SN Computer Science manuscript No.
(will be inserted by the editor)

hChain 2.0: Leveraging Blockchain and Distributed File System For EHR Management in Smart Healthcare

Musharraf N. Alruwaill * · **Saraju P. Mohanty** · **Elias Kougianos**

Received: date / Accepted: date

Abstract Within the context of the digital revolution, the domain of smart healthcare has emerged as a promising area with the aim of enhancing patient care, streamlining clinical operations, and facilitating prompt medical interventions. However, the main priority in smart healthcare revolves around the challenges of security and privacy. In addition to concerns over security and privacy, there are also other problems associated with the sharing of electronic healthcare records EHR through a robust mechanism that is both controlled and authenticated. The paper presents a proposed framework that aims to enhance security, privacy, and automation through the utilization of blockchain and IPFS technologies. Furthermore, the integration of wearable devices and deep learning techniques can be utilized to develop a risk evaluation system that facilitates fall detection and automated response, which helps with immediate medical assessment requests through a secured automated system. Integrating blockchain and IPFS provides a secure system that is cost-effective. Smart contracts provide secure and robust business logic and access control management.The integration of blockchain with IPFS offers a secure and cost-effective approach. The utilization of smart contracts enables reliable access control management and robust business logic. It provides a more restricted methods for EHR sharing such as the quantity of accesses, duration of access, and specific permissions granted.

Keywords Smart Healthcare, Blockchain, Smart Contract, Healthcare Cyber-Physical Systems (H-CPS), Deep Learning, Long Short-Term Memory (LSTM).

Musharraf N. Alruwaill (Corresponding Author)
Dept. of Computer Science and Engineering
University of North Texas, Denton, Texas, USA
E-mail: MusharrafAlruwaill@my.unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas, Denton, Texas, USA
E-mail: Saraju.Mohanty@unt.edu

Elias Kougianos
Dept. of Electrical Engineering
University of North Texas, Denton, Texas, USA
E-mail: Elias.Kougianos@unt.edu

1 Introduction

In the context of the smart city, smart healthcare is an essential and beneficial domain for urban residents [24]. As presented in Figure 1, smart healthcare utilizing emerging technologies such as Deep Learning, IoMT devices and wearable devices increases the significance of data for analyzing and predicting for improved quality of life [19]. However, medical data is sensitive and vital for comprehending the health status and making deci-sions [1]. Therefore, the security of the electronic health records EHRs must be maintained. Traditional healthcare systems can be characterized as centralized, hence giving rise to potential data security threats and challenges in effectively managing medical data [33]. In addition to the aforementioned security concerns, a lack of patient-centricity in the data poses challenges in obtaining consent for medical data access and delays in transferring such data, particularly across international borders.

Integration of technological advances into current systems can result in positive outcomes. In addition, the approach of transferring the data infrastructure from a centralized system to a decentralized system can effectively mitigate the inherent issues that arise from centralization [33, 3]. A decentralized system, such as blockchain, can enhance data security, privacy, transparency, and accessi-

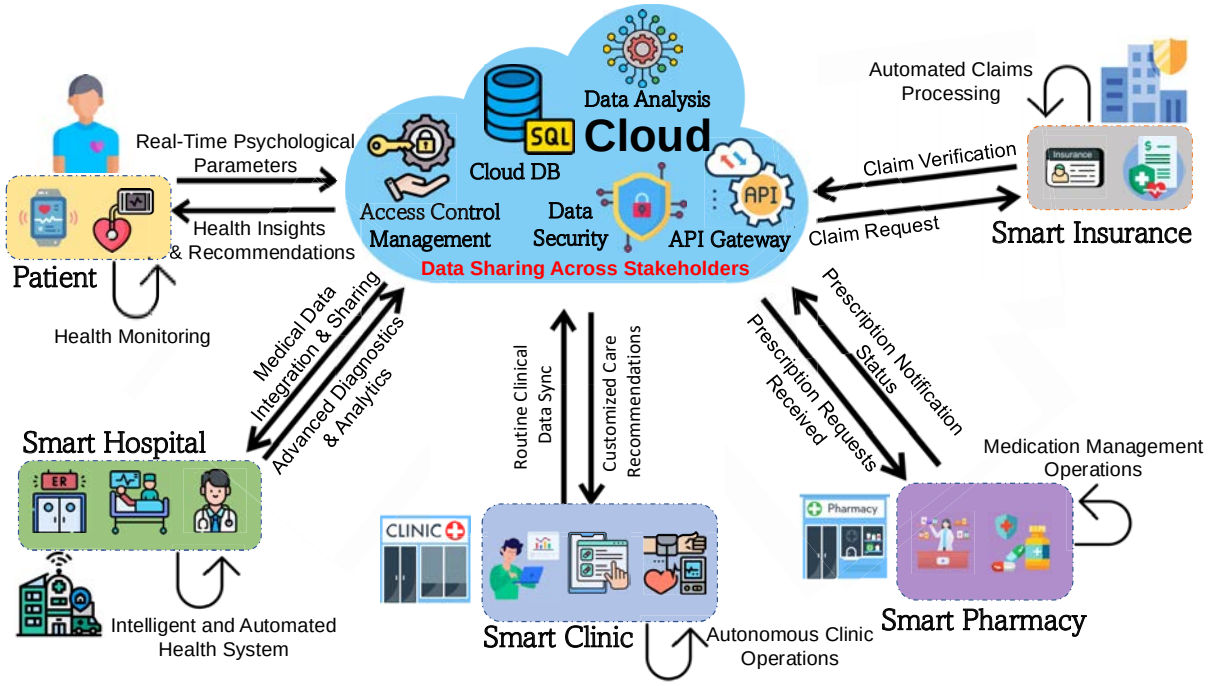

Fig. 1: Smart Healthcare

bility. Utilizing a distributed storage system may reduce the inherent storage capacity drawbacks of public blockchain architectures, thus enhancing the efficiency of storage and mitigating associated costs [15]. A distributed storage system, such as the InterPlanetary File System (IPFS), has several advantages, including enhanced resilience, fault tolerance, efficient data retrieval, and robust version control features.

1.1 IoMT Categories

The Internet of Medical Things (IoMT) is crucial in facilitating smart healthcare. The term Internet of Medical Things (IoMT) encompasses a range of medical sensors, equipment, and other devices that are interconnected over the internet [36] , as illustrated in Figure 2 . The primary objective of these devices is to gather data, store it for the purpose of data analysis, patient monitoring, and make decisions based on the processed data. IoMT devices can be classified into various categories [22].

1.1.1 Wearable Devices

These devices are wearable for the consumer to monitor physiological parameters [9]. It includes smart watches, glucose monitoring, and fitness trackers. The primary objective of using these devices is to maintain consumer health by monitoring patients in real-time and daily basis.

1.1.2 Implantable Devices

Its primary purpose is to oversee the treatment of chronic illnesses and closely monitor patients, utilizing sophisticated data analysis to prevent disease progression such as Implantable Cardioverter Defibrillators (ICDs) [7].

1.1.3 Health and Wellness Devices

Health and wellness devices are mainly for disease prevention through different devices such as smart scales and blood pressure monitoring. It focuses on tracking as a method of disease prevention.

1.1.4 Smart Medical Equipment

This IoMT devices is mainly used to enhance hospital workflow and oversee hospital equipment in order to enhance health services and real-time quality management. For instance, smart beds and remote vital signs monitoring smart infusion pumps. These interconnected gadgets enhance the overall quality of healthcare services in hospitals, and the hospital equipment operates based on pre-analyzed data.

1.1.5 Ingestible Devices

These devices are mostly utilized for two main objectives: medication and patient monitoring. They are employed for internal patient health monitoring to diagnose the patient and provide suitable treatment [18]. For instance, digestible sensors and smart pills.

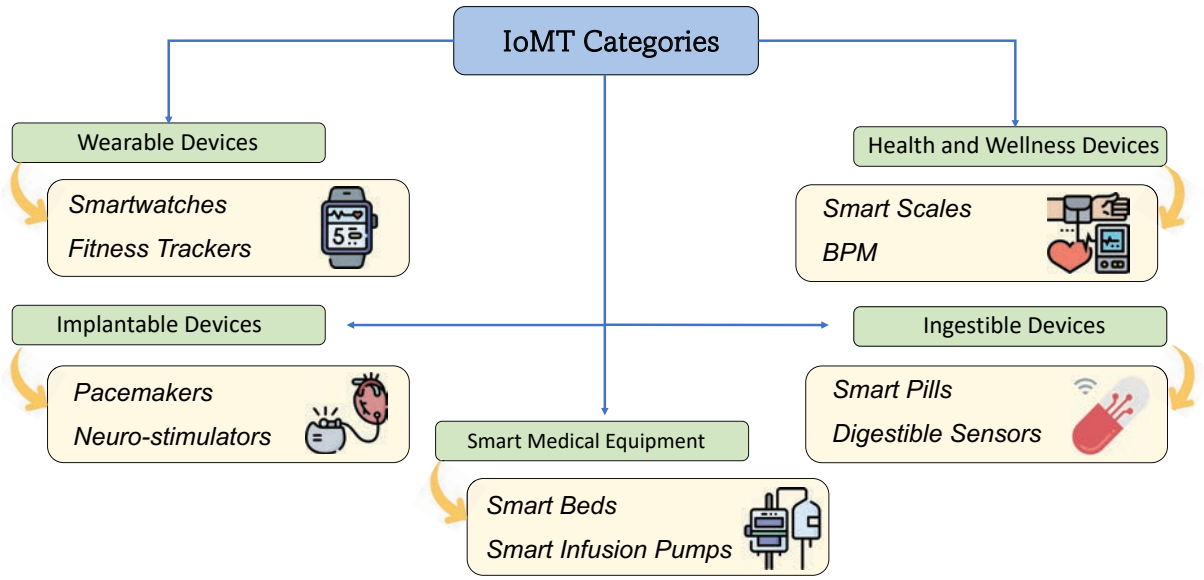

Fig. 2: IoMT Categories

1.2 The Effects of IoMT and Advanced Technologies on Smart Healthcare Innovation

The development of smart healthcare has led to the accumulation of substantial volumes of data in an ongoing manner [40]. This can be attributed to the proliferation of various technologies, such as gadgets, machine-to-machine connections (M2M), and the monitoring of systems and devices, including Internet of Medical Things (IoMT) devices and wearable devices. Hence, the utilization of artificial intelligence helps to optimize the extraction of valuable insights from data, thereby facilitating the enhancement of healthcare services and overall quality. Deep learning is a remarkable approach to data analysis, with the potential to discern various challenges and patterns that are pertinent and essential in the discipline of healthcare, such as cancer detection, disease prediction, medical imaging analysis, and patient monitoring data analysis [38]. The integration of deep learning and machine learning is of crucial significance in the advancement and efficiency of smart city ecosystems [17], specifically due to its substantial impact on the healthcare industry [25].

1.3 Contributions

The enormous volume of data generated each second presents major obstacles for existing healthcare technologies, particularly in terms of security and effective storage [8]. The proposed hChain 2.0 framework leverages public blockchain and distributed file storage to significantly enhance system-wide security and privacy, while also minimizing costs. Key contributions of the hChain 2.0 are listed below:

- **Blockchain and Distributed Storage Integration:** Utilizes a combination of blockchain technology and distributed file systems to improve data integrity, security, transparency, and privacy, while reducing storage-related costs.
- **Enhanced Data Utilization:** Capitalizes on the extensive amount of data gathered from patients to improve health outcomes and mitigate potentially fatal consequences.
- **Smart Contract:** Utilizes smart contracts to enhance the management and diversify the sharing options for Electronic Health Records (EHR). This approach provides advanced levels of access control and ensures user anonymity, offering significant improvements over traditional EHR management systems.
- **LSTM for Fall Detection:** Implements Long Short-Term Memory (LSTM) networks to handle time-series data for real-time fall detection, offering immediate assistance to solitary patients by automatically detecting falls, and facilitating urgent medical response by sharing EHR with emergency services.

1.4 Organization of The Paper

The rest of the paper is structured as follows: Section 2 reviews related works and discusses differ-ent

approaches. Section 3 delineates the novel contributions of the proposed framework, illustrating how it advances the current state of the art. Section 5 further elaborates on the innovation and uniqueness of our framework. Section 6 details the architecture and algorithms of hChain 2.0, providing comprehe-nsive details of the system's technical design. Section 8 discusses the implementation phase and includes a case study, detailing the tools utilized and the experimental results obtained. Finally, Section 9 presents the conclusion and future directions.

2 Related Prior Research

Various innovative approaches to EHR management extend beyond blockchain and fully decentralized infrastructures, offering scalable solutions. This section presents diverse techniques for EHR manag-ement, emphasizing high scalability and robust security, while also addressing the limitations of state-of-the-art proposed approaches.

2.1 EHR Management Solutions Integrating Distributed with Scalable Storage Approaches

Various techniques have been proposed to enhance EHR management through the integration of distributed technology and scalable storage solutions , as summarized in Table 1. Hybrid solutions [[30], [23], [6], [13]] integrate blockchain and cloud infrastructures to ensure data integrity, auditability, and scalability. Examples include Shaikh [30], who employs blockchain for audit trails with cloud scalability, and Mishra et al. [23], who advocate for a deletable blockchain for the management of EHRs. Cloud-based techniques [[41], [31]] emphasize the improvement of EHR security and accessibility through the application of cryptographic mechanisms. Walid et al. [41] utilize searchable encryption, whereas Shen et al. [31] present a certificateless provable data possession framework. IOTA-based products utilize the IOTA Tangle for instantaneous, cost-free data transmission. Lücking et al. [16] facilitate patient-centric management, whereas Reddi et al. [26] integrate IOTA with homomorphic encryption for secure data sharing.

2.2 Prior Related Works

A detailed comparative examination of hChain 2.0 and current frameworks is provided. Tables 2 and 3 offer insights into various aspects of these systems. Table 2 delineates essential technical elements, incl-uding blockchain platforms, data storage techniques, and smart contract functionalities. Table 3 analyzes key attributes such as IoMT support, EHR encrypti-on, and the availability of user interfaces. These tables combined illustrate the differences and simila-rities across the assessed frameworks, offering signifi-cant insights into their technical and functional characteristics.

The framework proposed by [27] proposes integrating public blockchain with IPFS in order to boost security and overcome storage restrictions inherent in blockchain technology. The author at [14] integrates blockchain and IPFS technologies in order to augment the resilience of smart contracts and maintain the integrity and traceability of data. These methods are additionally enhanced by an extra layer of authentication. [35] presented a fram-ework aimed at improving user access control man-agement by using Role-Based Access Control (RBAC) and leveraging blockchain technology to secure Electronic Health Records (EHR) while ensuring data integrity and enhancing security measures.

The paper introduces the "Fortified-Chain" system, which is a framework based on blockchain technology that ensures security and privacy in the IoMT. The system integrates blockchain technology, a Distributed Data Storage System (DDSS), and edge computing to improve security, minimize delays, and facilitate affordable data sharing. The design incorporates a Selective Ring based Access Control (SRAC) and algorithms for device authentication and patient record privacy, providing a resilient solution for decentralized IoT healthcare data mana-gement.

The proposed framework Fortified-Chain [11] employs a variety of technologies and algorithms to ensure privacy and security in constrained IoMT devices.Therefore, it maintains real-time EHR security and anonymity. The system incorporates blockchain technology and distributed data storage systems (DDSS) with edge computing to reduce delays, improve security, and reduce the costs of utilizing public blockchain. However, at the extended version Fortified-Chain 2.0 [12], the framework provides advanced access control methods and utilizes AI/ML-based contracts in place of event-based contracts. The system employs Random Forest Support Vector Machines (RFSVM) to achieve efficient real-time patient monitoring and automation system. A prop-osed automation and alert system operates by utiliz-ing data obtained from the intelligent layer to enhance healthcare services. In addition, it

Table 1: Summary of EHR Management Solutions Integrating Distributed with Scalable Storage Approaches

Technology	**Publication**	**Approach**
Hybrid	Shaikh [30]	Proposes blockchain for audit trails and data integrity with cloud storage for scalability.
	Mishra et al [23]	Combines blockchain immutability with cloud delete functionality to manage EHR.
	Arane et al [6]	Integrates blockchain and cloud to provide fine-grained access control.
	Fugkeaw et al [13]	Combines blockchain, fog, and cloud environments for optimized EHR management and adaptive load sharing.
Cloud-based	Walid et al [41]	Enhances access control for cloud-stored EHRs using searchable encryption.
	Shen et al [31]	Provides provable data possession in a cloud environment for secure EHR management.
IOTA-based	Lücking et al [16]	Utilizes IOTA Tangle for real-time, feeless transactions between healthcare stakeholders.
	Reddi et al [26]	Combines IOTA with homomorphic encryption for secure sharing of EHRs.
	Minhas et al [21]	Leverages IOTA Tangle for remote patient monitoring and telemedicine systems.
	Saweros and Song [29]	Proposes an IOTA-based system to bridge personal and electronic health records.

Table 2: Systems Devices, Security Comparing and EHR Storage Type and Format to hChain 2.0

Frameworks	Year	Tech./Blockchain	Data Storage	Smart Contract
Reza and Singh [27]	2023	Private Blockchain	On-chain & Off-chain	Storing & Sharing EHRs
Jain et al [14]	2023	Public Blockchain	On-chain & Off-chain	Storing & Sharing EHRs
Singh et al [35]	2023	Public Blockchain	On-Chain	Storing & Sharing EHRs
Singh et al [34]	2023	Cloud	Cloud	None
Sadashiv and Vachana S [28]	2022	Public Blockchain	On-chain & Off-chain	Limited Functionalities
Fortified [11]	2021	Public Blockchain	On-chain & Off-chain	Storing & Sharing EHRs
Fortified 2.0 [12]	2023	Private Blockchain	On-chain & Off-chain	Storing & Sharing EHRs
Alruwaill et al [5]	2023	Public Blockchain	On-Chain	Storing & Sharing EHRs
hChain2	2024	**Public Blockchain**	**On-chain & Off-chain**	**Numerous functionalities & EHR Sharing**

utilizes the Hyperledger fabric, which is a private blockchain, rather than the Ethereum platform.

The authors [34] propose an approach for enhancing data security, privacy, and providing anonymous authentication through the use of lightweight DNA sequence-based encryption and chaos. This method also involves securely storing the data on the cloud. In their study, the author at [28] presented up a conceptual framework that aims to address the weaknesses inherent in centralized systems by merg-ing the technologies of IPFS and blockchain. This integ-ration is intended to bolster security measures and enhance privacy protections. Furthermore, it effectively addresses the storage constraints associated with blockchain technology by leveraging the InterP-lanetary File System (IPFS). Additionally, it enhances data security by employing asymmetric encryption techniques to encrypt the information. hChain [5] proposed a secure EHR with using public blockchain and smart contract and RBAC for access control management.

The technical comparison between hChain 2.0 and existing works reveals significant distinctions. Table 2 highlights hChain 2.0's use of Ethereum blockchain with on-chain and off-chain data storage, unlike Singh et al. [34], which relies solely on cloud storage. Table 3 shows that hChain 2.0 supports IoMT integration, EHR encryption, and a user interface, setting it apart from frameworks like Reza and Singh [27]. Additionally, Table 4 emphasizes hChain 2.0's cost efficiency and advanced features such as RBAC with versatile EHR sharing and emergency response systems, which are not provided in many existing frameworks. hChain 2.0 and other Ethereum-based works, such as Jain et al. [14], utilize a public blockchain, whereas frame-

Table 3: Comparison of hChain 2.0 with Existing Frameworks on Key Features

Framework	**Year**	**Blockchain Platform**	**IoMT Support**	**EHR Encrypted**	**User Interface**
Reza and Singh [27]	2023	Hyperledger Fabric	No	NA	No
Jain et al. [14]	2023	Ethereum	No	NA	Yes
Singh et al. [35]	2023	Ethereum	No	No	No
Singh et al. [34]	2023	Cloud	Yes	Yes	No
Sadashiv and Vachana S [28]	2022	Ethereum	No	Yes	Yes
Fortified [11]	2021	Ethereum	Yes	Yes	No
Fortified 2.0 [12]	2023	Hyperledger Fabric	Yes	Yes	No
Alruwaill et al. [5]	2023	Ethereum	Yes	Yes	No
hChain 2.0	2024	Ethereum	**Yes**	**Yes**	**Yes**

Table 4: Technical Comparison of hChain 2.0 with Existing Frameworks

Frameworks	Year	Cost	Data Analysis	Access Control Management	Emergency & Response SyS
Reza and Singh [27]	2023	Very Low	No	RBAC	No
Jain et al [14]	2023	Low	No	RBAC	No
Singh et al [35]	2023	High	No	RBAC	No
Singh et al [34]	2023	Low	No	Tokenization-Based	No
Sadashiv and Vachana S [28]	2022	Very Low	No	Grant Based	No
Fortified [11]	2021	Very Low	No	Ring-based Selective Sharing	No
Fortified 2.0 [12]	2023	Very Low	Yes	SRBAC & Mutual Authentication	No
Alruwaill et al [5]	2023	High	No	RBAC	No
hChain2	2024	**Very Low**	**Yes**	**RBAC with Versatile EHR Sharing**	**Yes**

works like Reza and Singh [27] and Fortified 2.0 [12], which rely on Hyperledger Fabric, operate on a private blockchain. The consensus algorithms differ between public and private blockchains, affecting network performance. Hyperledger Fabric supports various consensus algorithms tailored for permission-ed environments, while Ethereum uses Proof of Stake (PoS), addressing the limitations of its previous Proof of Work (PoW) mechanism. Ethereum validat-ors use decentralized consensus like PoS, while Hyperledger Fabric relies on designated endorsers and orderers for transaction validation in permission-ed networks.

As compared to prior research, Chain 2.0 incorporates the integration of blockchain technology and distributed file storage systems to enhance security measures while maintaining EHR as patient-centric. Furthermore, this system enables the analysis of acceleration utilizing LSTM networks to detect instances of falls. Consequently, the alert system module may automatically share the patient's medical history through smart contract with the nearest emergency room (ER) with a high level of accuracy in detecting fall incidents.

3 Novel Contributions

3.1 Addressed Problem

There are several problems that are associated to solutions that depend on centralized systems. Furthermore, the hChain.1 framework's limitations give rise to additional concerns.

1. **Centered System Vulnerabilities**
2. **Single Point of Failure**
3. **Automated Risk Assessment**
4. **High Costs of Public Blockchain**
5. **Secured Data Sharing**
6. **Anonymity and Privacy**
7. **Data Security Challenges**

3.2 The Novelty of the Proposed Solution

The contributions of the proposed hChain 2.0 framework are outlined as follows:

1. **Decentralized Framework:** Transitioning from centralized to decentralized systems with blockchain and distributed file system technologies to address limitations such as single points of failure.
2. **Enhanced Security and Privacy:** Utilizing blockchain's immutability and decentralized fea-tures to enhance data security, ensure

user anony-mity, improve data integrity, enable transparent audits, and facilitate tamper-resistant record management.

3. **Smart Contract-Based Access Control:** Offering robust business logic for EHR sharing, including access types such as duration-based and expiration-based rights, role-based access control, quantity-based access control, and emergency override mechanisms for critical scenarios.
4. **Cost-Effective Solution:** Achieving cost-effectiveness by utilizing IPFS for off-chain storage of large data, thereby reducing the storage load on the blockchain and lowering associated operational expenses.
5. **Risk Assessment and Automated Response:** Leveraging deep learning techniques for fall detection to facilitate automated medical assistance, ensure rapid intervention, and enable secure data transmission to emergency services during critical scenarios.

4 Blockchain Technology

Blockchain technology is a type of distributed ledger technology that has garnered attention for its robustness in the field of cryptocurrencies, such as Bitcoin. It is composed of a sequence of blocks, with each block being linked to the preceding block via its hash value [39]. Every block comprises many verified transactions, as one of the objectives of the consensus algorithm is to maintain agreement between parties and ensure a single truth to be stored. Every transac-tion is verified in a decentralized manner as each miner or validator authenticates the transaction. Therefore, it relies on a decentralized system to ensure validity in an untrustworthy environment. Blockchain can be applied to various fields, including healthcare, agriculture, finance, and insurance. Figure 3 depicts the transaction flow in a straightforward manner. The consensus algorithm is a crucial compo-nent of blockchain, and there are a wide variety of existing consensus algorithms. The following subsections will examine the most widely recognized consensus algorithms, followed by a clarification of different types of blockchains.

4.1 Consensus algorithm

The primary objective of the consensus algorithm is to reach consensus among the participants of the network and then provide authenticated data through different cryptographic techniques and blockchain components [39]. Consensus algorithm helps to ensure the maintenance of an identical and synchronized records among all participants in the blockchain network and prevent double spending through several process such as transaction validation, block validation and creation across all nodes in decentralized manner as depicted in Figure 3. There are several consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), actical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA). Bitcoin uses PoW due to its high security level, but it requires a huge amount of computation power, so that makes it unsuitable for other application domains. Ethereum blockchain transitions from PoW to PoS to overcome PoW issues, the most important of which is waste computation power. Hyperledger Fabric is a private blockchain that utilizes the PBFT consensus algorithm due to its ability to enhance scalability. Due to the nature of being a private blockchain, the network participants are well-known. Each consensus method has advantages and drawbacks, with the main goal of prioritizing scalability, security, or energy efficiency.

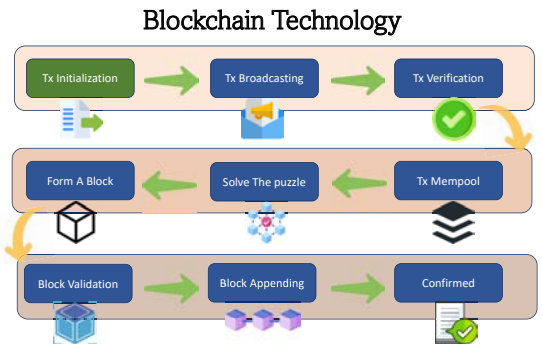

Fig. 3: Transaction Flow

4.2 Smart Contract

A smart contract is a self-executing code that has pre-defined rules and is deployed to the blockchain as a transaction, but it is a different transaction than transferring from one account to another. The transaction payload contains code written in a programming language such as Solidity. The transaction is payable due to the gas consumption. Once deployed, the smart contract becomes immutable to maintain the agreements unchanged.

4.3 Blockchain Types

Blockchain technology can be classified into several categories based on its level of openness, including

public blockchain, private blockchain, and consortium blockchain [5]. Each participant has certain privileges associated with them. The following will discuss the primary distinctions between each of them, accompanied by examples.

4.3.1 Public Blockchain

A public blockchain is a decentralized network that enables all parties to be a part of the blockchain and be of any node type without limitation of privilege. Hence, it is regarded as a completely decentralized network due to its unrestricted accessibility to all participants. The Ethereum blockchain and Bitcoin are remarkable examples of public blockchains. Its decentralized system makes it more secure compared to other types of blockchains. Nevertheless, it is plagued by scalability challenges.

4.3.2 Private Blockchain

A private blockchain is administered and authorized by a single entity, with network participants being selected as members through invitation. Each participant is assigned distinct privileges. The key advantages of a private blockchain lie in its network architecture and workflow, which offer enhanced privacy and scalability. Nevertheless, the network is highly restricted and Hyperledger Fabric is an outstanding example of a private blockchain.

4.3.3 Consortium Blockchain

A consortium blockchain, neither an entirely decentralized network or a highly restricted network, lies in between. It is governed by multiple entities and possesses a combination of public and private privileges. A consortium blockchain offers various benefits, including enhanced scalability and a lower security risk compared to private blockchains, due to the network control maintained among multiple organizations. Quorum is a well known example of a consortium blockchain.

4.4 Blockchain Innovation in Electronic Health Records Management

The inherent characteristics of blockchain technology allow for a unique and innovative approach to managing EHR, such as decentralization, highly secure mechanisms, transparency, immutability, and integrity. The nature of blockchain several issues in traditional healthcare, such as accessibility, patient-centricity, and integrity [42]. These challenges are crucial in smart healthcare, as it incorporates characteristics that ensure high-quality medical services by implementing advanced data security mechanisms due to the data integrity that is provided by blockchain technology. Hence, blockchain technology has the potential to enhance the management of EHR and establish a secure framework to facilitate interactions between various entities in the field of smart health-care, including healthcare insurance providers, pati-ents, and hospitals, by means of smart contracts.

Additionally, it significantly improves patient-centricity as the data is owned by the patient rather than the healthcare providers. Consequently, the patient has the ability to share their EHRs to various healthcare providers and hospitals without physical or electronic data transfers. These advantages of implementing blockchain technology as an data infrastructure management can enhance overall smart healthcare security, reliability, and availability. These factors are crucial for incorporating advanced constraint devices, such as IoMT devices.

5 A Novel hChain 2.0

5.1 Framework Components

5.1.1 Blockchain Technology

Blockchain technology transitions the system architecture from a centralized to a decentralized nature while providing robust, secure mechanisms such as immutability and transparency [2]. hChain 2.0 uses blockchain to ensure the data immutability, availability and transparency. Due to their sensitivity and high risk once altered, EHRs are collected and hashed through the hash algorithm SHA-256 and stored on the blockchain.

5.1.2 Smart Contract

A smart contract is a transaction that deploys self-executed business logic that defines rules that are written on solidity on the blockchain [37]. hChain 2.0 uses Solidity to define the rules, access control management mechanisms, and deploy them on the Goerli Test net. hChain 2.0 utilizes smart contracts to facilitate several forms of data access, including access count, granted access, and time-based access. Furthermore, it effectively maintains and arranges each medical record within a patient HashMap, facilitating enhanced inquiry and analysis capabilities.

5.1.3 Distributed Storage System

A distributed storage system is based on a P2P storage mechanism that maintains the data in a

secure manner and provides data immutability and integrity through the content identifier hash value [10]. The suggested system utilizes the InterPlanetary File System (IPFS) as a storage solution for medical data, thereby ensuring the preservation of data confidentiality, privacy, and cost-effectiveness.

5.1.4 LSTM Networks

Long Short-Term Memory Networks LSTM is a type of Recurrent Neural Network (RNN) [32].The utilization of LSTM Networks is due to the natural characteristics of the dataset, which primarily consists of sequential spatial data. The dataset used during this study is UniMiB SHAR, comprising a total of 11,771 instances representing various human activities such as running, walking, standing, and sitting, as well as different categories of falls such as backward, forward, and falling right from standing [20].

6 hChain 2.0 Architecture

The architectural framework for hChain 2.0 is illustrated in Figure 4. The framework comprises six primary components. The client layer's initial component encompasses IoMT, such as wearable devices, which are designed to detect and monitor the client's physiological parameter in real-time. The utilization of this lightweight data is crucial for healthcare providers as it enables the analysis of a patient's health status and its combination with the patient's medical history. The adoption of IoMT devices, including wearable devices, facilitates early detection of health problems and enhances patient awareness by allowing patients to monitor their health in real time. Additionally, the vast amount of real-time data captured by these devices enables healthcare providers to make more accurate diagnoses and predictions, leading to improved decision-making. Its primary objective is to enhance comprehension of the patient's health status and medical history during the course of treatment.

Additionally, the second component acts as an edge device, such as a smart phone, to facilitate data security management and analysis of fall detection nearby the patient. IoMT devices have lower capabilities in comparison to edge devices. Consequently, transferring the process to the edge device enhances the real-time data efficiency. The edge device formats the EHR data in a structured manner suitable for further processing, using the JSON format, and then saves the EHR in a buffer. Instead of transmitting EHR individually, it is more efficient to send a batch of EHR data to the IPFS. This approach improves data processing, reduces the frequency of transmission, enhances scalability, and increases cost-effectiveness. In addition, the EHR data is encrypted using the Paitnet private key. This enables protection against unauthorized access and maintains data integrity during transmission. It also enhances data privacy and secures the data even when transferred across an insecure network.

The third component entails the utilization of the LSTM network model in the development of an alert system module. The objective of this module is to identify instances of individuals falling and enable automatic response as soon as a fall is recognized. Initially, the patient must compile the list of predetermined emergency rooms in close proximity to their location. This way, in the event of a fall, the EHR can be promptly shared to the emergency room healthcare providers. The edge device handles data analysis using the LSTM model. If a fall is detected, it initiates a transaction with the smart contract ER transaction. This transaction shares the data with the nearest ER healthcare providers, enabling them to gain a better understan-ding of the patient's health and provide improved healthcare services. Additionally, this allows health-care professionals to access the patient's health history and gain a clearer vision of the patient's overall health. The edge device has an additional purpose of sharing the patient's EHR and initiating an automated emergency call. Consequently, it improves patient safety, ensures secure sharing of EHR during crucial periods, and enhances patient autonomy.

The middle layer has the fourth component which is distributed file storage to enhance data integrity, overcome the shortcomings of public blockchain data storage limitations, and avoid high costs [4]. EHRs are stored on the IPFS as distributed file storage and return a content identifier (CID) to the edge device, which then forwards the CID to the smart contract. After gathering data from the IoMT device, it is transmitted to the edge device. The edge devices then instantly publish the stored data to the IPFS and obtain the CID of the file. Subsequently, the CID is transferred to the smart contract via an edge device, so initiating a transaction to record the CID on the blockchain. It enables for the concurrent storing of several EHRs, hence decreasing the individual cost of each EHR in a distinct transaction. Consequently, after the patient grants permission to the healthcare practitioners, they will be able to retrieve all the data from the IPFS and confirm its integrity by comparing the hash values stored on the blockchain with the file hash value.

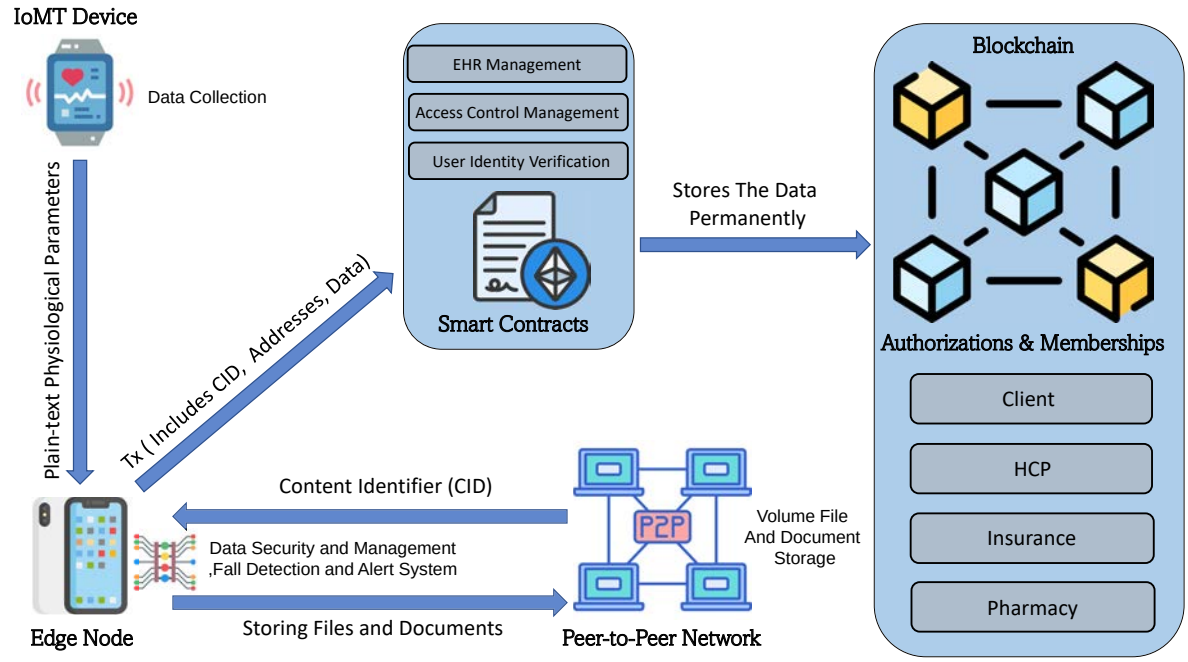

Fig. 4: hChain 2.0 Architecture.

The smart contract is the fifth component and has several functionalities, such as EHR sharing, with three kinds of sharing types: grant-based, limited-based access, and time-based. Therefore, the client can have multiple healthcare providers with different accessibility types. It also maintains the EHR pointer so that it can be retrieved by any permissioned healthcare providers or other stakeholders. This enables robust access control management while ensuring data integrity and cost effectiveness. Once the patient establishes that healthcare provider A has a grantee-based permission, it signifies that the healthcare provider has unrestricted and continuous access to the patient's EHR until the patient withdraws the permission. Limited-based access refers to the patient's ability to control the duration of healthcare provider B's access to the EHR within a specified time limit. The timestamp must not exceed the time determined by the patient, ensuring that the patient has access to the EHR during a treatment period. However, the duration may be extended if the patient initiates another transaction to extend it.

The sixth component is blockchain technology, which is placed as the third layer. Using the above procedures and protocols, the data is securely stored on a publicly accessible blockchain network, guaranteeing its integrity, traceability, security, and accessibility. The blockchain stores the CID of the file stored on IPFS and other necessary information such as sharing data and permission. Consequently, it improves security while remaining cost-effective, as the expense of storing all data on the blockchain is reduced, and it also promotes scalability. There are several stockholders in the proposed framework, which are the client or the patient, healthcare provider (HCP), insurance, and pharmacy. Each has the ability to access client EHRs. The administ-rator has the ability to grant clients and other stakeholders privileges. The access control manage-ment is based on Role-Based Access control (RBAC). As a result, it improves data confidentiality by assessing the privileges of each stakeholder, ensuring that they have designated responsibilities that align with the structure of the healthcare facility. Thus, it provides a decentralized framework, but it is not considered as serverless as it relies on blockchain nodes to maintain the ledger, validate transactions, and function as stateful entities, unlike stateless serverless platforms.

7 The Proposed Algorithms For hChain2

The proposed framework includes a variety of features, such as fall detection, secure data sharing, and EHR storage. Each individual client must possess a legitimate address that grants them certain privileges as a client. As presented in algorithm 1 shows the steps of storing the physiological parameters. The IoMT device detects and monitors physiological parameters, transmitting the data to the edge device in real-time. The edge device employs cryptographic hashing and signing algorithms

Algorithm 1 Procedure for Generating IoMT Data and Storing It on the Blockchain

Require: Physiological Parameters PP.
Ensure: Store EHR Data.
The wearable device sense PP
PP sent to the edge device
Edge device receives PP and format it in JSON format

Append the new PP to the previous PPs
if The PP buffer reach specified size **then**
    The PP is hashed using SHA-256
    Sign the hash value using client's private key
    Appends the signature at the end of JSON file
    Updates the JSON file
    Store the data to IPFS
    Edge device receives CID
    Format the CID to string
    edge device transacts the CID to the smart contract

    A smart contract validates the client's privileges
    Smart Contract append the new data with client's address in ehrData HashMap
    Transaction Confirmed
else
    Format PP in JSON format
    Appending PP with the previoues PP
    Updates the JSON file
end if

to provide a unique hash value and digital signature, respectively. Then, the signature is appended to the data in JSON format, thereby ensuring data integrity and authent-icity. Subsequently, the edge device receives a CID from IPFS in order to securely store it on the blockchain through a smart contract. This CID is then added to the client's ehrData hashmap. Furthermore, the proposed solution is designed to store any authorized data, which is first encrypted using the corresponding stakeholder's private key. The CID is transacted to the smart contract along with the stakeholder's blockchain account. The smart contract validates permissions based on prede-fined roles and appends the CID to the corresponding hashmap, ensuring access is strictly limited to authorized stakeholders. Therefore, retrieval of any authorized data occurs through the smart contract, which fetches the CID and enables access to the data stored in the distributed file storage system using the CID.

Once the capability of storing EHR data is enabled for client, it becomes crucial for facilitating the sharing of the EHR to healthcare providers.As shown in algorithm 2, the client has three options for sharing data: duration-based, granted-based, and quantity-based. In the event that the client selects for the duration-based , it is imperative that they provide the timestamp corresponding to the end date of their access. However, in the case that the client decides for a granted-based approach, it is sufficient for the client to provide merely the HCP

Algorithm 2 Data Sharing And Access Control Management

Require: HCP Address.
Ensure: Access Granted.
Client and HCP has to have a valid accounts
Client has the HCP address and detemines the type of sharing access
if Client choose time-based access **then**
    Client has to choose the time and date of access expiration
    Internal system converts the date and time to Unix timestamp
    It transacts to smart contract with HCP address and Unix timestamp
end if
if Client choose grant-based access **then**
    It transacts to smart contract using HCP address
end if
if Client choose quantity of accesses **then**
    Client determines the number of access
    It transacts through smart contract with HCP address and quantity of accesses
end if

address. The last type is the quantity of access required to pass the HCP address in conjunction with the number of accesses.

In order to enhance client welfare, a proposed module called as the Alert System Module (ASM) aims to facilitate emergency communication through the initiation of emergency calls as presented at algorithm 3. upon the wearable device senses accelerometer data, it transmits the data to an edge device, such as a smart phone. The edge device then utilizes the accelerometer samples as input for the LSTM model in order to identify instances of falling. In the event of a fall, the edge device changes ASM to risk mode and initiates a transaction to securely share the client's medical data with the nearest emergency room, utilizing a smart contract. Conversely, the edge device maintains the safe mode.

8 Implementation And Validation

8.1 Implementation

The development of hChain 2.0 involves the utilization of several technologies and cryptographic methods. Table 5 presents the main functions of smart contract, and as shown in Table 6, multiple software tools are utilized for the implementation of hChain2. Solidity is employed in the creation of Ethereum smart contracts. It facilitates the development of a sharing mechanism that enables stakeholders to engage in the exchange of EHRs and EHR storage in secure manner. Each stakeholder possesses a distinct externally owned account

Algorithm 3 Alert System Module

Require: Accelerometer Data *AD*.
Ensure: Activities of Daily Living Or Fall Detection.
1: The wearable device senses *AD*
2: The wearable device buffering *AD* samples for a period of time
3: The wearable devives sends *AD* samples to the edge device
4: Edge device receives *AD* samples
5: Edge device uses the samples as an input to LSTM model
6: **if** LSTM model classifies *AD* as Fall And no movement for short of Period of time **then**
7: Alert system module status changed to Risk Mode
8: Edge device makes a transaction through a smart contract to share EHR data with the nearest stored ER.
9: The alert system makes an auto emergency call.
10: **else**
11: Alert system maintains Safe Mode
12: **end if**

(EOA) to interact with the smart contract. The Brownie framework was utilized to test, compile, and deploy an Ethereum smart contract, as shown in Figure 5 which displays the successful compilation of the EHRManagement smart contract using Brownie with Solidity v0.8.20. Figure 6 shows the utilization of the Brownie frame-work for interacting with the Georli test net for the purpose of adding new roles and EHR. Figure 6(a) displays the interface for setting user roles, where role number 1 represents the patient role, and the patient's blockchain address is entered in the provided field. Figure 6(b) illustrates the process of adding new EHR data by entering the generated CID along with the patient's address. Figures 6(c) and 6(d) display the transaction confirmations, including the transaction hashes, gas prices, gas limits, and gas usage percentages for setting user roles and adding new EHR data, respectively. Figure 6(e) displays the interface for setting the healthcare provider role, where number 3 represents the health-care provider role, and the healthcare provider's blockchain address is entered in the provided field. Figure 6(f) presents the interface where the patient grants authorization to the healthcare provider for accessing and sharing their EHRs, while number 1 represents Unrestricted Access. Figures 6(g) and 6(h) present the transaction confirmations for grant-ing healthcare provider authorization to access patient EHRs and assigning the healthcare provider role, with corresponding transaction hashes displayed.

IPFS is utilized as a distributed file storage system for the purpose of storing medical data in a peer-to-peer manner. Python is utilized in the development and testing of smart contracts, web interfaces, as shown in Figure 7, displays the home page interface. The UniMiB SHAR dataset is utilized for the purpose of fall detection and comprises a total of 11,771 instances encompassing falls as well as daily activities [20]. The SHA-256 algorithm is employed as a cryptogra-phic hashing function in order to ensure the integrity of data. The implementation is developed on a Dell system with a 2.90 GHz Intel (R) Core i7 and 16384 MB of RAM. Windows 10 Enterprise 64-bit is utilized.

Fig. 5: Smart Contract Compilation.

8.1.1 Case Study

In the hChain 2.0 system, each stakeholder, including patients and healthcare providers, is assigned predefined roles and authorizations tailored to their respective responsibilities. Patients are equipped with smartwatches that continuously monitor physiological parameters, providing essential real-time data for the early detection of health issues. Smartphones serve as edge devices and host lightweight applications that process this data in real time, ensure data security, and format the data appropriately before transmitting it to a distributed file storage system.

Once the data is stored, the application receives a CID, which, along with the patient's wallet blockchain account, is transacted to the smart contract. Upon verifying the authenticity, the smart contract appends the new CID to the patient's hashmap, thus creating a comprehensive and secure record of the patient's health data. Healthcare providers interact with the system using a web-based user interface, which enables them to manage communications with both the distributed file storage system and the blockchain. These interactions require blockchain-based accounts belonging to the healthcare providers, ensuring that access to a patient's health history is permitted only to authorized accounts. This framework not only simplifies the management of large volumes of data but also enhances cost-effectiveness and facilitates the system's adoption.

Table 5: Smart Contract Main Functions

Function Name	Description
setRole	Sets the role of a user. Only the admin can assign roles.
setEHRData	Allows a patient to add their electronic health record (EHR) data.
grantUnrestrictedAccess	Allows a patient to grant unrestricted access to their EHR data.
grantTimedAccess	Allows a patient to grant timed access to their EHR data.
grantLimitedAccess	Allows a patient to grant limited access to their EHR data.
accessEHRData	Allows an authorized user to access a patient's EHR data.
setEmergencyRoom	Allows a patient to set or update their associated emergency room (ER) address.
grantERAccess	Allows a patient to grant their associated ER access to their EHRs.

(a) Setting Patient Role

(b) Adding EHR to The Patient

(c) Setting Patient Role Tx

(d) Adding EHR to The Patient Tx

(e) Setting HCP Role

(f) Granting EHR Access to HCP Account

(g) Granting Access to HCP Account Tx

(h) Setting HCP Role Tx

Fig. 6: Setting New Roles, Granting EHR Access and Adding New EHR

Table 6: Blockchain Development Tools and Versions

Tool Name	Version
Ganache Local Blockchain	v2.5.4
Visual Studio Code	1.84.0
Remix IDE	0.39.0
IPFS	0.26.1
Python Programming Language	3.10.9
Brownie development & testing framework	0.8.0
MetaMask	11.7.2
Solidity Compiler	0.8.0

8.2 Validation

8.2.1 Fall Detection

The LSTM model presents significant results with a validation loss of 0.0138 and a validity accuracy of 99.78%. Figure 8 displays the loss results for each epoch iteration, whereas Figure 9 depicts the accuracy values for each epoch. In the evaluation of our model's performance, we assess key metrics such as the F1 Score, precision, and recall. The F1 Score is the harmonic mean of recall and precision, combining them into a single value to assess the balance between these two metrics. Metrics like

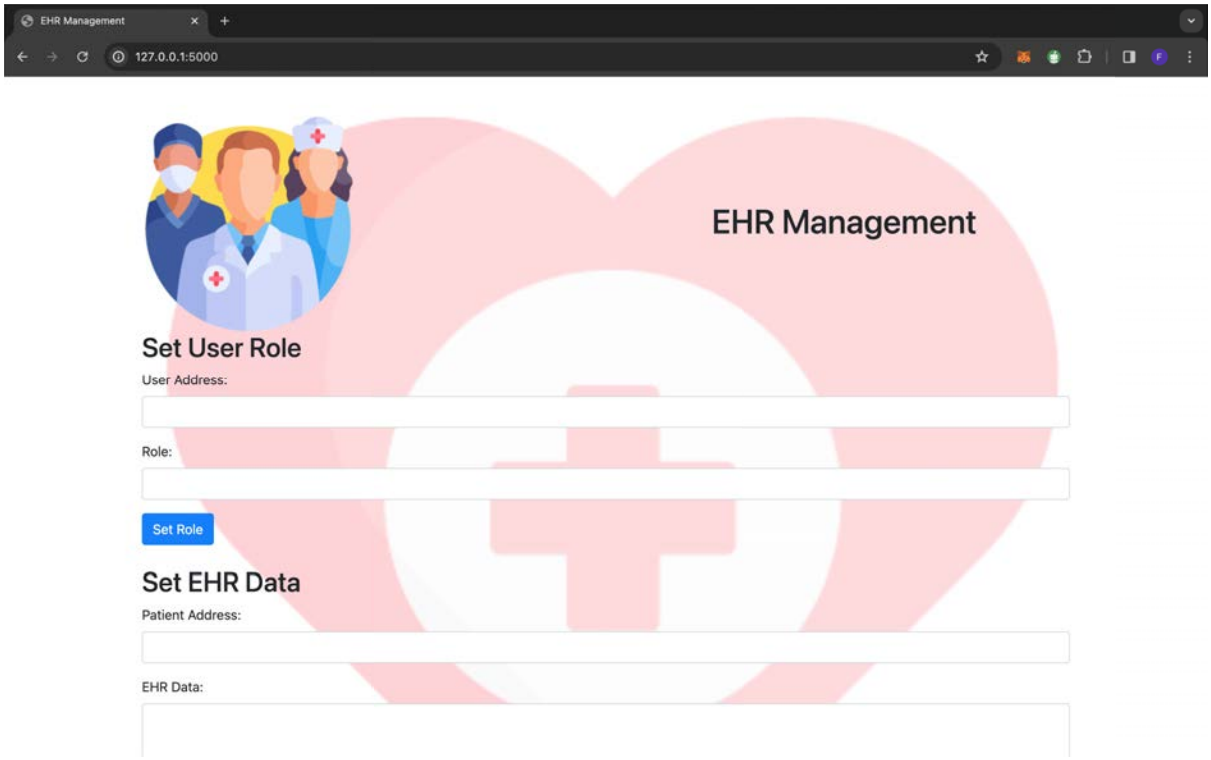

Fig. 7: hChain2 Implementation Python Web-Interace Flask-Based.

accuracy can be misleading, especially in datasets with imbalanced classes, as they often fail to reflect the model's performance on the minority class. The F1 Score overcomes this issue by giving equal importance to precision, which focuses on minimizing false positives, and recall, which focuses on minimizing false negatives. F1 Score is on our model is 0.9944, and its calculation method is as follows:

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (1)$$

Recall evaluates the proportion of actual positives that are correctly identified by the model. It specifically measures how effectively the model detects actual falls, focusing on both true positives and false negatives. A true positive occurs when a fall happens, and the model successfully detects it, while a false negative occurs when a fall happens, but the model fails to detect it. Therefore, recall is a critical metric that demonstrates the model's accuracy in identifying falls. Our model Recall is 0.9966 and it is calculated as the follow:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (2)$$

Precision is a metric that evaluates the correctness for positive identifications. Our model Precision is 0.9921 and it is calculated as the follow:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (3)$$

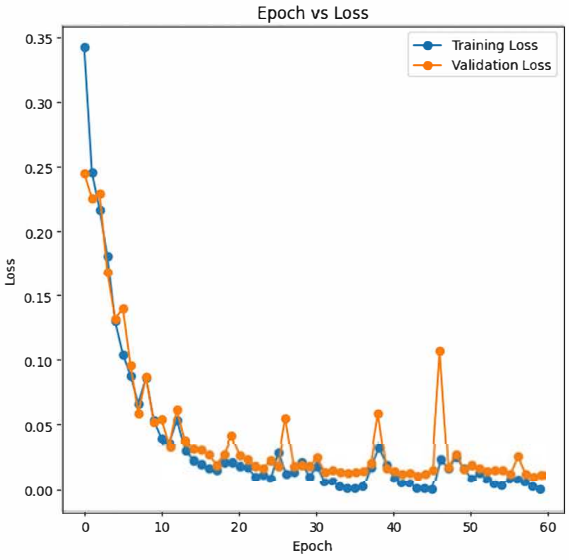

Fig. 8: Loss for Each Epoch.

Figure 10 depicts the confusion matrix, which displays classification accuracy and errors. The equation use the abbreviations TP for true positive, FP for false positive, and FN for false negative. As in previous results, our LSTM model has a notable effectiveness in detecting falls, with a remarkable accuracy rate of 99.78%. Consequently, it exhibits exceptional precision in identifying instances of falls. The model's overall performance

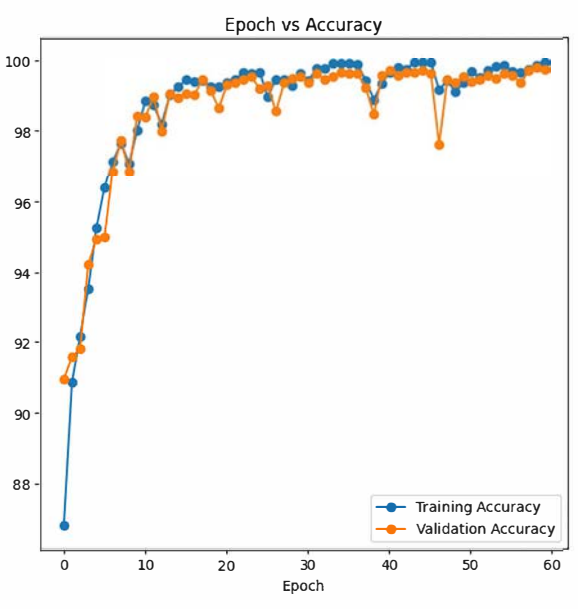

Fig. 9: Accuracy for Each Epoch.

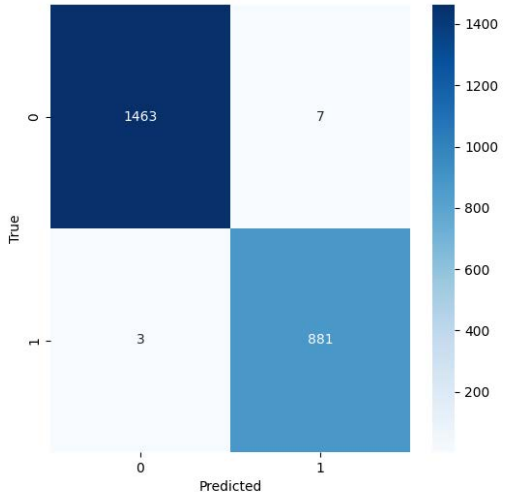

Fig. 10: Confusion Matrix.

demonstrates a strong ability to accurately classify between two distinct scenarios: fall detection and daily life activities.

8.2.2 Cost And Time Analysis

The cost study demonstrates a very low expense for ETH, as illustrated in Table 7 and Figure 11. The cost of deploying the smart contract is 0.000000000022128 85 ETH, and the time required for deployment is 4.25 seconds. The cost for granting access is 0.00000000-000121665 ETH, with a confir-mation time of 9.1 seconds for the transaction. whereas, the establishment of a role and the storage of 25 MG of data incur costs of 0.000000000001209286 ETH and 0.00000-00000-02522442 ETH, accompanied by time durations of 10.50 seconds and 9.4 seconds, correspondingly.

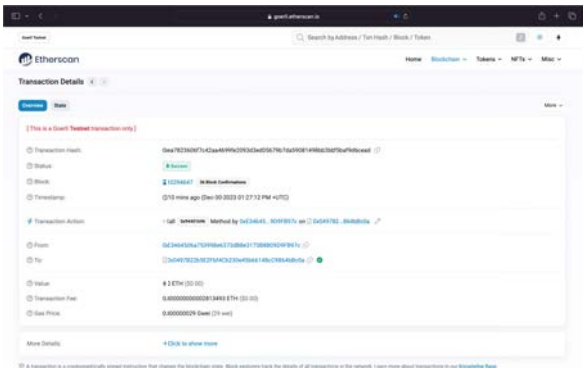

Fig. 11: Transaction Details In EtherScan

8.2.3 Privacy, Data Security and Scalability

The integration of blockchain, smart contracts, and IPFS yields notable enhancements in privacy as a result of EHR ownership and patient anonymity facilitated by the blockchain technology. The utilization of IPFS as a storage mechanism, along with the storage of CIDs on the blockchain, enhances the level of anonymity pertaining to data ownership. Furthermore, it offers immutability, integrity, and fault tolerance, hence increasing data security. Offloading data to IPFS improves scalability and decreases cost.

8.2.4 Availability and Auditability

The integration of IPFS and blockchain delivers stakeholders several advantages as a result of their inherent properties, which assure immutability and transparency. In addition, the utilization of smart contracts enhances the auditability of processes by facilitating the management of access control. Furthermore, the decentralized design of both systems enhances data availability by virtue of data redundancy.

8.2.5 Anonymity and Access Control Management

Each stakeholder has an EOA and private and public keys, which represent the person's identity, thereby increasing the anonymity beside transaction mechanism. Using IPFS as EHR storage and storing CIDs on blockchain also enhances anonymity because the raw data owner is anonymous. hChain 2.0 smart contract provides several kinds of access

Table 7: Cost Analysis

Data Size	Patient Address	IPFS Hash	Tx Hash	Tx Fee
1 MB	0xE3464506a753 998e6373dB8e3173 B8B09D9FB97c	QmVkbauSDEaMP4T kq6Epm9uW75mWm13 6n81YH8fGtfwdHU	0x298e109d16573792c 60163fc4642cde0621b3e1 befc6618da3ad19d3dfe237b5	0.0000000000 03195276 ETH
5 MB		QmS2s8GRYHEurXL 7V1zUtKvf2H1BGcQ c5NN1T1hiSnWvbd	0xb6ed4306c8815a4d 25064e35d8778136abd00bd 227e40107c71bd71daeea3b02	0.0000000000 02716476 ETH
14 MB		QmeEKZRvEt8a8Bgo AU8HrtRy1GhYMqbV CB4hv7VbimWQfX	0xb87992ce55dbed65 12181cfb1791c588968cd2 faf2eef688a495357d09b04aac	0.0000000000 02813493 ETH
45 MB		QmRzFkZ7nkn1p7bS PrPNs2FTCPLmCwCe ez2KMcNT2FtKAb	0x416ef05a94eac1de d96fed78c783a20c8d9bba dc5199b1a515cf5f98d148be78	0.0000000000 02813493 ETH
70 MB		QmZKjWW2CEbZy4Vz EdX1g7DaUNZL3Usj J2Ai1vTeKv87Yj	0x8c1c8a3364625 38a 775b4cdc93e9aaff655048a3 de99fb0949c40525ebb880a8	0.0000000000 02716476 ETH
102 MB		QmbBVEo8257xg2Zd 2bTc1PDukCsDKzZx qYtsshRLhxYjCD	0xea7823606f7c42aa4 6969fe2093d3ed05679b7da 59081498bb3bbf5baf9d6cead	0.0000000000 02813493 ETH

control management, such as grant-based, time-based, and quantity-based access control.

9 Conclusion and Future Directions

The hChain 2.0 framework addresses the inherent limitations of conventional centralized healthcare systems, including challenges related to availability, single points of failure, compromised data integrity, and unclear ownership of EHR. By adopting a decentralized architecture, hChain 2.0 mitigates these deficiencies, empowering patients with full ownership and control over their health records. The framework's decentralized nature ensures data integrity, security, availability, and traceability, establishing a robust solution for modern EHR management. While public blockchains offer robust security, they present significant challenges in the context of EHR management due to their high costs and inefficiencies in handling large-scale data storage. To overcome these limitations, hChain 2.0 integrates a distributed file storage system with blockchain technology. This hybrid approach enhances scalability and cost-efficiency by using the distributed file storage system to securely store encrypted, authorized data, while employing blockchain technology to record CIDs via smart contracts.

Moreover, hChain 2.0 incorporates advanced access control mechanisms through smart contracts, enabling grant-based, time-based, and quantity-based sharing options. These mechanisms are tailored to meet the diverse requirements of healthcare interactions, facilitating secure, traceable, and trans-parent sharing of EHRs across multiple entities. In addition, the framework leverages an LSTM model for fall detection, addressing critical risks faced by individuals in solitary environments. The proposed model demonstrates significant accuracy and efficiency in identifying falls, thereby enhancing patient safety and enabling timely intervention in emergency scenarios.

For future advancements, the proposed solution could integrate cloud computing technologies to enhance scalability and adaptability, enabling efficient handling of dynamic loads and growing demand. Smart contracts could be utilized for managing cloud-based authorizations and lightweight data storage, ensuring secure access and maintaining data integrity. Additionally, stakeholders could develop tailored smart contracts to address the unique requirements of individual clients, deliver-

ing person-alized and efficient services while preserving the transparency, automation, and security inherent in smart contract technology.

Compliance with Ethical Standards

The authors declare that they have no conflict of interest and there was no human or animal testing or participation involved in this research. All data were obtained from public domain sources.

References

1. Adane, K., Gizachew, M., Kendie, S.: The role of medical data in efficient patient care delivery: a review. Risk management and healthcare policy **12**, 67–73 (2019)
2. Alkhodair, A., Mohanty, S.P., Kougianos, E.: Flexichain 3.0: Distributed ledger technology-based intelligent transportation for vehicular digital asset exchange in smart cities. Sensors **23**(8) (2023). DOI: 10.3390/s23084114. URL https://www.mdpi.com/1424-8220/23/8/4114
3. Alruwaill, M., Bapatla, A.K., Mohanty, S.P., Kougianos, E.: FarmIns: blockchain leveraged secure and reliable crop insurance management system. In: 2023 IFIP International Internet of Things Conference (IFIP-IoT-2023), pp. 1–8. Denton, USA (2023)
4. Alruwaill, M.N., Mohanty, S.P., Kougianos, E.: Fortiins: A blockchain based framework to automate healthcare insurance processing in smart cities. In: Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES), pp. XX–YY (2023). DOI: XXX
5. Alruwaill, M.N., Mohanty, S.P., Kougianos, E.: Hchain: Blockchain based healthcare data sharing with enhanced security and privacy location-based-authentication. In: Proceedings of the Great Lakes Symposium on VLSI 2023, GLSVLSI '23, p. 97–102. Association for Computing Machinery, New York, NY, USA (2023). DOI: 10.1145/3583781.3590255. URL https://doi.org/10.1145/3583781.3590255
6. Arane, S.P., Mandhare, V.V., Vikhe, P.S.: Design of medi-chain: A blockchain and cloud based health record system. In: 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–6 (2021). DOI: 10.1109/ICECCT52121.2021.9616821
7. Ben Amar, A., Kouki, A.B., Cao, H.: Power approaches for implantable medical devices. Sensors (Basel, Switzerland) **15**, 28889–914 (2015)
8. Bhushan, B., Kumar, A., Agarwal, A.K., Kumar, A., Bhattacharya, P., Kumar, A.: Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. Sustainability **15**(7) (2023). DOI: 10.3390/su15076177. URL https://www.mdpi.com/2071-1050/15/7/6177
9. De Fazio, R., Mastronardi, V.M., De Vittorio, M., Visconti, P.: Wearable sensors and smart devices to monitor rehabilitation parameters and sports performance: An overview. Sensors (Basel, Switzerland) **23** (2023)
10. Doan, T.V., Psaras, Y., Ott, J., Bajpai, V.: Toward decentralized cloud storage with ipfs: Opportunities, challenges, and future considerations. IEEE Internet Computing **26**(6), 7–15 (2022). DOI: 10.1109/MIC.2022.3209804
11. Egala, B.S., Pradhan, A.K., Badarla, V., Mohanty, S.P.: Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal **8**(14), 11717–11731 (2021). DOI: 10.1109/JIOT.2021.3058946
12. Egala, B.S., Pradhan, A.K., Dey, P., Badarla, V., Mohanty, S.P.: Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system. IEEE Internet of Things Journal **10**(14), 12308–12321 (2023). DOI: 10.1109/JIOT.2023.3247452
13. Fugkeaw, S., Prasad Gupta, R., Worapaluk, K.: Secure and fine-grained access control with optimized revocation for outsourced iot ehrs with adaptive load-sharing in fog-assisted cloud environment. IEEE Access **12**, 82753–82768 (2024). DOI: 10.1109/ACCESS.2024.3412754
14. Jain, M., Pandey, D., Singh, N.P.: Ehr: Patient electronic health records using blockchain security framework. In: 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), pp. 710–715 (2023). DOI: 10.1109/ICIDCA56705.2023.10099789
15. Kaur, M., Gupta, S., Kumar, D., Raboaca, M.S., Goyal, S.B., Verma, C.: Ipfs: An off-chain storage solution for blockchain. In: Y. Singh, P.K. Singh, M.H. Kolekar, A.K. Kar, P.J.S. Gonçalves (eds.) Proceedings of International Conference on Recent Innovations in Computing, pp. 513–525. Springer Nature Singapore, Singapore (2023)
16. Lücking, M., Manke, R., Schinle, M., Kohout, L., Nickel, S., Stork, W.: Decentralized patient-centric data management for sharing iot data streams. In: 2020 International Conference on Omni-layer Intelligent Systems (COINS), pp. 1–6 (2020). DOI: 10.1109/COINS49042.2020.9191653
17. Mahamuni, C.V., Sayyed, Z., Mishra, A.: Machine learning for smart cities: A survey. In: 2022 IEEE International Power and Renewable Energy Conference (IPRECON), pp. 1–8 (2022). DOI: 10.1109/IPRECON55716.2022.10059521
18. Mandsberg, N.K., Christfort, J.F., Kamguyan, K., Boisen, A., Srivastava, S.K.: Orally ingestible medical devices for gut engineering. Advanced drug delivery reviews **165-166**, 142–154 (2020)
19. Manickam, P., Mariappan, S.A., Murugesan, S.M., Hansda, S., Kaushik, A., Shinde, R., Thipperudraswamy, S.P.: Artificial intelligence (ai) and internet of medical things (iomt) assisted biomedical systems for intelligent healthcare. Biosensors **12** (2022)
20. Micucci, D., Mobilio, M., Napoletano, P.: Unimib shar: A dataset for human activity recognition using acceleration data from smartphones. Applied Sciences **7**(10) (2017). DOI: 10.3390/app7101101. URL https://www.mdpi.com/2076-3417/7/10/1101
21. Minhas, N.N., Mubeen, M.W., Khawaja, H.: Distributed ledger technologies for electronic health care: Iota-based remote patient monitoring and telemedicine system. Computer **56**(10), 31–39 (2023). DOI: 10.1109/MC.2023.3303315
22. Mishra, P., Singh, G.: Internet of medical things healthcare for sustainable smart cities: Current status and future prospects. Applied Sciences **13**(15) (2023). DOI: 10.3390/app13158869. URL https://www.mdpi.com/2076-3417/13/15/8869

23. Mishra, R., Ramesh, D., Edla, D.R.: Deletable blockchain based secure ehr storage scheme in multi-cloud environment. In: 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1057–1064 (2020). DOI: 10.1109/HPCC-SmartCity-DSS50907.2020.00142
24. Mohammadzadeh, Z., Saeidnia, H.R., Lotfata, A., Hassanzadeh, M., Ghiasi, N.: Smart city healthcare delivery innovations: a systematic review of essential technologies and indicators for developing nations. BMC health services research **23**, 1180 (2023)
25. Oladipo, I.D., AbdulRaheem, M., Awotunde, J.B., Bhoi, A.K., Adeniyi, E.A., Abiodun, M.K.: Machine Learning and Deep Learning Algorithms for Smart Cities: A Start-of-the-Art Review, pp. 143–162. Springer International Publishing, Cham (2022). DOI: 10.1007/978-3-030-82715-1_7. URL https://doi.org/10.1007/978-3-030-82715-1_7
26. Reddi, S., Rao, P.M., Saraswathi, P., Jangirala, S., Das, A.K., Jamal, S.S., Park, Y.: Privacy-preserving electronic medical record sharing for iot-enabled healthcare system using fully homomorphic encryption, iota, and masked authenticated messaging. IEEE Transactions on Industrial Informatics **20**(9), 10802–10813 (2024). DOI: 10.1109/TII.2024.3397343
27. Reza, M.R., Singh, S.K.: A framework to secure electronic health records using privacy-enabled hyperledger fabric. In: 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), pp. 1–7 (2023). DOI: 10.1109/GlobConET56651.2023.10150086
28. Sadashiv, N., G, V.S.: Swaasthya sampathee: Blockchain based ehr framework. In: 2022 International Conference on Industry 4.0 Technology (I4Tech), pp. 1–6 (2022). DOI: 10.1109/I4Tech55392.2022.9952557
29. Saweros, E., Song, Y.T.: Connecting personal health records together with ehr using tangle. In: 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 547–554 (2019). DOI: 10.1109/SNPD.2019.8935646
30. Shaikh, R.: Blockchain based cloud storage of patients health records. In: 2022 IEEE Delhi Section Conference (DELCON), pp. 1–5 (2022). DOI: 10.1109/DELCON54057.2022.9753574
31. Shen, J., Zeng, P., Choo, K.K.R., Li, C.: A certificateless provable data possession scheme for cloud-based ehrs. IEEE Transactions on Information Forensics and Security **18**, 1156–1168 (2023). DOI: 10.1109/TIFS.2023.3236451
32. Sherstinsky, A.: Fundamentals of recurrent neural network (rnn) and long short-term memory (lstm) network. Physica D: Nonlinear Phenomena **404**, 132306 (2020). DOI: https://doi.org/10.1016/j.physd.2019.132306. URL https://www.sciencedirect.com/science/article/pii/S0167278919305974
33. Shuaib, K., Abdella, J., Sallabi, F., Serhani, M.A.: Secure decentralized electronic health records sharing system based on blockchains. Journal of King Saud University - Computer and Information Sciences **34**(8, Part A), 5045–5058 (2022). DOI: https://doi.org/10.1016/j.jksuci.2021.05.002. URL https://www.sciencedirect.com/science/article/pii/S1319157821001051
34. Singh, A., Chatterjee, K., Singh, A.K., Kumar, N.: Secure smart healthcare framework using lightweight dna sequence and chaos for mobile-edge computing. IEEE Internet of Things Journal **10**(6), 4883–4890 (2023). DOI: 10.1109/JIOT.2022.3219113
35. Singh, S., Gupta, S., Indu: Medehr-electronic health record using blockchain. In: 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), pp. 58–62 (2023). DOI: 10.1109/CICTN57981.2023.10141053
36. Srivastava, J., Routray, S., Ahmad, S., Waris, M.M.: Internet of medical things (iomt)-based smart healthcare system: Trends and progress. Computational intelligence and neuroscience **2022**, 7218113 (2022)
37. Taherdoost, H.: Smart contracts in blockchain technology: A critical review. Information **14**(2) (2023). DOI: 10.3390/info14020117. URL https://www.mdpi.com/2078-2489/14/2/117
38. Thong Tran, N.D., Leung, C.K., Madill, E.W., Binh, P.T.: A deep learning based predictive model for healthcare analytics. In: 2022 IEEE 10th International Conference on Healthcare Informatics (ICHI), pp. 547–549 (2022). DOI: 10.1109/ICHI54592.2022.00106
39. Tripathi, G., Ahad, M.A., Casalino, G.: A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decision Analytics Journal **9**, 100344 (2023). DOI: https://doi.org/10.1016/j.dajour.2023.100344. URL https://www.sciencedirect.com/science/article/pii/S2772662223001844
40. Verma, P., Fatima, S.: Smart Healthcare Applications and Real-Time Analytics Through Edge Computing, pp. 241–270. Springer International Publishing, Cham (2020). DOI: 10.1007/978-3-030-37526-3_11. URL https://doi.org/10.1007/978-3-030-37526-3_11
41. Walid, R., Joshi, K.P., Geol Choi, S., Kim, D.y.: Cloud-based encrypted ehr system with semantically rich access control and searchable encryption. In: 2020 IEEE International Conference on Big Data (Big Data), pp. 4075–4082 (2020). DOI: 10.1109/BigData50022.2020.9378002
42. Zhang, R., Xue, R., Liu, L.: Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing **15**(6), 3668–3686 (2022). DOI: 10.1109/TSC.2021.3085913