computing and blockchain for efficient medical data exchange [26]	The authors of this paper proposed a medical-ledger blockchain- (MEdge-chain-) enabled holistic framework for exploiting the integration to aggregate diverse healthcare entities. Such medical entities' scheduled processes of storage are, for example, swift first, then secure sharing, and lastly, preservation.	(i) Optimal blockchain configuration (ii) Data priority assignment challenge (iii) Limited resources (iv) Connectivity issue (v) Local healthcare service provider management (vi) Monitoring a large number of patients	(i) Delegated proof-of-stake consensus (ii) Edge-based remote monitoring (iii) Efficient data discovery (iv) Permissionless blockchain public network

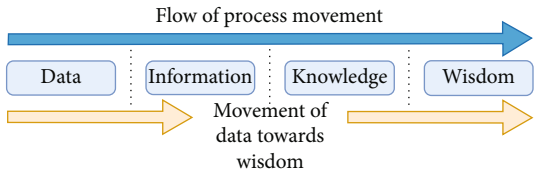

Figure 2: DIKW process movement.

and quality, the distributed system-based solution is proposed to enhance system usability, as dissatisfaction reduces and increases availability.

Still, most of the e-healthcare system relies on a centralized mechanism with a lack of security and availability. For this purpose, healthcare departments need to be concerned about the adoption of secure data, information, knowledge, and wisdom architecture as an integral component of medical information [28]. In this act, the data obtained from the system usability is evaluated by end-users (patients) and transformed into information. Whereas knowledge is the result of understanding the implications of information analysis. And so, the medical ledger of extracting wisdom is the distributed system of knowledge to enhance e-healthcare processes for clinical trials.

3.1. A Layered Hierarchy of Medical DIKW and Blockchain E-Healthcare Distributed Applications. The layered hierarchy has rigidly set building nodes in this pyramid-like structure, where the data comes first. It collects medical/clinical facts in an unorganized form, such as a number or character [30]. However, without patient context, medical data can mean little, such as a patient name, which cannot provide a complete, detailed understanding of the specific record. On the other hand, data is provided in the form of a tracking number, for example, through the patient ID "12011," which gets all the descriptions regarding the utilized medical services and their personal information as well. But the view in the context of data needs to transform the raw sequence of numbers into meaningful [31].

Information is the next node of the layer hierarchy. This is data that has been cleaned of errors and further processed in a way that makes it easier to evaluate, present, and analytically explain. To process information, the data processing mechanism involves distinct operations [32], for example, aggregation/accumulator, validation, and organizing in a way that explores the relationship between several disconnected points of data. If medical processed data/information is viewed as a description of collected objectives, facts, and discrete points, but also understood to apply it so to achieve the healthcare meta-information that helps in future investigations, it is turned into knowledge [33]. If medical processed data/information is viewed as a description of collected objectives, facts, and discrete points, but also understood to apply it so to achieve the healthcare meta-information that helps in future investigations, it is turned into knowledge [33]. This medical-related knowledge is often the edge that the healthcare sectors have over their research investigations. We uncover relationships that are not explicitly stated as information, as shown in Figure 3. However, in the domain of healthcare, wisdom is knowledge applied in action. Knowledge and wisdom are associated with what was achieved in the clinical investigation, whereas data and information are a look back in time.

To protect the layered hierarchy of healthcare DIKW, the proposed blockchain distributed ledger architecture facilitates the secure transfer of patient medical records, manages the healthcare-related supply chains, and helps e-healthcare systems/applications for privacy management. Giant organizations are adopting blockchain-healthcare technology, such as Akiri, Factom, MedicalChain, RoboMed, and Chronicled, for medical ledger integrity, transparency, provenance, immutability, and availability in a distributed nature [34, 35]. This technology keeps all the important medical data safe and secure at the moment (processing schedule dynamically). The blockchain decentralized mechanism manages all the patients' logs transparently and makes patient data available on a technology rife for security distributed applications. Substantially, blockchain does not only provide transparency; it manages medical ledgers privately, concealing the patient's identity with complex hash-based encryption and secure codes that tackle protection-related challenges and make sensitive medical records safe in the immutable storage [36, 37]. Moreover, the distributed nature of blockchain healthcare allows stakeholders to exchange the same information more quickly and efficiently.

4. Proposed Architecture for Information Management and Privacy

In this context, we proposed a distributed architecture of medical ledger management and privacy protection using a hyperledger fabric and blockchain-enabled smart contracts for secure information preservation in the immutable storage. This whole process is initiated after collection of medical data through the edge devices. One type of input that is allowed for handling real-time medical ledger management, and privacy from data to wisdom is as follows.

4.1. Fabric Endorsement and Service Orderer. The healthcare distributed ordering service (OS) starts with the application request of the medical node transactions, where the overall order in this ledger is endorsed by the connected nodes on the blockchain hyperledger fabric P2P network. The healthcare-related medical node transactions contain a unique signature (signed by each stakeholder before publishing transactions) and SHA-256 cryptographic encryption by the individual connection for committer/endorsement. This is all then submitted to the fabric orderer, where it is transmitted to the fabric commit for digital medical ledger security, shown in Figure 4. After that, the medical services are broadcast among participating stakeholders, from the orderer to the fabric committer on the blockchain network. For validation, the KAFKA verification predefined fabric mechanism for security purposed used; the defined consensus and hash reencryption are shown in Contract 1 and Figure 5.

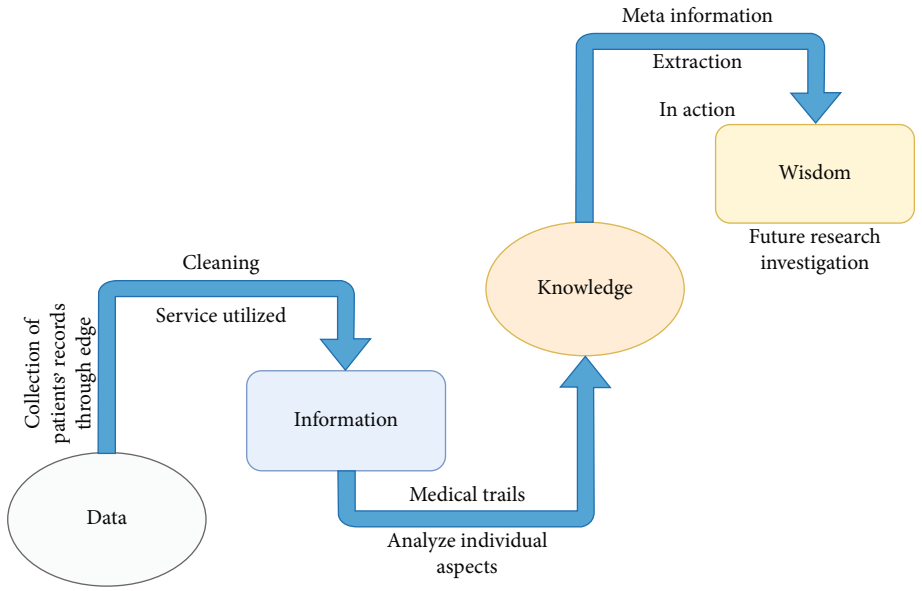

Figure 3: The layered hierarchy of DIKW in healthcare environment.

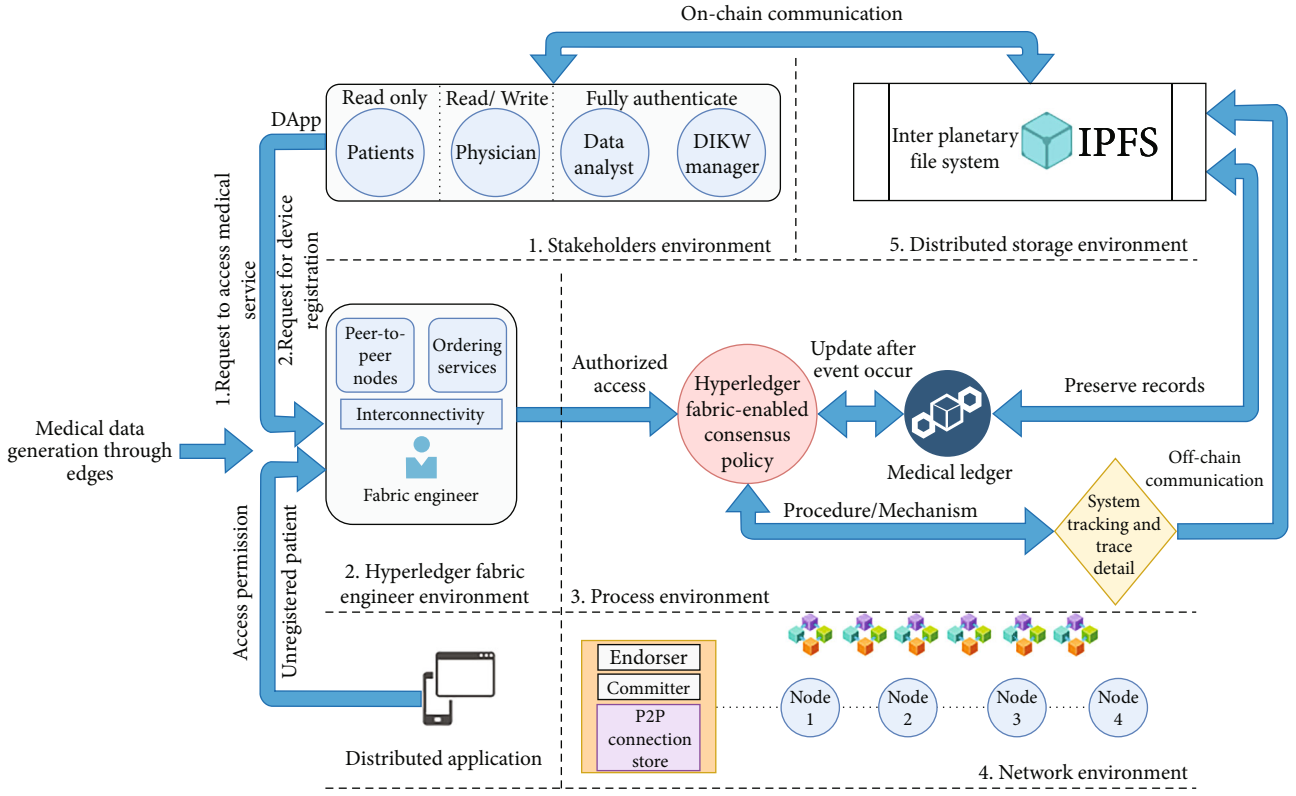

Figure 4: Proposed medical-ledger architecture for information management and privacy.

4.2. Certificate Authority of the Proposed Architecture. In the blockchain hyperledger fabric network, a certificate authority network is designed to analyze different untrusted connected stakeholders in the medical-ledger architecture, shown in Figure 4. If it has device registration and a root authenticate (participating identity), identify the stakeholders who are participating. The engineer provides certificate identity only to the participating stakeholders or requests participation after verification and validation. The healthcare system binds specific connected nodes and orders/requests. For certificate allocation, the blockchain fabric network engineer mimics all the transactions among stakeholders and is also responsible for managing overall renewal transactions, updates, and addresses. These private

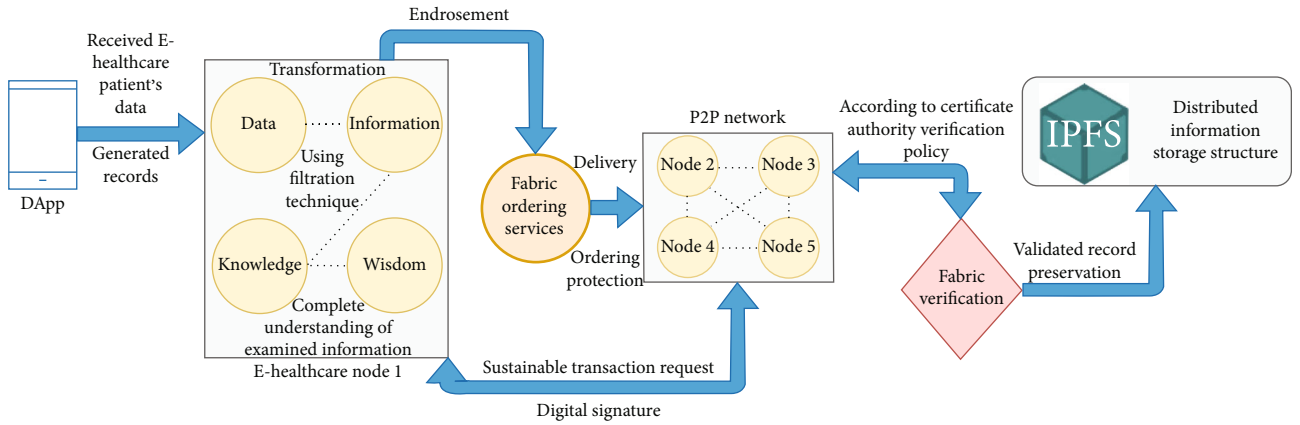

Figure 5: DIKW of e-healthcare node transaction and verification process.

on-chain and off-chain communications are singed digitally by the participating stakeholders and share private keys (for off-chain communication) to protect medical ledger management and preservation. These whole scenarios occur after the verification. It only uses the public key (on-chain communication) within the system.

4.3. Peer-to-Peer Permissioned Network (P2P). In the proposed architecture, the private network is designed to resist direct message delivery and pathway reception because of medical-ledger node transactions related to private security and integrity. The proposed medical ledger provides a strong communication channel, including transaction protection while exchange, secure stakeholders connection, and consensus workload, which is not directly accessible, so the channel can only be operated by the engineer and participating stakeholders with their registered devices. However, the execution of medical transactions is fully private and separate. This fabric network enables efficient medical transaction delivery and manages ledger maintenance as compared to other centralized systems. In this proposed network, the smart contract design protects individual transactions using a hash-based encryption mechanism and invokes specific types of node transactions execution on the secure private defined channel using blockchain protocols, as shown in Figure 5.

4.4. Distributed Nodes of Medical Transactions and Storage. The log and state execution are designed between multiple connected nodes in a private network channel. The system synchronizes automatically and runs two main objectives for managing information and security, such as committer to endorsement and endorsement to the committer. The medical node transaction request is submitted to the engineer according to the procedure of the predefined fabric endorser. As shown in Figure 4, this process is scheduled after the completion of node peering (connectivity). In this private network, blockchain distributed ledger management and storage are defined, where InterPlanetary File Storage (IPFS) is used for secure medical record preservation. IPFS is a third-party storage system that is utilized by just paying a small fee.

4.5. Smart Contracts. As shown in Contract 1 (and Figure 6), first patient device registration is required to turn on the blockchain ledger environment for the novel and secure smart contract-aware medical information management and privacy architecture. The blockchain hyperledger fabric-enabled engineer starts the system and implements the patient device registration contract (pDeviceReg()) and customized fabric stakeholders' privacy and exchange-related consensus policies designed for private device registration of individually connected stakeholders. It also records collected medical-related data such as service utilization and delivery of the healthcare application in accordance with the defined consensus, shown in Contract ((newNodeTransaction()) and (updateTransPreserve())). Furthermore, the pDeviceReg() function also stores additional records related to the medical-ledger, including device ID (dID()), patient device registration (pdReg()), patient ID (pID()), patient name (pName()), blockchain timestamp [execute], and all the activities are performed, as shown in Figure 5.

As a result, the blockchain hyperledger fabric-enabled engineer implemented and managed an automatically updated ledger for the (newNodeTransaction()) with hash-based events of node transaction protection (reEncryption()) for medical ledger privacy security, as shown in Figure 6. As well as storing medical/clinical services related to collected healthcare data, this adds new transactional details (after analysis of knowledge/wisdom) to the healthcare immutable storage for future research investigation. The function of newNodeTransaction() is created to update the medical-ledger with newly collected medical data and validate it against the daily scenario. In addition, this contract also records more details of the contract, such as patient service pService(), physician counseling (pCounseling()), new transaction (nTransaction()), updated ledger (uLedger()), blockchain timestamp [execute], and all the performed activities, shown in Contract 1.

The update ledger for immutable storage is designed and implemented to automatically update medical data whenever a new event of node transactions occurs. The updated contract function updateTransPreserve() records and evaluates the newly added details that have connected the previously-stored transactions related to medical nodes and

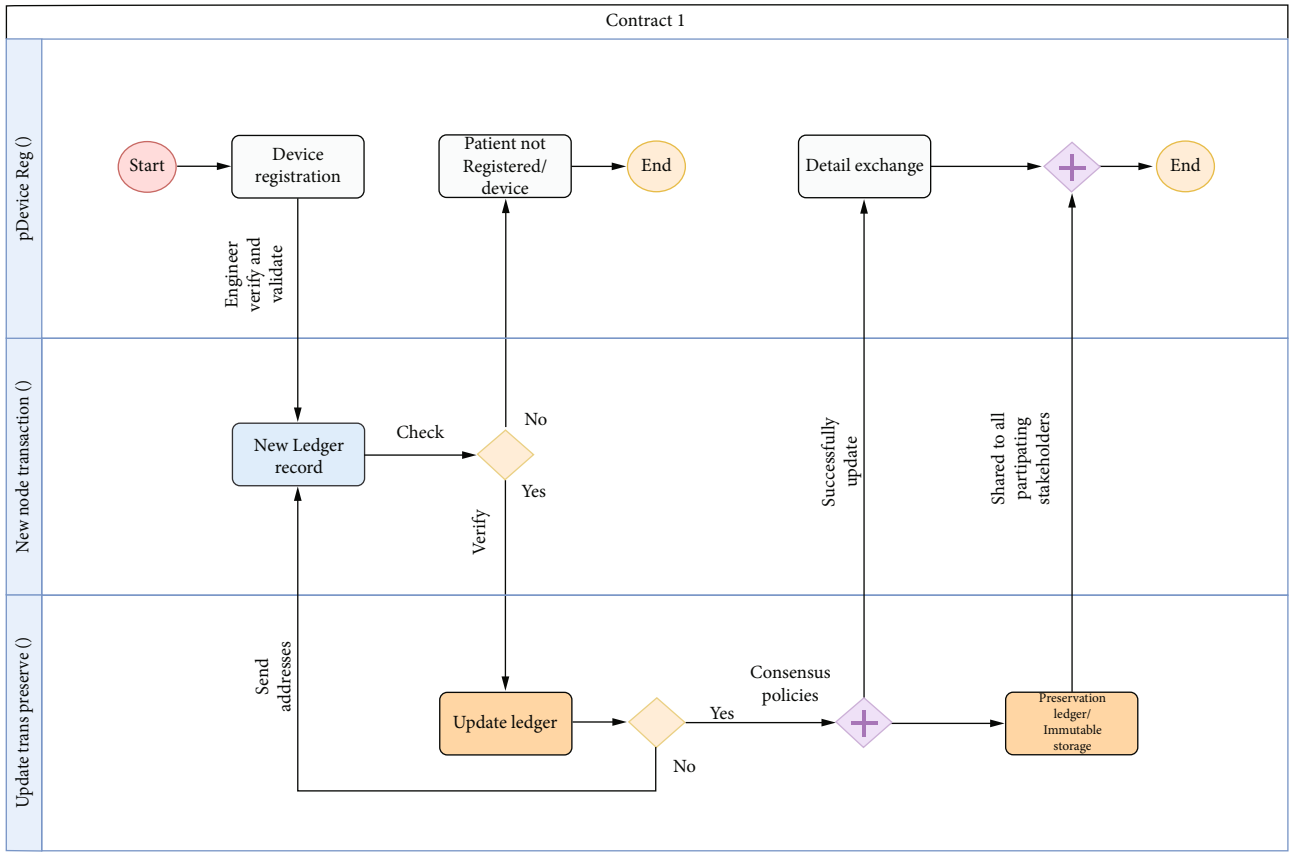

Figure 6: Operations of smart contract presented through flow of control diagram.

preservation descriptions in the distributed storage. The updateTransPreserve() contract also records the details of an updated ledger with reEncryption() to protect individual medical information, such as protecting each transaction (pETrans()), medical ledger management and privacy (mLMPrivacy()), generating hashes for individual records (gHash()), protecting storage (pStorage()), blockchain timestamp [execute], and all the activities in the immutable ledger, as shown in Appendix A (Table 2).

5. Comparison with Other State-of-the-Art Methods/Architectures/Models/ Frameworks of Healthcare

The mobile-enabled healthcare application is proposed by Khan et al.; in this paper, the authors explore several related kinds of literature and present a viewpoint regarding artificial intelligence (AI) and big data analytics [38]. The purpose is to improve the process of the mobile-based medical system and patients' transactions for utilizing e-healthcare services. The collaborative strategy of AI and big data analysis is important with respect to the source of medical data, the process of filtration for information retrieval, and create knowledge towards wisdom. The applications of the collaborative approach provide insight to the patients and enable service plans and allow patients to manage services and schedules. Medical scheduler handles cost-efficient transactions between parties based on AI and metaheuristic-enabled techniques, such as consultant and patient. However, these systems are unsecure and unprotected in nature, such as server-based medical transactions and service deliveries, public networks, and most importantly the data tampering and forgery (unauthorize access and information integrity issues).

Alotaibi presented the current status of the Indian States and updated the health system regarding the use of point-to-care devices and efficient diagnosing and highlight healthcare system impact on this pandemic (COVID-19) [39]. As compared to conventional clinical devices, point-of-care devices are provided a solution in terms of acquiring particularly clinical information with less amount of cost and managing settings of medical resources and limitations. Although there is a lot of improvement in the healthcare diagnostic. Still, the use of point-of-care devices is in its nascent phase. However, there are various state-of-the-art solutions proposed in past few years, some of them which are related to the E-healthcare DIKW process (as mentioned in Table 3) are discussed as follows.

5.1. Open Research Issues, Challenges, and Limitations. In this domain, we discuss the proposed medical information management and ledger privacy protection-related healthcare distributed application limitations and challenges. Also, we mention and explain some critical aspects of medical analysis in the existing e-healthcare systems as follows.

Table 2: Contract 1: implementation of smart contracts for medical information management and privacy.

System constraints and initialization: blockchain hyperledger fabric-enabled healthcare medical information engineer system manage (pDeviceReg())
Start e-healthcare distributed applications
Schedule addresses and manage
Preserve changes in the ledger
Data and constant: blockchain hyperledger fabric-enable engineer initiate process of edger/device registration and receive request via e-healthcare distributed applications
Activities addresses schedule accordingly
Int main():
Type.File[a.txt];
Device ID,
(dID());
Patient device registration,
(pdReg());
Patient ID,
(pID());
Patient name,
(pName());
Blockchain timestamp,
[execute];
Hyperledger fabric engineer maintain all the registration addresses,
Records validation details,
Update ledger,
Counter (each time when new event occur);
The engineer examine, analysis, verify, validate, and records all the details of patients' devices,
Responsible and authorized set of nodes;
If int main():
Type.File[a.txt] = blockchain fabric engineer (true)
Then,
If check device ID = true
Then, change state of ledger
And records additional details, device ID (dID()), patient device registration (pdReg()),
Patient ID (pID()), patient name (pName()), blockchain timestamp [execute];
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Output: edger registration edgeregister()/pDeviceReg();
System constraints and initialization: blockchain hyperledger fabric-enabled healthcare medical information engineer system manage ((newNodeTransaction()) and (updateTransPreserve()))
Start e-healthcare distributed applications
Schedule addresses and manage
Preserve changes in the ledger
Data and constant: blockchain hyperledger fabric-enable engineer initiate process of new transactions information and receive request via e-healthcare distributed applications
Activities addresses schedule accordingly
Int main ():
Type.File[a.txt];
Patient service,
(pService());
Physician counseling,
(pCounseling());
New transaction,
(nTransaction());
Update ledger,
(uLedger());
Blockchain timestamp,
[execute];
Hyperledger fabric engineer maintain all the new nodes transactions addresses,
Records verification and validation details,
Update ledger,
Counter +1 (each time when new event occur);
Engineer examines, analyses, verifies, validates, and records all the details of patients' devices,
Responsible and authorized set of nodes;
If int main():
Type.File[a.txt] = blockchain fabric engineer (true)
Then,
If check device ID = true
Then change state of ledger
And records additional details, patient service pService(), physician counseling (pCounseling()), new transaction (nTransaction()), update ledger (uLedger()), blockchain timestamp [execute];
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Output: add new nodes transactions (newNodeTransaction()); and update nodes transactions
System constraints and initialization: blockchain hyperledger fabric-enabled healthcare medical information engineer system manage (hashRecord()))
Start e-healthcare distributed applications
Schedule addresses and manage
Preserve changes in the ledger
Data: blockchain hyperledger fabric-enable engineer initiate process of hash-based re-encryption for e-healthcare distributed applications-related ledger security
Activities addresses schedule accordingly
Int main ():
Type.File[a.txt];
Protect each transaction,
(pETrans());
Medical ledger management and privacy,
(mLMPrivacy());
Generate hashes for individual record,
(gHash());
Protect storage,
(pStorage());
Blockchain timestamp,
[execute];
If int main():
Type.File[a.txt] = blockchain fabric engineer (true)
Then,
If check device ID = true

Then change state of ledger
And records additional details, protect each transaction (pETrans()), medical ledger management and privacy (mLMPrivacy()), generate hashes for individual record (gHash()), protect storage (pStorage()), blockchain timestamp [execute];
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Else
Record, maintain ledger, error generation, change state,
Traceback,
Terminate;
Output: ReEncrption (hashRecord());

5.1.1. Cross-Chain Interoperability Issue. Recently, most of the massive organizations that have large-scale data management requirements are moving to adopt blockchain hyperledger enabling technology for modular architectural solutions [44]. For this purpose, there is no specific platform specifically available and no effective protocols that achieve proper exclusivity. Interoperability issues are one of the challenging aspects. The cross-chain blockchain interoperable solution is required for designing a medical distributed enabling ecosystem. Provenance and transparency are required in the design, implementation, and deployment of blockchain hyperledger fabric-enabled medical information management and protection [45].

The restriction of node capacity in terms of size and gazette of scalability and protocols makes the e-healthcare application more reliable, such as node-time and increased security [46, 47]. Implementing a cross-chain solution that reduces transactional costs and improves communication with the fully connected network. The lack of direct connectivity between more than two distributed chains of healthcare makes interoperable communication within the ecosystem. This cross-chain technology facilitates blockchain hyperledger-enabled healthcare applications with distributed serverless transactions across different chains of nodes without involving vendor technology. Medical relays, atomic swaps, stateless server and scalability management, collaborative consensus mechanisms, and compliance for secure and protected chronological chains interconnective platforms must be considered by large healthcare sectors. Moreover, there are still some unsolved interoperable problems in the healthcare field, for example, transactional trust and the rate of bottlenecks in serverless node transactions.

5.1.2. Scope of Medical Record Privacy and Sustainability. In recent years, the healthcare system has drastically altered the environment of medical assessment and service delivery. As the system becomes digitalized, the scope of medical information and privacy has become a concerning issue because of its distinct vulnerability and the number of attacks that are increasing. For this purpose, a secure system is required for the protection of medical information to maintain patients' records, physician information, and consultant and hospital ledger preservation. Significantly, a network that stores large amounts of sensitive medical information exchanged between various medical engineers creates a forgery opportunity for information leakage and alteration [48, 49]. While the blockchain hyperledger fabric enabled distributed platform provides incentives for e-healthcare application adaptation, it also increases the associated patients' records security and privacy rights under the policy and regulation, designs the blockchain immutable structure, and deploys it for ledger preservation in a permissioned network [39, 47]. And so, it creates a new burden for engineers to tackle regulatory compliance-related issues, and private network enables intelligence verification and validation limitations and pertains to healthcare information sustainability management and challenges.

5.1.3. Sensitive Medical Information Protection and Scalability Limitations. Information concerning healthcare means sensitive personal records related to cognitive and physical health information, such as potential services of medical ledger details for physician consoling. Without getting any details, the physician cannot initiate treatment. These records need to be fully protected and cannot reveal any type of data about the patients. The types of medical information that fall under a critical category are information concerning cognitive and physical health. At the same time, handling large numbers of patients' records is a big task for cloud engineers, in which the data is continuously added to the cloud storage. To tackle such kinds of problems, we used blockchain hyperledger fabric technology that provides information integrity, transparency, provenance, immutability, and ledger scalability. Moreover, blockchain reencryption hash-based algorithms ensure the protection of medical information and also retain information confidentiality while sharing with the connected stakeholders in the private network [45, 46, 48]. However, in a permissioned private network, the fabric engineers are responsible for device registration, managing addresses of individual events and preserving all the details in the distributed storage. Dynamic management of engineer activities and smart scheduling is still an active problem in the hyperledger fabric.

5.1.4. Compliance and Policy Management Related Challenges. The various problems associated with the existing e-healthcare systems include errors in the digital medical services related transactions, such as record-keeping in centralized server-based storage and relying on cloud-based storage and related security scalability solutions [44, 49]. In addition, inappropriate and unreliable tools are used to protect medical record integrity and collect patients' transactions from portable, ubiquitous devices, and after analysis, they are submitted to the ledger storage through different network communication protocols, which is an insecure strategy.

Table 3: Comparison with other state-of-the-art proposed methods.

Other state-of-the-art methods	Research description	Research objectives and contributions	Comparison with the proposed BIoMT modular architecture
A blockchain-enabled healthcare system (HSBC) proposed for revocable attribute-based digital signature and access control [40, 41]	The highlight of this paper is (i) Proposed attribute-based signature scheme (ii) With attribute revocation (iii) For the purpose to protect the privacy of the registered patients (iv) Patient's identity in HS-BC	The main features of the proposed model are discussed as follows: (i) Security: blockchain (ii) Network: public network (iii) Ledger protection mechanism: blockchain-based predefined protection (iv) Hyperledger: no hyperledger (v) Consensus: predefined (vi) Node size: not defined (vii) Storage: cloud storage (viii) Response: not applicable (ix) Transactions executions delay: not applicable (x) User: patients	The proposed blockchain hyperledger fabric-enabled secure distributed e-healthcare architecture is designed for scheduling and managing DIKW medical processes in a protected manner. The main attributed and architectural features are defined as follows: (i) Security: blockchain-enabled privacy and security (ii) Network: consortium network structure (iii) Ledger protection mechanism: hash-based encryption (SHA-256) (iv) Hyperledger: fabric (v) Consensus: customized consensus policies (shown in contract 1) (vi) Node size: variable in between 2-4 MB (vii) Storage: IPFS (viii) Response: depend of traffic/direct (ix) Transactions executions delay: less delay (x) User: distributed e-healthcare registered patients
A secure and scalable control policy and access management for healthcare system using collaborative blockchain, IoT, and artificial intelligence techniques [41–43]	The paper discussed the collaborative nature and the impact of the current e-healthcare systems. The contribution of this paper are as follows: (i) An enhanced Bell–LaPadula is used to scalable digital ledger (ii) Dynamic access control policies developed by creating smart contracts using blockchain (iii) Provide dynamic access control and functionality (iv) Other state-of-the-art is used artificial neural network technique for classification of medical records for focusing on the personal healthcare records (v) IoT-blockchain-enabled real-time monitoring and medical diagnostic-based on four layers of data processes	The critical characteristics and attributes of the proposed model are discussed as follows: (i) Security: blockchain (ii) Network: public network (iii) Ledger protection mechanism: blockchain-based predefined protection (iv) Hyperledger: no hyperledger (v) Consensus: predefined (vi) Node size: not defined (vii) Storage: cloud storage (viii) Response: not applicable (ix) Transactions executions delay: not applicable (x) User: patients	

6. Conclusion and Future Work

This paper discusses the core concepts of data, information, knowledge, and wisdom and their management and privacy-related issues in the current e-healthcare systems using a centralized database. The layered hierarchical process of DIKW collaborates with the blockchain hyperledger fabric to secure the process of scheduling and management. One of the critical limitations is the protection of sensitive medical information through real-time distributed processing, management, and monitoring. The current scenario of information management and privacy of e-healthcare applications has gaps and challenges, including two-way authentication issues, the event of node transactions execution,

adding new or updated transactions approval, and preservation in secure storage. It is proposed to use blockchain hyperledger fabric for unified dynamic medical information management and DIKW hierarchical processing. In this paper, we have also added three different folds, which highlight the main contributions of this paper, such as the blockchain hyperledger fabric-enabled information management process. So, smart contracts are for privacy (hash-encrypted SHA-256) and preservation and an efficient blockchain P2P communication (hybrid channel). A hyperledger fabric is provided with a modular infrastructure, which enables the process of capturing data from the private channel, managing all the nodes' transactions between stakeholders, and storing medical ledgers in the IPFS distributed data storage. A detailed design of information management by a blockchain hyperledger fabric engineer is substantial, including raw medical data capture, examination to drive information, analysis of individual aspects to form knowledge, refining knowledge to present it in the form of wisdom, and storage of the ledger. We also designed and deployed chaincode (smart contracts) to secure and protect the ledger and patients' device credentials. Three contracts are created for efficient P2P communication, such as device registration (pDeviceReg()), adding new node transactions (newNodeTransaction()), and updating transactions and preservation (updateTransPreserve()). The deployment of a blockchain-enabled secure distributed DIKW architecture is becoming a necessity for the healthcare sector. The private network deals with the efficient execution of transactions, privacy, and security-related challenges of medical nodes. Furthermore, the proposed architecture maintains overall events of node integrity, provenance, transparency, and immutability and provides effective performance in information management, monitoring, and privacy. The working of events of node transactions and preservation in an action of this architecture is presented through the use case diagram. While designing the proposed BIoMT modular architecture, we highlight and separate a number of open issues that need expert concern. These become our fundamental objectives where we are expected to work in the future and provide possible solutions to the emerging issues and challenges discussed in this paper.

Data Availability

Data sharing is not applicable to this research work as no new data (simulated) were created or analyzed in this paper.

Disclosure

The sponsors have not been involved in this research work design and implementation, data collection, analysis, or decision-making related to the publication or preparation of the paper.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

A.A.K. have written original draft and preparation. A.A.K, Z.A.S., L.T., A.A.W., and A.A.L. have reviewed, rewrote, performed part of the literature survey, and edited, investigated, designed the architecture, and explored software tools. All authors of this paper read and agreed to the published version (online) of this paper.

Acknowledgments

This paper is partially funded by Lin Teng (Software Collage, Shenyang Normal University).

References

[1] Y. Duan, E. Kajan, and Z. Maamar, *Crossing "Data, Information, Knowledge, and Wisdom" Models—Challenges, Solutions, and Recommendations*, Information (Mdpi), 2022.

[2] M. Alisie, "Blockchain and the evolution of information society," *Theories of Change: Change Leadership Tools, Models and Applications for Investing in Sustainable Development*, pp. 351–374, 2021.

[3] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF)," *Neuroscience Informatics*, vol. 2, no. 1, article 100030, 2022.

[4] Z. Sardar, "The smog of ignorance: knowledge and wisdom in postnormal times," *Futures*, vol. 120, article 102554, 2020.

[5] M. Hussain, F. A. Satti, S. I. Ali et al., "Intelligent knowledge consolidation: from data to wisdom," *Knowledge-Based Systems*, vol. 234, article 107578, 2021.

[6] P. Müürsepp, "Making sense of wisdom management," *International Journal for Applied Information Management*, vol. 1, no. 2, pp. 63–69, 2021.

[7] A. A. Khan, A. A. Shaikh, O. Cheikhrouhou et al., "IMG-forensics: multimedia-enabled information hiding investigation using convolutional neural network," *IET Image Processing*, vol. 16, no. 11, pp. 2854–2862, 2022.

[8] M. Jakubik and P. Müürsepp, "From knowledge to wisdom: will wisdom management replace knowledge management?," *European Journal of Management and Business Economics*, vol. 31, no. 3, pp. 367–389, 2022.

[9] A. A. Khan, Z. A. Shaikh, L. Baitenova et al., "QoS-ledger: smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing," *Electronics*, vol. 10, no. 24, p. 3083, 2021.

[10] K. Ali, Z. A. Shaikh, A. A. Khan, and A. A. Laghari, "Multiclass skin cancer classification using EfficientNets - a first step towards preventing skin cancer," *Neuroscience Informatics*, vol. 2, no. 4, article 100034, 2022.

[11] L. Tamine and L. Goeuriot, "Semantic information retrieval on medical texts," *ACM Computing Surveys*, vol. 54, no. 7, pp. 1–38, 2022.

[12] M. G. Rhodes, K. E. Fletcher, F. Blumenfeld-Kouchner, and E. A. Jacobs, "Spanish medical interpreters' management of challenges in end of life discussions," *Patient Education and Counseling*, vol. 104, no. 8, pp. 1978–1984, 2021.

[13] V. Chang, P. Baudier, H. Zhang, X. Qianwen, J. Zhang, and M. Arami, "How Blockchain can impact financial services–

the overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, vol. 158, article 120166, 2020.

[14] U. Bodkhe, S. Tanwar, K. Parekh et al., "Blockchain for industry 4.0: a comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[15] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, article 102397, 2021.

[16] S. Liu, Y. Dai, Z. Cai, X. Pan, and C. Li, "Construction of double-precision wisdom teaching framework based on blockchain technology in cloud platform," *IEEE Access*, vol. 9, pp. 11823–11834, 2021.

[17] J. Ducrée, "Research - a blockchain of knowledge?," *Blockchain: Research and Applications*, vol. 1, no. 1-2, article 100005, 2020.

[18] R.-G. J. Pablo, D.-P. Roberto, S.-U. Victor, G.-R. Isabel, C. Paul, and O.-R. Elizabeth, "Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology," *Journal of Integrative Bioinformatics*, vol. 19, no. 1, 2022.

[19] W. Chen, "Exploration and practice of university students health education promotion model under big data information," in *EAI International Conference, BigIoT-EDU*, pp. 375–384, Cham, 2021.

[20] R. Huang, Y. Jiang, and X. Le, "Prevention and nursing research of PICC catheter-related complications in patients with digestive system malignant tumor based on smart medical block chain," *Journal of Healthcare Engineering*, vol. 2021, Article ID 5519722, 11 pages, 2021.

[21] C. A. Ardagna, R. Asal, E. Damiani, N. El Ioini, M. Elahi, and C. Pahl, "From trustworthy data to trustworthy IoT," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, pp. 1–26, 2021.

[22] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Computing*, vol. 11, no. 11, pp. 4613–4641, 2020.

[23] H. Huang, F. Peng Zhu, X. S. Xiao, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," *Computers & Security*, vol. 99, article 102010, 2020.

[24] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[25] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of Medical Systems*, vol. 44, no. 2, pp. 1–11, 2020.

[26] A. A. Abdellatif, L. Samara, A. Mohamed et al., "MEdge-chain: leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762–15775, 2021.

[27] I. Mahmood and H. Abdullah, "WisdomModel: convert data into wisdom," *Applied Computing and Informatics*, 2021.

[28] K. D. Cato, K. McGrow, and S. C. Rossetti, "Transforming clinical data into wisdom," *Nursing Management*, vol. 51, no. 11, pp. 24–30, 2020.

[29] S. Khan and M. Shaheen, "From data mining to wisdom mining," *Journal of Information Science*, 2021.

[30] D. Alvarez-Coello, D. Wilms, A. Bekan, and J. M. Gómez, "Towards a data-centric architecture in the automotive industry," *Procedia Computer Science*, vol. 181, pp. 658–663, 2021.

[31] D. Yin, X. Ming, and X. Zhang, "Understanding data-driven cyber-physical-social system (D-CPSS) using a 7C framework in social manufacturing context," *Sensors*, vol. 20, no. 18, p. 5319, 2020.

[32] Y. Yao, "Tri-level thinking: models of three-way decision," *International Journal of Machine Learning and Cybernetics*, vol. 11, no. 5, pp. 947–959, 2020.

[33] X. Peng and W. Bian, "How is data-driven precision teaching possible? From the perspective of cultivating teacher's data wisdom," *Journal of East China Normal University (Educational Sciences)*, vol. 39, no. 8, p. 45, 2021.

[34] A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: a secure degree attestation and verification traceability architecture for higher education commission," *Applied Sciences*, vol. 11, no. 22, 2021.

[35] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: a scoping review," *International Journal of Medical Informatics*, vol. 142, p. 104246, 2020.

[36] A. A. Khan, Z. A. Shaikh, A. A. Laghari, S. Bourouis, A. A. Wagan, and G. A. Ali, "Blockchain-aware distributed dynamic monitoring: a smart contract for fog-based drone management in land surface changes," *Atmosphere*, vol. 12, no. 11, p. 1525, 2021.

[37] A. A. Khan, A. A. Laghari, T. R. Gadekallu et al., "A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment," *Computers and Electrical Engineering*, vol. 102, article 108234, 2022.

[38] A. A. Khan, A. A. Laghari, D. S. Liu et al., "EPS-ledger: blockchain Hyperledger Sawtooth-enabled distributed power systems chain of operation and control node privacy and security," *Electronics*, vol. 10, no. 19, p. 2395, 2021.

[39] S. R. Alotaibi, "Applications of artificial intelligence and big data analytics in m-health: a healthcare system perspective," *Engineering*, vol. 2020, article 8894694, pp. 1–15, 2020.

[40] A. N. Konwar and V. Borse, "Current status of point-of-care diagnostic devices in the Indian healthcare system with an update on COVID-19 pandemic," *Sensors International*, vol. 1, article 100015, 2020.

[41] Q. Su, R. Zhang, R. Xue, and P. Li, "Revocable attribute-based signature for blockchain-based healthcare system," *IEEE Access*, vol. 8, pp. 127884–127896, 2020.

[42] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT: a state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," *IEEE Access*, vol. 10, pp. 78887–78898, 2022.

[43] S.-K. Kim and J.-H. Huh, "Artificial neural network blockchain techniques for healthcare system: focusing on the personal health records," *Electronics*, vol. 9, no. 5, p. 763, 2020.

[44] T. Alam, "Blockchain-enabled mobile healthcare system architecture for the real-time monitoring of the COVID-19 patients," 2021.

[45] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, "The revolution of blockchain: state-of-the-art and research challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1497–1515, 2021.

[46] N. Upadhyay, "Demystifying blockchain: a critical analysis of challenges, applications and opportunities," *International Journal of Information Management*, vol. 54, article 102120, 2020.

[47] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in internet of things," *Transactions on Emerging Telecommunications Technologies*, no. article e4621, 2022.

[48] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," in *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*, pp. 1–5, Edmonton, AB, Canada, 2019.

[49] A. D. Dwivedi, "Brisk: dynamic encryption based cipher for long term security," *Sensors*, vol. 21, no. 17, p. 5744, 2021.