DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System

Sujit Biswas, *Member, IEEE,* Kashif Sharif, *Senior Member, IEEE,* Fan Li, *Member, IEEE,* Iqbal Alam, and Saraju P. Mohanty, *Senior Memeber, IEEE*

Abstract—The use of the Internet of Things and modern technologies has boosted the expansion of e-health solutions significantly and allowed access to better health services and remote monitoring of patients. Every service provider usually implements its information system to manage and access patient data for its unique purpose. Hence, the interoperability among independent e-health service providers is still a major challenge. From the structure of stored data to its large volume, the design of each such big data system varies, hence the cooperation among different e-health systems is almost impossible. In addition to this, the security and privacy of patient information is a challenging task. Building a unified solution for all creates significant business and economic issues. In this work, we present a solution to migrate existing e-health systems to a unified Blockchain-based model, where access to large scale medical data of patients can be achieved seamlessly by any service provider. A core blockchain network connects individual & independent e-health systems without requiring them to modify their internal processes. Access to patient data in the form of digital assets stored in off-chain storage is controlled through patient-centric channels and policy transactions. Through emulation, we show that the proposed solution can interconnect different e-health systems efficiently.

Index Terms—Blockchain, E-Health Systems, Digital Assets, Access Control, Electronic Medical Records (EMR), Interoperability.

1 Introduction

THE use of information and communication technologies in the healthcare sector has greatly increased the development of e-health systems (EHS). The efficient utilization of these technologies ensures the transmission of health records as digital assets to relevant entities in the whole e-health ecosystem. The modern EHS provides a cost-effective way to improve the availability of personal & resources and monitoring of patient conditions, especially in developing countries [1]. In recent years, the emergence of Internet of Things (IoT) devices for healthcare (HIoT), also known as Internet of Medical Things (IoMT) have further improved the availability and quality of services. As a result, the digital health market will reach approximately 206 billion USD worldwide by 2020 [2], and about 161 million IoT devices will be in use by the year 2020 alone [3]. World health organization estimates that more than 80% of the countries have taken e-health initiatives in some context, and this percentage is expected to increase with the deployment of 5G technologies [4]. Most of this effort is geared towards a national level health service, such as [5], while some developed countries already have national level health services.

There are two major challenges in building a national level e-health ecosystem. The first deals with the interoperability and unification of existing independent healthcare service providers (i.e. hospitals, diagnostic centers, primary health facilities, IoMT applications, insurance providers, etc.). The second deals with secure access to patients digital records by different internal and external elements of the initial service provider's system. The volume and scale of such data is extremely large, which complicates the unified access control mechanisms. The primary objective of the complete national healthcare ecosystem is to enable cross-communication of medical data among various service providers while maintaining the individual process and procedures (technical/administrative) unchanged. Moreover, the solution cannot be a total replacement of existing systems, and rather a gradual migration towards interoperability. Due to these reasons, the unification and integration at the national level or even organizational level must consider issues, such as the format of digital assets, structure of stored data, application interfaces of information management systems, types of users, and centralized/distributed networks, to name a few. Assuming that such a unification is done where a centralized system connects individual EHS and allows the exchange of patient records (digital assets) among them, security and privacy of assets becomes paramount. In an independent system, all users (e.g. patients and physicians) could be registered and policies for access control could be defined using role-based access control (RBAC) mechanism. But in a unified system, the same patient might visit another healthcare facility whose physician may not be recognized by the initial service provider. Hence, access control becomes extremely complicated in such scenarios. Similarly, different users may have different privileges to access data, for example, a physician may have complete access while a nurse may only ready prescribed medication information. In addition

- *S. Biswas, K. Sharif, F. Li, and I. Alam are with the School of Computer Science, Beijing Institute of Technology, Beijing, China. E-mail: {sujitedu, kashif, fli, iqbalalam}@bit.edu.cn*
- *S. P. Mohanty is with the University of North Texas, TX, USA E-mail: saraju.mohanty@unt.edu*

This work is partially supported by the National Natural Science Foundation of China No. 61772077, 61370192, and the Beijing Natural Science Foundation No. 4192051.
Manuscript received November 3, 2020; revised XXXX.
Co-corresponding authors: Kashif Sharif, Fan Li

to this, the integration of third-party IoMT devices, such as smartwatches and health monitors, upload the data to their respective servers. Starting from device level permissions [6], [7] to wireless access [8] and then server integration with the ecosystem, several passive privacy attacks can compromise a patient's information [9]. Moreover, the centralized nature of this solution will always create a single point of failure as well as scalability issues in terms of big data and storage/access.

Blockchain (BC) has recently emerged as a technology that can provide unparalleled security features to several types of systems [10]. It has been primarily used for cryptocurrencies, but it can also be applied to other domains such as IoT, asset tracking, access control, and business processes [11], [12]. Moreover, its properties of encryption support, the immutability of ledger, user anonymization, validation through multi-peer consensus can be extremely beneficial for e-health systems [13]. Based on these motivations, in this article, we present a BC-based unified ecosystem for e-health systems. The proposed solution is based on gradual migration and integration of existing EHS towards a unified model, where digital assets can be exchanged among different entities in a secure manner. The architecture mainly comprises of a core blockchain network with a trusted authority and multiple peers. Individual EHS information systems connect to peers through programming interfaces, which allows seamless interconnectivity while allowing individual processes and storage systems to remain unchanged. More precisely, the proposed unified solution makes the following contributions.

- We present a comprehensive migration solution to integrate independent centralized EHS and the massive number of EMRs into a unified blockchain-based network.
- We present a novel solution to use patient-centric blockchain channels to enable access control of creating and managing the EMRs through a compound key. This solution limits the requirement of frequent smart contract changes.
- The solution utilizes a unified Trust Authority and distributed off-chain storage as part of the overall architecture. This enables users to access big data across different EHS.
- We present novel algorithms to store digital assets in BC ledger and off-chain storage, without compromising the validation and consensus formation principles of blockchain.
- We prove through practical implementation that the proposed solution is scalable for big data storage and efficient in providing access control.

The rest of paper has been organized into seven sections. Section 2 presents the background information on blockchain and challenges of EHS unification along with related works. Proposed framework architecture is detailed in section 3, while the individual processes of registration and access control are described in sections 4 & 5 respectively. Section 6 gives the analysis and evaluation, and conclusion is presented in section 7.

2 Background & Related Works

In this section, we first describe the background information required to understand the working of a typical Blockchain system, followed by conventional e-health system architecture basics. We also discuss the related works done in integrating both systems.

2.1 Blockchain Basics

Blockchain is a peer-to-peer decentralized networking technology where any kind of transaction is approved through a consensus mechanism [14]. Transactions can be the exchange of information/data, digital assets, or cryptocurrency between two users of the system. Consensus is the mechanism of validating and legitimizing a transaction to become part of an immutable block, through a voting process among Peers of the network. The validation is done based on a pre-agreed smart contract (or chaincode) among the transacting users. Transactional data is stored in a block, which is linked to its predecessor block through its hash value making a chain structure. This structure is stored in the Ledger, where every peer maintains identical information, thus eliminating a single point of failure. Moreover, the data stored in blocks is not only encrypted but also immutable, eliminating the threat of malicious modification after commit. Most of Blockchain systems available are for cryptocurrency exchange or payments, hence they are not suitable for digital asset exchange or information tracking. Ethereum [15] and Hyperledger Projects (Fabric, Sawtooth, Iroha) [16] are more suitable solutions for complex business application which require business logic to be part of smart contracts. Access control in the blockchain is related to the capability of generating transactions. This is primarily a role-based scheme, where the smart contract determines the permissions of the transacting parties.

2.2 Challenges of BC and E-health Unification

EHS Limitations: The architecture of current independent e-health systems is entirely centralized, which means that the application server, database, access control, and certification authority are all at a single place, hence creating a single point of failure. Even if they are separate physical machines, they are usually located in the same subnet, which can be attacked. This also leads to a single point of information leakage. Another important factor is the transfer of information, as a patient may visit different service providers over time. As there is no direct connectivity among different EHS, hence the historical medical records are often not available. Although this process can be automated, this cooperation among EHSs has to be done at a higher managerial level which may be hampered by procedural and bureaucratic issues. Finally, the information access is not patient controlled, rather is defined by as part of the system and same for all users. Although this is not a drawback, but as owner of their data the patient should be in complete control of their information.

In order to address these issues, a blockchain based e-health system can be realized. However, this migration has several challenges which are listed below.

- *Architecture:* Resolution of network type differences, as different networks very in architecture and nature, such as one is centralized whether another is decentralized.

- *Synchronization of Transactions:* Multiple peers in BC network handle large concurrent transactions, while centralize systems handles transactions synchronously.
- *Data Atomicity:* Maintaining atomicity of previous data is quite challenging. Single patient medical data is recorded in several individual servers in different ways with/without timestamps, which may also have contradictory information.
- *Data Migration:* Migration of all previous records to the BC system directly is impossible. BC ledger is unable to accept previous record with old timestamps. Every new transaction must have a current timestamp.
- *Data Types:* Adoption of medical images/documents in BC block not possible, because it has limitation of capacity, such as 1MB for Bitcoin, 8MB for Hdac [17]. However, large medical images/documents are always part of data in an e-health system. Moreover, data can be generated by different devices at different rates, i.e. IoMT sensor as compared to MRI.
- *User Types:* There are numerous types of users with diverse access control requirements. As prime service seekers, a patient gets services from various types of service providers such as physicians, diagnostics centers, nurses, etc. and all may have different access specifications.
- *Access Limitation:* Limiting access rights by a patient to their current caregiver is also important. A patient may wish that the old physician should not access new data, and this may change frequently. Similarly, the data may also require anonymization before sharing. Hence, role-based access control has to be integrated with transaction generation capabilities.

2.3 Related works on E-Health and Blockchain

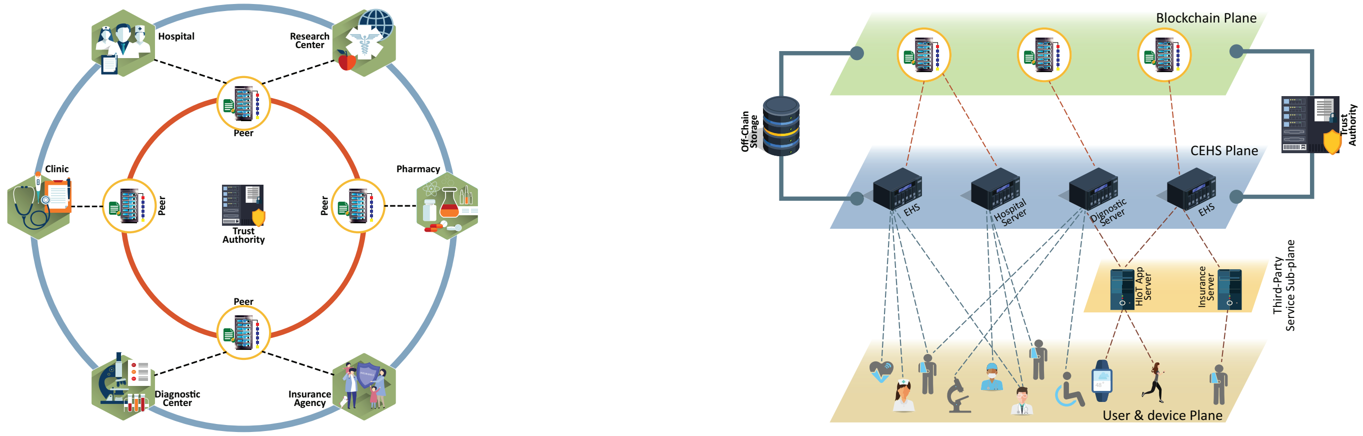
In this section, we cover the relevant state-of-art research works in the respective domains.

Conventional E-Health Security Solutions: Since the centralize architecture processes everything at a single point, hence most of the contributions focus on efficient security and privacy assurance by adding extra processes to the existing centralized architecture. Most of these contributions are key (i.e. public/private key, biometric key, etc.) based access control solutions, such as [18] proposed a three-factor authentication scheme using both asymmetric and symmetric crypto-systems which could meet most security needs. In [19], authors discuss the limitations of three-factor key authentication which is unable to resist the insider attack and propose a new three-factor scheme based on the elliptic curve discrete logarithm problem. Moreover, the authors added additional findings such as useless user identity, no session key, no mutual authentication, and impersonation attacks, etc., to present a new scheme [20], which is more costly than the previous. [21] proposed a solution considering user-centric security issues, where a single user acts as both the data owner and the data retriever. This scheme uses authentication key agreement schemes for accessing or submitting transactions. In most cases, the patient's data is accessed by multiple service providers in an EHS. Considering the issue, instead of single user [22], a multi-user Searchable Encryption Schemes (SES) is prosed in [23]–[25], that are capable of data leakage prevention. Although authors mostly focus on multi-users access control on the cloud-based server, data encryption or storage security is not considered strictly. Authors in [26] propose an SES based EHS which allows encryption and store data in cloud storage periodically as well as allows multi-users access keys. Moreover, the monitoring of remote patients and support of interoperability in intra-EHS services is claimed. [5], [27] discuss challenges that are faced in such centralized e-health systems. Although interoperability allows flexible data exchanges between EHSs, it also creates privacy leakage challenges. In [9], authors propose a biometric authentication based dynamic privacy protection mechanism using hash values. Although anonymity is maintained, however, all transactional and authentication data are stored in a centralized server. Authors [28] discuss the inference attack-resistant cloud system for access control. They propose a two-layer encryption scheme for fine-grained access control and a blind data retrieving protocol to confirm anonymous property. Mitigating the denial of service (DoS) attack [29], a smart card, and password-authentication based scheme has been proposed in [30]. It addresses DoS issues because of centralized storage, but a multi-user authentication based scheme is not possible. All the schemes discussed here are key-based security and privacy solutions for a centralized e-health system, which are still challenged by a single point of failure as well as interoperability among different EHS.

Blockchain-based E-Health Solutions: Some works related to blockchain and e-health has been done, which primarily focuses on adding security features to individual e-health systems in a centralized environment. Work in [5] proposes a pairing technology for data sharing in EHS using BC but does not describe the complete architecture for IoMT integration or unification at the national level. Similarly [31] suggests a BC-based continuous patient monitoring & data management while [27] presents concepts related to HoT devices and BC integration. These works do not consider core integration challenges, digital asset management, access control to digital assets, or transaction/block size constraints (such as 1MB [32] in Bitcoin [33]).

Blockchain for Access Control: BC has been used to some extent in providing access control in different domains. In [34], a BC-based distributed key management architecture for cross-domain access that satisfies fine-grained auditability and access control in IoT. It proposes a security access manager which is similar to the peer of a generic Blockchain that responsible for key management. In [35], authors propose a decentralized architecture for access control of IoT applications and BC is used for decentralization security. They use a permission delegation mechanism where a set of permissions is assigned for IoT devices/users which are checked every time. BC is only used to act as a permission delegation service based upon the device owner's smart contract. However, as there can be millions of IoT devices with different access requirements, creating a smart contract for each costly and sub-optimal.

Blockchain-based Access Control in EHS: Some specific



(a) Unified BC based EHS

(b) Complete ecosystem of BC-EHS

Fig. 1: BC based EHS access control framework

works have focused on the use of BC in EHS to provide access control. [36] proposes a BC-based EHR system that allows interoperability and integrity of data records, by using a collective authority. However, it does not consider the frequent changes in privileges (and thus the smart contracts), multiple EHS for a single patient, and large medical image data. Moreover, the use of incentives for block creation is unnecessary in a private or consortium blockchain. In [37], authors use BC for secure access to the medical history of patients. It performs mutual authentication among patients with common diseases and shows how physicians can access a patient's information. In [38] a BC-based privacy-preserving EHR sharing protocol is proposed where a keyword search & encrypted response based access control mechanism is used. However, all of these solutions only address a specific issue and provide a very basic solution for it. In this paper, we present a complete BC-based solution that not only performs data authentication and sharing, but also focuses on the diversified access control for different roles, cross-organizational challenges, big data challenges of EHR, medical data as transaction payload, smart contract and channel scalability, migration issues, and off-chain storage systems. To the best of our knowledge, there is no work which presents a similar solution.

3 System Architecture

The complete system architecture of a unified blockchain based e-health network is presented in this section. We first elaborate on the basic assumptions, followed by details of the system model and entities involved in it. The basic workflow is also described in detail.

3.1 Preliminaries

The objective of this work requires that some of the infrastructure and policies are established before such a unified architecture can be built. The first and foremost is the availability of blockchain network. It should be clear that the objective is to unify all e-health service providers under a single umbrella while allowing them to operate independently. Hence, each one of them cannot have their own BC network. We assume that such a unified BC network is established with governmental support and has national-level policies for service providers to comply with. This is quite realistic given the fact that the most advanced countries have national level health services. However, this is not a public BC, where anyone can join without authorization or authentication. The second requirement is that all users should be identified with a unique identifier, where it can be their bio-metric data including fingerprints and retinal scan along with their national ID number.

3.2 Architecture Overview

The complete architecture has been illustrated in Figure 1. It is important to understand that traditional hospitals and clinics are independent stand-alone entities with their information systems. Any patient who visits a hospital registers with that specific service provider, and has to register again if visiting another. This also means that each information system will have separate trust authorities (TA) for digital signatures and certificates, relational database systems for information storage, and application programming interfaces (APIs) for user apps.

Figure 1a shown the general structure of the unified system, where different e-health service providers are connected to the national/common blockchain network. Each service providing entity is connected to a single peer, while a single peer may provide services to multiple CEHS. The common TA is primarily part of the BC network responsible for all certificates, signatures, and keys in the complete ecosystem. Figure 1b shows a more detailed perspective interaction among entities, where the whole ecosystem can be visualized as a multi-tier architecture. The user plane at the bottom contains all types of users including patients, physicians, healthcare staff, IoMT devices, etc. A patient or physician may be associated with multiple entities in the CEHS server plane. This plane represents each CEHS as a server, which runs the mainframe application for that service provider. Each of these mainframes is in turn connected to peers in the backbone BC network. The Trust Authority of the ecosystem can be accessed by both the BC plane as well as the CEHS Server plane. Similarly, we introduce specialized off-chain storage facilities, which

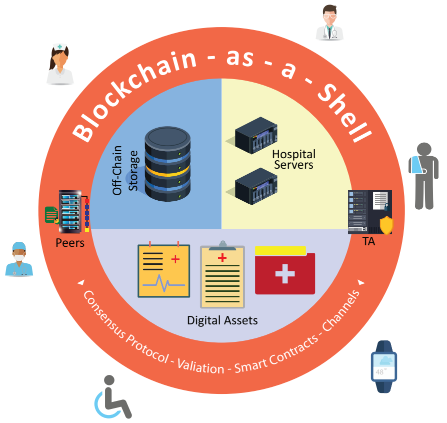

Blockchain - as - a - Shell
Off-Chain Storage
Hospital Servers
Peers
TA
Digital Assets
Consensus Protocol - Valiation - Smart Contracts - Channels
48°

Fig. 2: Conceptual structure of Blockchain acting as a shell restricting access to EMRs and other components.

can be accessed from both planes. The objective of these facilities is to allow large data storage which cannot be part of blockchain transactions. Finally, there is a sub-plane between the User and CEHS plane, which comprises of 3rd party IoMT application servers. Numerous IoMT devices (smart watches, medical sensors, etc.) upload their statistics to these servers, which can be synced with the e-health service providers servers. Figure 2 presents the conceptual structure of the system, where Blockchain works as a shell around the core entities of the system. Access to sensitive data and other elements is only possible, if the BC Shell allows it, hence making it resistant to the data breaches and insecure access. In the proposed system, any kind of data store is not accessible until the user passes through the Blockchain-based access control mechanism. As the access control is decentralized, hence the unified storage becomes much more resilient to service attacks and breaches.

In the following sections, different elements of each of the planes are discussed in further detail.

3.3 The User & Device Plane

In the proposed infrastructure, there are different kinds of users, which can primarily be grouped into three classes: patients, healthcare personnel, and devices. Patients are the main users of the system, while the other two can be considered as health service providers (SPs). It is important to note that the service providers are selected by the patient, which forms a group. An SP may be a member of multiple groups, each of which is centered around a patient. To ensure the privacy of the user and restrict access to their data, it is extremely important to define customized access policy for individual groups. Nature and purpose to access data of each SP are different, for example, a physician may have complete access to current records, while a pharmacist may only access the currently prescribed medication. Before any user can become part of a group or even access the network, they must register with the system using their biometric data. The registration process is defined in section 4.

An important point to note here is that a patient may visit multiple hospitals that could be independent of each other, however, they are recognized through their unique ID across the ecosystem. The same principle applies to healthcare personnel. On the other hand, IoMT devices are usually associated with a specific user at any given point in time. Moreover, in our system, IoMT devices are limited to sensors and similar measurement devices which monitor the statistics of a patient [9], [39]. Hence, a computerized tomography machine is not necessarily an IoMT device and more of a service provider.

3.4 E-Health System Plane

This plane primarily represents the conventional e-health system (CEHS), however, in the proposed unified system its components have been redefined for new roles and functions. In the traditional structure, a single CEHS would maintain an application server that would run the main user interface, a certificate authority (CA) for its users, and a relational database for information storage. Once the complete ecosystem migrates to a blockchain based system, the purpose of some of these elements may not be required. Here, we define the current and future role of these elements in details.

3.4.1 *Certificate Authority (CA)*

In any information system, individual credentials are required for communication among front-end applications, back-end server, and other programs. These credentials include Transport Layer Security Certificate (`TLS cert`), enrollment certificate (`eCert`), digital signatures, public key (`pk`), and private key (`sk`). In a CEHS, the CA generates and maintains an active list of these credentials for all users and devices. Moreover, these credentials are also generated for remote devices such as a collaborating diagnostic center's server, or an insurance agency's server.

In the proposed migration process, the CA must bind each user to a unique biometric ID, each device to a unique ID (for the whole ecosystem), and any remote service to a unique identifier. Following this, it performs a one-time registration process with the TA of the blockchain network. It is imperative that all members $m_i \in \texttt{CA}$, must become $m_j \in \texttt{TA}$ in the unified BC network. Following this, all authentication and credential generation for m_j is done by TA, and any new registration for a user is also handled by TA. This process practically elements the requirement of CA after a CEHS has joined the common BC network.

3.4.2 *E-Healthcare Server (S')*

This is the mainframe of any e-health information system, which runs the backend applications, websites, remote access destination, and hooks the whole system with the relational database. In a unified system, this is the anchor point for all local activity and connecting point for the CEHS to the BC backbone. Let S' represent the CEHS server, then there is a direct connection between S' and a corresponding peer in the blockchain. Hence, S' deploys additional modules to forward transactions to the peer network and obtain results and responses accordingly. Furthermore, a specialized module to handle the relational database is used which treats the DB as off-chain storage for the BC network. The relational database itself can be locally present or stored in the cloud. Distributed Ledger Application (DAP) executes a migration script (similar to Catena [40]) which synchronizes the relational DB with the blockchain file DB.

3.4.3 Third Party Sub-plane

This plane represents servers that are not part of a conventional e-health service provider but are present in the ecosystem. The prime examples are, IoMT application servers and insurance agency servers, that are represented as S''. In common practice, a user may have several wearable IoT devices, which may be manufactured and maintained by different vendors. Some of them may communicate and upload data to S', while others may use a mobile phone app to upload it to a third party application server (e.g. Fitbit, etc.). In some cases, S' can sync with the third party servers to obtain the sensory data. Hence in the proposed architecture as shown in Figure 1a, the IoT devices can send the data to S'', which can then be connected to a hospital's information system in the e-health system plane. A similar approach can be used for insurance agencies. However, this connectivity and sharing of information are not in the scope of this work. We assume that S' has obtained the data only after S'' has been registered with CA, and after migration with TA.

3.5 Blockchain Plane

This plane mainly comprises of the complete blockchain network maintained by a single authority. Different elements can be distributed geographically, but are linked through the Internet and work as a unified system. Here, we explain three main entities that are implemented through this plane.

3.5.1 Peer Network

This is the core blockchain network which comprises of peer nodes. In this work, we propose that there should be a minimum of three peers in the network for Byzantine fault-tolerant consensus formation. In a real-world scenario, the number of peers may increase, however, it should be noted that more peers also increases the consensus processing time. Let P be a set of all peers, while $P^E \subseteq P$ represents the endorsing peers for a given transaction. Every $p_i^E \in P^E$ must hold the smart contract (SC) which is used to validate the terms of the transaction between two elements, and take part in the consensus formation.

In Hyperledger Fabric a specialized *Orderer* is used as a leader for block creation, while in Ethereum the concept of *Leader Peer* is used for block creation. In this work, the architecture is not specific to either of these design choices, hence our solution can work with any type of BC implementation. In this work a peer acts and an anchor peer for an S' (and possibly for S''), creating a bridge between the leader peer/orderer and the transaction initiator element. Consequently, the transactions received in a *block formation time* are verified by P^E and added to the block B_i. As all peers maintain the ledger L, hence B_i is committed to all P, where it is linked with the last block (B_{i-1}) and stored. The ledger itself has two parts as *World State* and *block chain*. The newly generated transactions use the world state as a key-value store for indexing, whereas blockchain stores all transactions as blocks for historical information.

3.5.2 Trust Authority (TA)

TA plays an important role in a blockchain network, by providing different certificates and digital signatures to all the elements of a BC network. These elements include peers, orderer, users, devices, channels, and third-party servers. It is important to note that TA is an integral part of any BC implementation, and should not be considered as a single point of failure. They are implemented using clusters and have redundant backup systems. Hence, the TA acts as a Membership Service Provider (MSP) for the unified e-health network.

As described earlier, during the migration process, CA of every CEHS registers all existing users with the TA. Afterward, any new user is directly registered with the TA by S' without any intervention of CA. TA generates the required credentials during this instantiation phase, which are then used with every transaction generated by that user. Any change to credentials is done through a specialized policy transaction τ, which is explained in later sections. As shown in Figure 1b, the TA can be directly accessed by the elements of EHS plane and BC plane.

3.5.3 Off-chain Storage

In a conventional independent EHS, the back-end server always maintains a local relational database as part of the information system. It is important to note that the digital assets in EHS are usually large images, such as CT scans, MRI images, etc. Their storage in a relational database is only limited by the hardware storage capacity which can be increased easily at any time. On the contrary, in a blockchain based system, the storage of information or digital asset exchange is done through transactions, where all relevant data (images, etc.) should be part of the transaction. The transactions (in the form of blocks) are stored in a file-based ledger, which cannot store large images. The typical size of a single block in any BC system is limited to a few megabytes, as it directly impacts the performance of the system.

In this work, we use the concept of off-chain storage, accessible from both the BC plane and EHS plane, as shown in Figure 1b. This storage can be distributed, clustered, or cloud-based. Moreover, the relational DB of CEHS can also be treated as off-chain storage. The transactions maintain a pointer to digital assets stored in the off-chain storage rather than large data itself. This ensures that hardware changes to storage system have zero effect on BC system, while volume of big data does not negatively effect the Ledger. The off-chain storage is only accessed when the transaction to retrieve data is validated and the concerned transaction contains the pointer to the heavy data element stored in off-chain. It is important to note that, the pointer is encrypted data and can only be retrieved if the BC validates the query. This process is explained in later sections. The data in off-chain storage is encrypted locally, which can be easily implemented by traditional local database systems. However, in this work, we propose that such big data should be anonymous, and any identifiable information should only be part of the transaction in BC. Hence, even if the off-chain is compromised and encryption is broken, the data cannot be linked to any patient. Moreover, the transaction stores the hash of the such digital assets, and cross checks with the retrieved data to ensure its integrity.

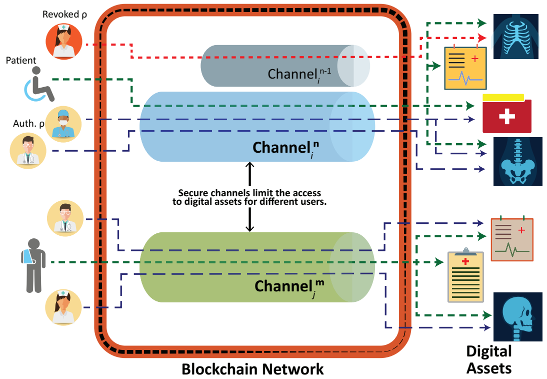


Fig. 3: Digital asset access control through channels.

3.6 System Work Flow

The objective of this work is to establish the basic parameters of migration of conventions EHS towards a unified blockchain based e-health network. Based on the system architecture and element details described above, this objective can be achieved in three phases.

In the first phase, every entity like patients, service providers, CEHS & BC network elements are registered with the TA. A described earlier, this process can be automated for existing users, and then can be done on a need basis when new users join. Details of this process are given in section 4. Once the users successfully receive their credentials, they can generate a transaction to store newly created digital assets (from sensed data, diagnostic reports, scans, prescriptions, etc.), or query to retrieve these digital assets in a secure, privacy-preserving, and controlled manner. The second and third phases of the ecosystem ensure this digital asset access and are described in section 5.

For a *transaction*, the patient or service provider originates and sends the transaction to the anchor peer using their credentials as well as SC information. It is important to note here, that we assume that appropriate APIs have been developed for users to create and forward a transaction. This task is trivial and not part of this work. The peer verifies the signature of the transaction originator and contract between both parties and approves it through consensus with other peers. When the positive acknowledgment is received, the transaction originator can upload large data to off-chain storage while the transaction itself is committed to the Ledger. In a similar process, user/service provider initiated *queries* are sent to the related peer, which verifies the SC for permission privileges of the requester. Given a positive acknowledgment is received by the requester application and the desired pointer to digital asset exists, the requester is allowed to retrieve the off-chain data.

4 Setup & Registration Process

In the proposed unified blockchain based e-health system, there are three broad categories of elements that are involved directly in registration. Users (υ), who are service seekers i.e. the patients. Service Providers (ρ), who process user data and provide medical services, i.e. physicians, devices, healthcare works, etc. Peers (P) are the BC nodes that maintain and update the records with the help of associated components. Below, we first explain the different credential management points followed by the registration algorithms.

4.1 Credential Management

To ensure a user (patient) centric security and privacy-privilege model, it is imperative that all access to a patients data is controlled by the patient themselves. Hence, in our scheme, the patient is responsible for creating and maintain a channel and the associated smart contract, both of which jointly dictate who can access which digital asset related to the user. Besides, a specialized compound key is used for authentication. These three elements are described in detail below.

4.1.1 Channel Management

A channel is a user/patient υ_i defined private group for communication, used to conducting private and confidential transactions between its members $\rho_x^{\upsilon_i}$. Any transaction to or from members is executed on a specific channel and members must be authenticated and authorized to transact on that channel. During the sign up process, υ_i creates a new channel through the SDK/APIs, which is added to the genesis block of the blockchain and stores the configuration information about channel policies and members. Any change to an existing channel is in the form of channel updates. The user υ_i generates a specialized transaction and encrypts the payload information by $\texttt{sck}_{\upsilon_i,\rho_x}$. Peers in the network approve the transaction and update the ledger. Here, $\texttt{sck}$ is a secret compound key only known to current valid members (ρ_x) of the channel. Also, the channel can be viewed as an RBAC enforcer. However, as described earlier, access to data is based on permission to execute the transaction, and the different types of transactions (discussed later) determine if a specific role will be able to generate or access data elements.

4.1.2 Smart Contract Management

Any registered user and service provider can initiate a transaction (if they are allowed) on a channel, however, their control over digital assets and the validity of the transaction is dictated through the smart contract among them. In this research, we use a user-centric smart contract where the smart contract is defined based upon the service provider group. In other words, a smart contract is created for a group of users or service providers, where individual access rights are limited through policy transactions. This allows multiple service providers to be part of the channel while having limited access to information related to the patient.

4.1.3 Secret Compound Key Generation

The previous two elements are related to the authorization of entities for asset control and transaction verification. For authentication, we make use of a secret compound key ($\texttt{sck}$) created by the TA for a specific channel version. Any changes in the channel properties, i.e. member addition, change in SC, creates a new version of the channel, which triggers the generation of a new $\texttt{sck}$, only known to the members of that channel version. The generation process is described in the next section. It is important to note that the $\texttt{sck}$ is used to determine the privilege to generate a

Algorithm 1: User υ_i registration and credential generation process at TA

```
Input  : $(\texttt{Bio}^{\upsilon_i}, \texttt{ID}^{\upsilon_i}, \texttt{Pass}^{\upsilon_i})$
Output: 0:Failure / Credentials:Success
set flag $\leftarrow 0$
set $\acute{\text{Bio}} \leftarrow$ hash$(\texttt{Bio}^{\upsilon_i} + \texttt{ID}^{\upsilon_i} + \texttt{Pass}^{\upsilon_i})$
set $\widehat{\text{Bio}} \leftarrow$ query.NationalDB$(\texttt{ID}^{\upsilon_i})$
if $\texttt{Bio}^{\upsilon_i} \equiv \widehat{Bio}$ then
    cred$^{\upsilon_i} \leftarrow$ cryptogen$(\upsilon_i)$
    TA.registry $\leftarrow (\acute{\text{Bio}} + \text{cred}^{\upsilon_i})$
    flag $\leftarrow$ cred$^{\upsilon_i}$
    peer.CreateChannel(cred$^{\upsilon_i}$)
        \\ peer invokes algo. 3 in turn
end
return flag
```

Algorithm 2: Compound Key Generation Process

```
Input  : $(C_i^{\text{ID}}, \upsilon_i^{\text{ID}})$
Output: Compound Secret Key (sck)
Initialize $SP^{\upsilon_i}$ as a list
  $\texttt{sk}_{\varepsilon_{nc}}^{\upsilon_i}, \texttt{pk}^{\upsilon_i} \leftarrow$ cryptogen$(\varepsilon_{nc}(\,))$
while $SP$ do
    $\texttt{pk}^{\upsilon_i} \rightarrow \forall_{SP_i}$
    Resp[ ], $\texttt{pk}^{SP_x}[\,] \leftarrow$ response$(SP_i^{\upsilon_i})$
end
if Resp is True then
    sck $\leftarrow$ compound.key$(\texttt{pk}^{\upsilon_i}, \texttt{pk}^{SP_x}[\,], \texttt{sk}_{\varepsilon_{nc}}^{\upsilon_i})$
end
return sck
```

transaction on a channel. Each transaction is bound to a sck, hence, without the correct sck, previous transactions cannot be retrieved. An old sck of an earlier version of the channel can enable a service provider to retrieve it. This is allowed by design, as an old service provider may retain legitimate access to the previous medical records of a patient. However, this allows only limited access to specific data elements. Note that the transaction once committed cannot be modified, hence, they will be able to read it but not modify it. Similarly, the old sck cannot be used to generate new transactions for data creation. On the contrary, if the access of a medical service provider has to be revoked completely (i.e. even to the transactions generated by them), then such a restriction has to be enforced by TA, and such a scenario may have legal ramifications.

4.2 Registration Process

Every entity and element in the whole ecosystem needs to register before it can communicate over the blockchain network. These include not only the patients and service providers, but also servers, devices, application modules, peers, orderer, and storage devices. Primarily from registration algorithms perspective, they can be divided into two types: *i*) the patients which own the channel, and *ii*) all other components which may become a member of a channel. The algorithms for each are discussed below.

4.2.1 User (υ) Registration Process

User registration follows the process shown in Algorithm 1. For all users who are already registered with the CA, the migration to TA can be automated as a one time process. Any new user is directly registered with the TA in a unified system. In this work, we use biometric-based identification along with a national level ID. TA first cross-checks the biometric information of the user ($\texttt{Bio}^{\upsilon_i}$) against the stored information in the national database ($\widehat{\text{Bio}}$). Credentials (signatures and keys) are only generated if this verification is passed. The TA then stores the hash of biometric data, national ID along with new keys for each registered user for future reference. Storing hash also prevents stolen DB [9] attacks. Finally, the TA calls for channel creation by the peer for the new user. Channel creation is a generic blockchain process, hence we do not describe it as it depends on the blockchain implementation. However, we propose that as part of the channel creation the peer should use Algorithm 2 to generate the secret compound key. Initially, the service provider list in Algorithm 2 may only include the EHS server the patient is visiting, but can later expand to include other elements.

For logging into the network, the user υ_i provides biometric along with ID and password. Combination of these three as hash$(\texttt{Bio}^{\upsilon_i} + \texttt{ID}^{\upsilon_i} + \texttt{Pass}^{\upsilon_i})$ is verified by TA, and approved for generating transactions.

4.2.2 Component Registration

Every network element, as well as applications, are required registration for ensuring that only legal entities can access the digital assets of patients. These include the servers, peers, orderer, devices, third-party application servers and devices, and healthcare providers. None of these components are allowed to generate the channel or invoke the sck generation process. Moreover, biometric identification is not possible for them, hence their registration is done by the administrator of the system, and is essentially limited to credential generation by TA. For the BC plane elements such as orderer and peers, the administrator can execute the cryptogen() method and configure the keys. A similar process can be adopted for servers in the EHS system plane. An important point to note here is that any IoMT device should always be registered in a pair formation {S,D} with the TA, where S is the connecting application server, and D is the device ID. The same holds for third-party IoMT devices, which push data to third-party servers. Hence, the credential generation is also in pair form as cryptogen$(\texttt{S}_\texttt{i}'', \texttt{d}_\texttt{j})$.

5 Transaction Based Access Control

Access to digital assets is granted by the owner, i.e. the patient, during the registration process & the channel is specifically created for this purpose. To grant/revoke privileges to different service providers a specialized policy transaction $\mathcal{T}$ is generated by υ_i. For any service provider to create or access a digital asset, they generate a data transaction δ. Below we describe each type of transaction and algorithms that govern the permissions' access control.

5.1 Policy Transactions (τ)

In the proposed patient-centric EHS system, υ_i instantiates or modifies the permission privileges of any other entity towards its digital assets. Let $R^{\upsilon_i} = \{R_1, R_2, \ldots, R_n\}$ be a set of digital assets belonging to υ_i, where R represents all

```
Algorithm 3: Permission Checking Process
   Input  : $(\mathtt{sck}, \rho_i, \delta, \mathtt{pk}^{\rho_i}_{\text{sign}}, \mathtt{pk}^{\upsilon_i}_{\text{sign}})$
   Output: Ture/False
 1 validate sck   \\ (from genesis Block)
 2 validate $\mathtt{pk}^{\rho_i,\upsilon_i}_{sign}$  with $\delta$
 3 if validations hold then
 4     $R_{\text{list}}[\,] \leftarrow$ extract($\forall R \longmapsto \rho_i$)
 5     if ($\delta$ in $R_{list}[\,] \wedge \mathtt{SC}_{\upsilon_i \leftrightarrow \rho_i}$) then
 6         return True
 7     else
 8         return False
 9     end
10 else
11     return False
12 end
```

assets and $R_j^{\upsilon_i}$ represents a specific asset. The permission policy for any digital asset can be of three levels: create, read, or both. It is important to note that, for the sake of transparency and tracking, there is no modification possible to an existing data element in blockchain or health records. Hence, any change to a digital asset is considered as a new digital asset with a timestamp. In this work, the permission level is represented as $\overset{\cdot}{\longmapsto}$, where the number of dots represents create, read, and both respectively. Hence, to grant read permission for a specific physician $\mathtt{Py}_i$, υ_i generates $\mathcal{T}= \{R_i \overset{\cdot\cdot}{\longmapsto} \mathtt{Py}_j\}$.

The smart contract of a patient dictates which type of ρ_i can be granted what type of permissions. For example, the contract may restrict that a diagnostic center ($\mathtt{DC}_k$) may only create new medical reports (as digital assets), but never read or be able to create and read at the same time. Similarly, it may restrict a physician to have only access to specific assets and not all assets, while another physician may have complete access to read or create new prescriptions. Hence, in a single policy transaction, υ_i can group different permissions as $\tau^{\upsilon_i}= \{R_i \overset{\cdot\cdot}{\longmapsto} \mathtt{Py}_i, R \overset{\cdot}{\longmapsto} \mathtt{DC}_k, R \overset{\cdot\cdot\cdot}{\longmapsto} \mathtt{Py}_k, R_m \overset{\cdot\cdot}{\longmapsto} \rho_n\}$. As the transaction is initiated by υ_i, hence it is by default assumed that all R referenced in the transaction belong to it. Note that, create permissions are given to set R, and not a specific R_n. Moreover, for any block, there can only be one transaction from a user. The initiated transaction is received at the anchor peer. Peer verifies and approves a $\mathcal{T}$ through the consensus process which includes credentials and smart contract verification of relevant parties. The resultant of this execution requires generation of a new sck by TA as described in Algorithm 2, which is then stored in the genesis block as a new version of the channel specified for that υ_i.

The compound key formation process ensures that whenever a new access rights a granted, the compound key to enable transaction on the channel is also update. Every single key is generated against a specific channel and restricted within channel members, as approved by the patient. In Algorithm 2 line 3, υ_i choose the service providers, and consequently, an irreversible hash is used to generate a new key based on public keys of all service providers & user, and secret key of the user. As the hash is not reversible, hence individual keys cannot be extracted.

5.2 Data Transactions (δ)

In these types of transactions, the objective is that the requester is either creating a digital asset or retrieving a digital asset from the blockchain or off-chain storage. Unlike τ where the initiator owns the channel, δ is generated by service providers, who may or may not be allowed to send a transaction on that specific channel. Hence, Algorithm 3 is used by the anchor peer to first verify the legality of the transaction. The algorithm takes the transaction δ, sck of the channel, and public key of υ_i & ρ_j provided by the sender of the transaction. It then checks whether the provided sck is valid for the requester from the genesis block, followed by validation of signatures as provided by the sender against the ones encrypted in the transaction. This ensures that the sender has the right to send a transaction on this channel, and is also the originator of the trade. If both checks pass, then in line 4–7 we extract the policy list for requesting ρ_j, and return a positive response if δ is allowed. If any of the checks fail, a negative response is sent and anchor peer immediately rejects the transaction.

Once the verification is positively complete, the leader peer has to execute the requested transaction. Here, we classify the data transactions into two categories: Query Transaction ($\check{\delta}$), which is done to retrieve existing digital assets, and Payload Transaction (δ), which is done to create new digital assets. The payload transactions have a specialized type ($\bar{\delta}$) due to the size of the digital asset. The processing of each is explained below.

5.2.1 Query Transaction ($\check{\delta}$)

On the reception of this transaction, the anchor peer executes Algorithm 3 as described earlier. It is important to note that the query is received from the elements of the EHS plane, hence, the response of validation is sent back to the concerned server/application. Only if the response is positive, then the rest of processing as shown in Algorithm 4 is done by the EHS server. It is important to note that, the $\check{\delta}$ is not sent for consensus and locally verified by the peer. This improves the efficiency of the blockchain network, without compromising security and privacy. Any query to retrieve a digital asset contains the Digital Asset ID, which is used to retrieve the original transaction from ledger L of the peer, as shown in line 4. If the digital asset is a simple string (e.g. a prescription, or dosage of medication) then it is stored as part of the transaction, otherwise, if it is an image (or a file) then it is stored separately in the off-chain storage. This process is explained in the next section. In line 5 the transaction ($\mathtt{T}_o$) is parsed to the retrieve digital asset, and if it contains a hash corresponding to an off-chain file, then it is extracted & appended to the response as shown in line 6–9. Finally, the response is sent back to the originating user of the transaction.

5.2.2 Payload Transaction (δ, $\bar{\delta}$)

A regular transaction by any of the current channel members (i.e. with current sck) is executed as a payload transaction, where the objective is to add a new digital asset to the blockchain network. For example, $\mathtt{Py}_j$ prescribes a medication to the patient (υ_i), hence the transaction is executed as δ, and the digital asset (i.e. prescription) is stored as a string in the ledger. However, if the digital asset cannot be stored as a string, then it cannot be part of the blockchain in Ledger. The size of ledger transactions and blocks do not allow it, as discussed earlier. Hence, to address this challenge, we

Algorithm 4: Query Transaction

```
Input  : $\check{\delta}$
Output: $\check{\delta}_{\text{Rsponse}}$
if Algorithm 3 returns False then
    Abort
end
$\mathtt{T_o} \leftarrow$ retrieve($\check{\delta}$.DigAsstID, $L$)
$\check{\delta}_{\text{Rsponse}} \leftarrow$ parse.JSON($\mathtt{T_o}$)
if $\check{\delta}_{Rsponse}$.data  contains  hash(DigAsst) then
    $D_{\text{Asst}} \leftarrow$ search($\check{\delta}_{\text{Rsponse}}$.DigAsstID.path)
    $\check{\delta}_{\text{Rsponse}} \leftarrow$ JSON.merge($\check{\delta}_{\text{Rsponse}}, D_{\text{Asst}}$)
    return  $\check{\delta}_{\text{Rsponse}}$
else
    return  $\check{\delta}_{\text{Rsponse}}$
end
```

Algorithm 5: Payload data Processing

```
   Input  : $(\mathtt{sck}, \rho_i, \delta, \mathtt{pk}^{\rho_i}_{\text{sign}}, \mathtt{pk}^{\upsilon_i}_{\text{sign}})$
   Output: Success/Failure
1  if Algorithm 3 returns False then
2      return  Failure
3  end
4  $D_{\text{Asst}}, \mathtt{T_o} \leftarrow$ parse($\delta$)
5  if $D_{Asst}$  exists then
6      $\overline{D_{\text{Asst}}} \leftarrow$ hash($D_{\text{Asst}}$)
7      $P_{\text{off-chain}} \leftarrow$ generate(offChainPath)
8      $\mathtt{T_o} \leftarrow$ append($\mathtt{T_o} + \overline{D_{\text{Asst}}} + P_{\text{off-chain}}$)
9  end
10 $\mathtt{T_o} \rightarrow$ LeadPeer\Orderer       \\ for block formation
11 if $\mathtt{T_o}$  Commit  recieved then
12     if $D_{Asst}$  exists then
13         upload($D_{\text{Asst}}$, $P_{\text{off-chain}}$)
14     end
15     return  Success
16 else
17     delete($P_{\text{off-chain}}$)      \\ for $D_{\text{Asst}}$ only
18     return  Failure
19 end
```

use a specialized payload transaction $\bar{\delta}$ that is processed differently.

From the transaction initiator's perspective, they create a complete δ, which contains all types of digital assets. The classification is done at the peer level, where the heavy payloads are separated from the rest of the data and stored in off-chain storage. The rest of the transaction is verified and committed to the ledger. Algorithm 5 shows this complete process at the peer. After receiving the transaction, the peer first validates all parameters as given in Algorithm 3. For a valid transaction, the peer first determines if it contains digital assets that are too large for the block. Following this, the transaction is parsed to extract any large digital assets from the string data in line 4. In line 5-9, a hash of digital asset is generated, a path in off-chain storage is determined, and the hash and off-chain path are appended to the transaction $\mathtt{T_o}$. Hence, the transaction becomes purely string based and within the size requirements of BC systems. At this point in the algorithm, $\mathtt{T_o}$ is ready to be sent for consensus to P'. As discussed earlier, consensus formation and block creation is done by the leader peer or orderer depending on the BC implementation. It is possible that the anchor peer is the leader peer for the current block. In any of the cases, all peers in P' use Algorithm 3 to validate the transaction and respond with positive feedback if validations hold. On completion of block formation, the anchor peer is notified of the commit, which in turn uploads the digital assets to off-chain storage (if applicable), and sends a success message to the user. If the validations fail at any point the transaction also fails.

6 Analysis and Evaluation

The objective of this research is access control of digital assets by different elements of a unified blockchain based e-health system. In this section, we first present an analysis of the complete scheme on how it addresses some of the challenges in the unified system. In the later part, we present quantitative evaluations of performance, for which we have implemented a unified model (with proposed access control) and a unified but non-blockchain EHS system for comparative analysis. The non-BC model does not implement any access control and works as a central point for handling transaction (native request) from multiple EHS. In the unified BC-based model, the EHS application generates transactions are JSON format for a Hyperledger Fabric based blockchain network. The three peer network is emulated using docker environment on an Intel i7 2.7GHz system, while the orderer and TA run on an Intel i5 3GHz computer. A Kafka-zookeeper based ordering service generates the blocks a one block per second, while the off-chain database uses MongoDB to store the digital assets. Node-red is used to generate parallel transactions (or queries) between the range of 1–50 depending on the evaluation scenario. The algorithms designed are implemented as integral part of Fabric code, while a synthetically generated EMR dataset is used to create payload for transactions.

6.1 Design Analysis

Blockchain technology was primarily designed for cryptocurrency and it has been effective in several examples such as Bitcoin [33], Ethereum [15]. Its adoption for other domains such as business processes, access control, and logistical tracking, has opened new challenges of scalability, ledger expansion, complex data structures, interoperability, and privacy, etc. Some solutions have addressed the scalability and ledger expansion especially in IoT [11], [41], [42], however, these solutions may not be as effective for large scale e-health systems. From the proposed solution and its details, once can identify the unique features of and EHS as, privacy of patient's data, ubiquitous nature of transactions (i.e. sensor data, medical images, textual reports, historical information, bills, insurance payments, etc.), frequent changes to smart contract, continuous data generation, third-party application access, and collaboration among different administrative e-health network. Below, we present the analysis of the proposed solutions for some of these challenges.

6.1.1 Scalability

Medical data exists in various types such as heavy images (x-ray, ECG, CT-scan), documents (pathological report), strings (prescriptions), etc. However, storing all of them in the file-based structure of ledger is not possible, not only due to the structure of the database but also due to the limits on the size of transactions and blocks. For example,

TABLE 1: List of Symbols used in Section 6.1.

Symbol	Meaning
δ_ω, $\bar{\delta}_\omega$	Transaction weight without/with Digital Asset
$\delta^{\mathbb{B}}_\omega$, $\bar{\delta}^{\mathbb{B}}_\omega$	Transaction weight in Block without/with Digital Asset
δ_o	Transaction overhead size
$\mathbb{B}_\omega$	Block weight
$\mathbb{B}_o$	Block overhead size
$\mathcal{H}^j_\omega$	Hash & Path weight for Digital Asset of jth transaction
$\mathcal{S}^{P'}_\omega$	Sign weight of endorsing peer
$\mathcal{F}_\omega$	Flag weight of chaincode response

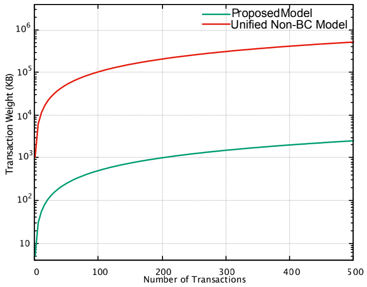


Fig. 4: Comparison of transaction weight growth.

the maximum limit of block size in Bitcoin is 1MB [32]. Even if the limit is removed or increased, other factors are adversely affected by transaction size. Bandwidth requirement is the prime among these. As each transaction has to be validated by peers, hence sending digital assets across the network for validation significantly increases the bandwidth requirement of the network. In the proposed work, we use an off-chain storage, while ensuring that the hash and path of the asset are part of the transaction. Until access to these is not given, any element cannot retrieve the digital assets. Based on the scheme the size of a block can be calculated by (1), and Table 1 gives the description of symbols.

$$\mathbb{B}_\omega = \sum_{i=1}^{n} \delta^{\mathbb{B}}_{\omega i} + \sum_{j=n+1}^{m} \bar{\delta}^{\mathbb{B}}_{\omega j} + \sum_{k=1}^{m} \delta^k_o + \mathbb{B}_o \tag{1}$$

Here, we assume that the leader peer/orderer arranges the transaction in a candidate block such that the transaction without digital assets are listed before the ones with digital assets. Hence, n is the number of transactions without digital assets, and m is the total number of transactions in the block. The transaction overhead is computed as,

$$\delta_o = \sum_{i=1}^{e} \mathcal{S}^{P'_i}_\omega + \mathcal{F}_\omega$$

where e is the total number of endorsing peers P' participating in the validation of that transaction. The weight of a transaction with digital assets as created by the user is calculated as,

$$\bar{\delta}_\omega = \delta_\omega + \sum_{j=1}^{x} \mathcal{H}^j_\omega$$

where x is the number of digital assets in this transaction.

Figure 4 illustrates the significant difference in ledger growth against a varying number of transactions per block, while Figure 5 depicts the bandwidth requirements for consensus formation of one block per second in the blockchain.

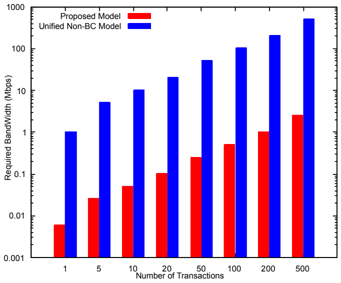


Fig. 5: Required bandwidth analysis.

Both figures show the comparative result of the proposed work with a generic blockchain solution, where digital assets are forcefully made part of the transaction, and stored in the ledger. Endorsing peers P' for each transaction is set to three. It can be observed that the memory requirement per block is approximately 0.5 GB when the number of transactions per second is 500, while every digital asset carries maximum 1MB (average 500KB). For a normal e-health system to work, it would be fair to assume that 10K transactions per second would be created across the different EHS nodes. Hence, using 0.5 GB as a baseline, the required memory size in the ledger would be impractical. On the other hand, the proposed solution uses off-chain storage, which eliminates such requirements, and the ledger size remains practical. Similarly 515 Mbps (approximately) of bandwidth is required per block with 500 transactions which is very costly for an EHS. With the increase in the number of peers, this value will rise, as the complete transaction has to be sent to each endorsing peer for validation.

6.1.2 Access Control

In an EHS network, any data of a user (patient) is private and should only be accessed by authorized personnel. Unlike, traditional blockchain users who have equal rights (for trading or creating transactions), in an EHS role of ρ varies. A physician treating the patient may know them by name, while a physician conducting a general analysis or survey should get the same data but anonymized. Moreover, a patient's physicians may change over time, which will require that old service providers do not have access to new data. All of these access control schemes are usually implemented through smart contracts. However, implementing smart contracts, and changing them frequently is costly for a blockchain network.

In the proposed work, this challenge is solved through a patient-centric model, where the owner of digital assets explicitly grants or revokes access to any of the other elements in the network. All elements which are registered with the `TA`, which adds another layer of protection to the system. Each time the users grants or revokes any service provider's access rights, a new version of the channel is created, keys are updated, and a new `sck` is generated. As all the previous versions of the channel are stored with the genesis block, hence past physicians may still be able to access past data which they are legally allowed to, but they may not access new data. Hence, frequent changes do not require new smart contracts, but rather only a new version

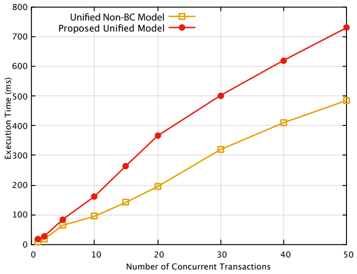
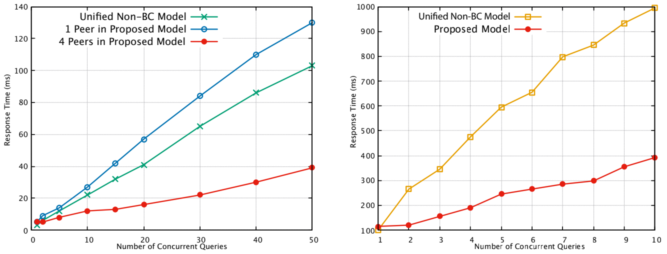


Fig. 6: Processing time of concurrent transactions.



(a) Without digital assets

(b) With digital assets

Fig. 7: Transaction time of query.

of the channel. This makes the system more robust and allows a patient-centric grouping scheme.

6.1.3 Single Point of Failure

Centralized systems are prone to denial of service attacks. As e-health systems are mission-critical, hence, their disruption can be life-threatening. Migrating and unifying national health services through blockchain eliminates the single points of failures. Primarily, the ledger is distributed and replicated, hence, the records can be obtained from any one of them. In our design, certain entities may be considered as a single point of failure but they are not.

Trust Authority: As all users and other elements are registered with the TA, hence, it becomes a central point for the whole ecosystem. It is important to note that current Internet architecture also works with similar certificate authorities, and in our design, it has to be implemented at the national level with appropriate protection. Moreover, it is not a single server, rather it is built using clusters with redundant backup systems. Thus, it is not easy to attack or disrupt the services of a TA.

Anchor Peer: Each EHS system is connected to a peer of the blockchain backbone network. However, this binding is only logical, and any peer can serve as an anchor peer for any EHS system. As the peers are identical in implementation and ledger, hence if one anchor peer fails, the system can seamlessly use any other peer as it anchor.

Off-chain Storage: These database servers can be in the cloud and the architecture does not put any constraint on their number or capabilities. Hence, they also do not form a single point of failure.

6.2 Basic Findings

The registration process for both patients and other elements are different due to channel creation and policy transaction completion. The average time to register any element is 3ms from log observations, while the channel creation takes an additional time depending on initial permissions. In most cases, this time is negligible (≈1–2ms), while with a larger number of policy changes the `sck` generation/distribution and τ completion required up to 1 second. It is important to note that the performance of the BC network is not affected by the size or number of digital assets, as they are not sent to endorsing peers. Hence, they are uploaded to the off-chain storage by a separate process on the anchor peer.

At this point, it is worth mentioning that the transaction rate of Hyperledger has significantly improved as compared to other blockchain solutions [43]. The major reason for the delay in committing the block is directly related to the consensus algorithm. The improvement in the performance of these algorithms will reduce the delay in future. In the next subsections, we specifically present the execution time analysis of the delay involved in the proposed solution.

6.3 Digital Asset Transaction Analysis

In this experiment, we evaluate the time required to complete a digital asset transaction in a unified BC-based and unified non-BC system. Figure 6 presents the transaction execution time in ms, and the x-axis shows the number of concurrent transactions submitted to the unified network. As discussed earlier, every BC based transaction is endorsed by 3 peers (in a 4-peer network), hence, a single BC-transaction takes approximately 18ms, while a non-BC system can process the digital asset uploading in 12ms. For 20 transactions non-BC requires 200ms while BC-based uses 365ms. Likewise, at 50 concurrent transactions submitted BC-based requires about 720ms while non-BC takes almost 0.5s. Hence it can be observed that the transaction execution/approval time increases steadily with a difference to the non-BC system. It is important to note that although the time required is higher, this is not due to the proposed architecture. The inherent complexity of BC systems (against the benefit of security) is the primary reason for this. As the blockchain systems will mature and efficient consensus algorithms are developed, this time will become at par (if not better) with the non-BC systems. Similarly, fine-tuning of the blockchain platform with respect to transaction size, block size, available bandwidth, desired transaction rate, log level, etc. can also be helpful. From experimentation, it was observed that minor misconfigurations or added system logs can add up to 20ms to block formation time.

6.4 Query Transactions Analysis

The query transactions are used to retrieve the digital assets from the off-chain DB or ledger by different types of users. In this experiment, we analyze the response time of the proposed system against a unified non-BC system. Figure 7a shows the performance for queries without digital assets (i.e. string data retrieved from ledger only) for 1-peer and 4-peer network, while Figure 7b represents the time for queries with digital asset retrieval from off-chain storage (4-per network only). It can be observed from Figure 7a, that an increase in load of verification and retrieval increases the response time for all models. However, the benefit of the BC-based system is the distributed nature of peers. As each EHS only has to connect to its anchor peer, hence the workload is distributed. This is evident from the performances of a single peer network which is essentially working as a unified non-BC model. Both verification and retrieval are done by a single point, hence it takes more time as compared to 4-peer network. It is important to note that the unified non-BC model does not enforce access control and user verification based on different types of policies and users, hence its processing time is lower than that of a single peer model. As the number of verifications increase, the single-peer model experiences a drastic increase in the response time. In terms of scalability, a BC-based system is more scalable than conventional centralized solutions, and provide better security for access control. However, more number of peers requires increased maintenance cost.

Figure 7b presents the time required to process the queries with digital assets stored in off-chain storage. Here we only show the proposed model with a 4-peer network against the unified non-BS model. It can be observed that the query response time is proportional to the number of concurrent queries. Compared to the queries without digital assets from off-chain storage, the response times are much higher in both cases. For a single query, the time required is identical in both models, but as the number of queries increases, the distributed nature of anchor peers give a clear advantage over a unified non-BC system. The difference is almost 2.5 times that of the BC-based model. Although, the performance depends on digital asset quantity and size, however, with approximately the same transactions BC-based model outperforms the centralized model.

7 Conclusion

The rapid spread of e-health systems and related health IoT devices has prompted a renewed search for security and privacy solution for data and users. Blockchain technology in recent years has enabled secure transactions for information exchange. In this article, we show that e-health systems can be made interoperable through a core Blockchain network. Independent EHS can be migrated to form a national e-Health network, where a patient's digital assets can be transferred from one service provider to the other using policy transactions. Moreover, as the digital assets cannot be stored as part of the ledger, we make use of off-chain storage to store the large volumes of data, while access to controlled by blockchain based channels. The emulated evaluations of the system show, that the solution is scalable in the face of an increased number of users and transactions, and the off-chain storage does not impact the ledger size.

References

[1] R. M. Scheffler, J. X. Liu, Y. Kinfu, and M. R. D. Poz. Forecasting the global shortage of physicians: an economic and needs based approach. [Online]. Available: https://www.who.int/bulletin/volumes/86/7/07-046474/en/

[2] Global digital health market from 2015 to 2020, by major segment (in billion U.S. dollars). [Online]. Available: https://www.statista.com/statistics/387867/value-of-worldwide-digital-health-market-forecast-by-segment/

[3] Estimated healthcare IoT device installations worldwide from 2015 to 2020. [Online]. Available: https://www.statista.com/statistics/735810/healthcare-iot-installations-global-estimate/

[4] A. K. Bairagi, S. F. Abedin, N. H. Tran, D. Niyato, and C. S. Hong, "QoE-enabled unlicensed spectrum sharing in 5g: A game-theoretic approach," *IEEE Access*, vol. 6, pp. 50 538–50 554, 2018.

[5] H.-T. Wu and C.-W. Tsai, "Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, 2018.

[6] S. Biswas, K. Sharif, F. Li, and Y. Liu, "3p framework: Customizable permission architecture for mobile applications," in *Proceedings of International Conference on Wireless Algorithms, Systems, and Applications*, 2017, pp. 445–456.

[7] S. Biswas, W. Haipeng, and J. Rashid, "Android permissions management at app installing," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 223–232, 2016.

[8] A. K. Bairagi, N. H. Tran, W. Saad, Z. Han, and C. S. Hong, "A game-theoretic approach for fair coexistence between LTE-u and wi-fi systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 442–455, 2019.

[9] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.

[10] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[11] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, June 2019.

[12] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, Jan 2020.

[13] S. Biswas, K. Sharif, F. Li, Z. Latif, S. Kanhere, and S. P. Mohanty, "Interoperability and synchronization management of blockchain based decentralized e-health systems," *IEEE Transaction on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, Nov 2020.

[14] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343–2355, Mar 2020.

[15] V. Buterin. A next generation smart contract & decentralized application platform. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[16] Hyperledger: Hyperledger Business Blockchain Technology. [Online]. Available: https://www.hyperledger.org/projects

[17] HDAC : Transaction Innovation - IoT Contract & M2M Transaction Platform based on Blockchain. [Online]. Available: https://github.com/Hdactech/doc/wiki/Whitepaper

[18] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 933–945, 2009.

[19] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *Journal of Medical Systems*, vol. 39, no. 10, Jan 2015.

[20] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[21] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[22] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proceedings of IEEE Conference on Computer Communications INFOCOM*, 2010, pp. 1–5.

[23] Q. Wang, Y. Zhu, and X. Luo, "Multi-user searchable encryption with coarser-grained access control without key sharing," in *Proceedings of International Conference on Cloud Computing and Big Data*, 2014, pp. 119–125.

[24] Z. Yaling, J. Zhipeng, and W. Shangping, "A multi-user searchable symmetric encryption scheme for cloud storage system," in *Proceedings of International Conference on Intelligent Networking and Collaborative Systems*, 2013, pp. 815–820.

[25] Z. Liu, Z. Wang, X. Cheng, C. Jia, and K. Yuan, "Multi-user searchable encryption with coarser-grained access control in hybrid cloud," in *Proceedings of International Conference on Emerging Intelligent Data and Web Technologies*, 2013, pp. 249–255.

[26] L. Yang, Q. Zheng, and X. Fan, "RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks," in *Proceedings of IEEE Conference on Computer Communications INFOCOM*, 2017, pp. 1–9.

[27] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–5.

[28] W. Zhang, Y. Lin, J. Wu, and T. Zhou, "Inference attack-resistant e-healthcare cloud system with fine-grained access control," *IEEE Transactions on Services Computing*, pp. 1–1, 2018.

[29] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.

[30] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 2, pp. 793–800, Feb 2010.

[31] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32 700–32 726, 2018.

[32] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Future Internet*, vol. 9, no. 3, 2017.

[33] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: http://bitcoin.org/bitcoin.pdf

[34] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34 045–34 059, Mar 2019.

[35] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in internet of things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, Sep 2019.

[36] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," *Concurrency and Computation: Practice and Experience*, Aug 2019.

[37] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118 943–118 953, Aug 2019.

[38] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136 704–136 719, Sept 2019.

[39] J. Kim, "Energy-efficient dynamic packet downloading for medical IoT platforms," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1653–1659, Dec 2015.

[40] T. van der Vorst. Catena - SQL on a blockchain. [Online]. Available: https://github.com/pixelspark/catena/

[41] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4694–4701, Nov 2019.

[42] G. Greenspan, "Scaling blockchains with off-chain data," MultiChain, Private blockchains. [Online]. Available: https://www.multichain.com/blog/2018/06/scaling-blockchains-off-chain-data/

[43] C. Ferris. Does Hyperledger Fabric perform at scale? [Online]. Available: https://www.hyperledger.org/blog/2019/04/04/does-hyperledger-fabric-perform-at-scale

Sujit Biswas received his Ph.D degree in Computer Science and Technology from Beijing Institute of Technology, China, and M. Engineering degree in Computer Engineering from Northwestern Polytechnical University, China in 2015. He is an Assistant Professor with Computer Science and Engineering department, Faridpur Engineering College, University of Dhaka, Bangladesh. His basic research interest is in IoT, Blockchain, Mobile computing security and privacy, Big Data, Machine Learning, Data driven decision making, etc.

Kashif Sharif received his M.S. degree in information technology in 2004 from National University of Sciences and Technology, Pakistan, and Ph.D. degree in computing and informatics from University of North Carolina at Charlotte, NC, USA in 2012. He is currently an Associate Professor (Research) at Beijing Institute of Technology, Beijing, China. His research interests include data centric networks, blockchain & distributed ledger technologies, wireless & sensor networks, software defined networks, and 5G vehicular & UAV networks. He also serves as associate editor for IEEE Access.

Fan Li received the Ph.D. degree in computer science from the University of North Carolina at Charlotte, Charlotte, NC, USA, in 2008, the M.Eng. degree in electrical engineering from the University of Delaware, Newark, DE, USA, in 2004, and the M.Eng. and B.Eng. degrees in communications and information system from the Huazhong University of Science and Technology, Wuhan, China, in 2001 and 1998, respectively. She is currently a Professor with the School of Computer Science, Beijing Institute of Technology, Beijing, China. Her current research focuses on wireless networks, ad hoc and sensor networks, and mobile computing. Her papers have won Best Paper Awards from IEEE MASS (2013), IEEE IPCCC (2013), ACM MobiHoc (2014), and Tsinghua Science and Technology (2015). She is a Member of the ACM and the IEEE.

Iqbal Alam received B.S. degree in Computing and Information Systems from London Metropolitan University, UK, in 2009, and M.S. Degree in Software Engineering from Beijing Institute of Technology, China, in 2015. His research interests include IoT virtualization, Programmable Blockchain, and Distributed Ledger Technology.

Saraju P. Mohanty received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 350+ research articles, 4 books, and invented 4 U.S. patents. His Google Scholar h-index is 36 and i10-index is 136 with 6300+ citations. He has over 20 years of research experience on security and protection of media, hardware, and system. He introduced the Secure Digital Camera (SDC) in 2004 with built-in security features designed using Hardware-Assisted Security (HAS) or Security by Design (SbD) principle. He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He is a recipient of 12 best paper awards, Fulbright Specialist Award in 2020, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 9 keynotes and served on 5 panels at various International Conferences. He is the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE). He has been serving on the editorial board of several peer-reviewed international journals, including IEEE Transactions on Consumer Electronics (TCE), and IEEE Transactions on Big Data (TBD). He has mentored 2 post-doctoral researchers, and supervised 12 Ph.D. dissertations and 26 M.S. theses.