SSHealth: Toward Secure, Blockchain-enabled Healthcare Systems

SSHealth: Toward Secure, Blockchain-enabled Healthcare Systems

Alaa Awad Abdellatif*†, Abeer Z. Al-Marridi*, Amr Mohamed*, Aiman Erbad*, Carla Fabiana Chiasserini†, and Ahmed Refaey+
*Department of Computer Science and Engineering, Qatar University
†Department of Electronics and Telecommunications, Politecnico di Torino
+Department of Electrical and Computer Engineering, Manhattan College
E-mail: {alaa.abdellatif, chiasserini}@polito.it, {aa1107191, amrm, aerbad}@qu.edu.qa, ahussein01@manhattan.edu

***Abstract*—Future of healthcare systems is being shaped by incorporating emerged technological innovations to drive new models for patient care. By acquiring, integrating, analyzing, and exchanging medical data at different system levels, a new level of understanding and practice can be introduced, offering a radical improvement to healthcare services. This paper presents a new smart and secure Healthcare system (ssHealth), which, leveraging advances in edge computing and blockchain technologies, permits epidemics discovering, remote monitoring, and fast emergency response. The proposed system also allows secure medical data exchange among local healthcare entities, thus realizing the integration of multiple national entities and enabling the correlation of critical medical events for emerging epidemics management and control. Indeed, such advantages come with some challenges that should be addressed, including fulfilling diverse Quality of Service (QoS) requirements. We therefore develop a blockchain-based approach to be implemented at the proposed ssHealth architecture, in order to optimize medical data sharing between different health entities, hence providing effective and secure healthcare services. Finally, we highlight the benefits of the proposed ssHealth system and possible directions for future research.**

***Index Terms*—Secure and smart health, blockchain, edge computing, medical data sharing, block verification.**

I. Introduction

Developing a smart, efficient and secure healthcare systems for improving people's quality of life is a top interest worldwide. A pivotal contribution to the development of smart-health systems has come from some emerging technologies such as Internet of Things (IoT), Blockchain, and Edge Computing. Advanced e-health applications are expected to inspire fundamental transformations for the healthcare industry towards Healthcare Industry 4.0 (Health 4.0) [1], especially in pre-hospital emergency care situations and for geographically remote areas. In the age of IoT and Health 4.0, health-related applications are gaining momentum, as the huge amount of data generated through that allows for more in-depth medical studies and patients feel more secure if their status is precisely monitored even outside the hospital . Moreover, medical data exchange across multiple entities can lead to a better quality level in the care for the patients, improving the response time in emergency conditions and a more accurate control and management of diseases. However, critical challenges have emerged, which need to be faced in order to ensure high-quality healthcare services, specifically:

- the massive real-time data collected from different health monitoring systems, which need to be stored, processed, and shared;
- data management in untrusted cloud servers, with risks for the patients' privacy;
- fulfilling diverse security and privacy requirements, while dealing with the complexity of data processing and transfer;
- remote accessibility of medical data by different authorized entities is essential to large-scale, low-cost healthcare and personalized medicine.

Note, in particular, that traditional healthcare systems exhibit weak security protection and are often victim of hackers: from 2016 to 2017, the number of reported healthcare attacks increased by 89% [2]. Developing complex encryption techniques for healthcare systems, on the one hand, provides more security guarantees, on the other, it may result in exceedingly high computational overheads and latency.

In this work, we argue that building a secure, trusted, and decentralized smart-healthcare system addressing the above challenges can be established leveraging edge computing and blockchain. Blockchain is a decentralized ledger of transactions that are shared among multiple entities while preserving the integrity and consistency of the shared data. It is considered as a revolutionary technology that will have a huge impact on the society: in the 2015 World Economic Forum[1] report, 58% of the participants foresaw that 10% of global Gross Domestic Product (GDP) will be related to the blockchain

This work was made possible by grant # QUHI-CENG-19/20-1 from Qatar University. The work of Abeer Z. Al-Marridi is supported by GSRA grant # GSRA5-1-0326-18026 from the Qatar National Research Fund (a member of Qatar Foundation). The findings achieved herein are solely the responsibility of the authors.

[1]https://www.weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact

technology by 2025. Being decentralized, it well matches the potentiality of edge computing, which can effectively support data storage and processing at different entities as well as their interconnection. We therefore aim at paving the way to efficient smart-health systems and applications, by answering the following fundamental questions:

(i) is blockchain a valid solution for realizing healthcare systems?

(ii) how can we leverage the blockchain capabilities and the edge computing potentialities to fulfill diverse healthcare applications' requirements?

Specifically, the contributions of this work can be summarized as follows:

1) we propose a smart, secure, and decentralized healthcare system that relies on blockchain and edge computing technologies to provide a convenient data sharing among multiple entities;
2) we formulate a flexible configuration model that enables blockchain to support diverse QoS requirements. Then, we develop an efficient algorithm to solve this model;
3) The obtained results demonstrate the effectiveness of the proposed approach in improving the blockchain performance for healthcare applications.

In what follows, we highlight the advantages of using blockchain within a healthcare system and present some of the recently proposed healthcare systems that exploit a blockchain (Section II). We then introduce the proposed ssHealth system architecture and the associated blockchain configuration (Section III). Finally, we present the benefits of leveraging blockchain capabilities within the proposed architecture (Section IV) and conclude the paper by highlighting possible directions that are worth to be further investigated (Section V).

II. Blockchain for Healthcare Systems

This section discusses the key features and motivations for using a blockchain within healthcare systems, also in the light of recent proposals appeared in the literature.

A. Why blockchain is needed for healthcare systems?

A healthcare system comprises diverse organizations, people, and actions whose fundamental role is to monitor, promote, and maintain people's health. It includes, for instance, private clinics, pharmacies, hospitals, health insurance companies, occupational health and safety legislation, as well as the ministry of health. Effective e-health systems must provide fast response with high quality service level and security for the entire population, while simultaneously promoting disease prevention and managing costs. To achieve this, the following issues have to be adequately addressed.

Privacy and security: Real-time access to clinical patient's records enables e-health systems to give timely care to the patients through the nearest point of care. Furthermore, healthcare entities may need to share relevant data to provide national first response to epidemics, improved national wide statistics, and enhanced quality of healthcare services. Finally, the dissemination, processing, and analysis of medical data have been perceived to be crucial for the diagnosis and discovery of new therapies for emerging diseases. However, medical data exchange across multiple organizations comes with many security risks. Additionally, privacy is a critical issue: without ensuring that privacy-preserving schemes are applied, users may not accept sharing their data with others, which would impair the creation of a national system integrating all healthcare entities. Thus, it is mandatory to provide secure data access and to prevent tracking users' identity and raw data disclosure.

Management of patients' flow: While detecting and predicting patients' state through data analytic within one organization maybe possible, managing and correlating patients' related data across multiple entities is quite hard. The problem is not due to insufficient resources, but due to insufficient resource management. The challenge is the ability of healthcare providers to foresee patients' flow, which demands for predictive analytics and collaboration among different entities to align available resources to the forthcoming demand.

Support of diverse QoS requirements: E-health systems require high data rates and data accessibility anytime and anywhere, with low latency. Such requirements impose major challenges in terms of network load and connectivity, as well as security.

Blockchain appears as a perfect solution to all of the above issues. It provides fast, secure exchange and storage of medical data, and it can aggregate different health entities, with diverse policies, and make them part of a unique national healthcare system. The power of security in blockchain comes from the collective resources of the crowd, since, most of the entities have to verify each block of data using a consensus algorithm[2], e.g. Delegated Proof-of Stake (DPoS) [5]. Hence, any cyber attack has to beat the resources of the whole crowd collectively to be able to hack the integrity of the data.

B. Related work on blockchain-based healthcare systems

Recently, different types of blockchains have been envisioned for the healthcare sector, including public and private blockchains. Public blockchains offer decentralized and secure data sharing, however, when advanced control and privacy are required, private or permissioned models turn to be more efficient. Several blockchain frameworks (e.g., Ethereum and Hyper ledger Fabric), smart contracts[3], and consensus algorithms have been investigated in the literature. The general blockchain architecture mainly consists of: data sender, Blockchain Manager (BM), and verifiers. First, data senders upload their data as "transactions" to the nearby BM. Then the BM acts as a verifiers' manager: it generates

[2]Consensus algorithms are mechanisms that ensure the integrity and consistency of the blockchain across all the participating entities [5].

[3]A smart contract is a software that contains all instructions and rules agreed upon by all the entities to be applied on the blockchain: all the transactions need to be consistent with the smart contract before being added to the blockchain.

TABLE I
SUMMARY OF THE RELEVANT WORK ON BLOCKCHAIN IN HEALTHCARE SYSTEMS

Blockchain Type	Description	Limitations	Entities
Private (Ethereum) *Consensus*: Practical Byzantine Fault Tolerance (PBFT) *class*: patient [3]	Blockchain system links patients with doctors using customized smart contract to record all events on the blockchain	Latency scalability	Patients Hospitals
Private (Ethereum) *Consensus*: Proof of Work (PoW) *class*: patient [4]	A blockchain framework is proposed for searching encrypted index of Electronic Health Records (EHRs) while real data stored in database	Scalability	Patients Hospitals Medical labs Insurance companies
Private (consortium) *Consensus*: delegated proof of stake (DPoS) *class*: patient [5]	Parallel healthcare system using blockchain, technology is proposed to link various parties for medical data sharing	Latency scalability security	Patients Hospitals Healthcare communities Researchers
Private (Ethereum) *Consensus*: PoW *class*: patient [6]	Blockchain framework is proposed to connect the patients with the hospitals to enable health-related information exchange	Scalability	Patients Hospitals Healthcare institutions
Private (Hyperledger fabric) *Consensus*: Byzantine fault-tolerant state machine replication *class*: patient [7]	Blockchain framework is proposed for sharing processed medical data between different healthcare entities	Scalability Patients approval	Patients Healthcare providers
Private (Ethereum) *Consensus*: proof of conformance *class*: entity [8]	Framework of dual blockchains is proposed, one to store and share the index of the EHR with multiple hospitals, and the other to store the original data	Storage scalability	System manager Hospitals
Public (Ethereum) *Consensus*: PoW *class*: entity [9]	Propose a framework of two coupled blockchains for managing the storage of two types of data to enhance the throughput, accessibility, and fairness among users	Latency scalability computational cost	Patients Medical institutions
Private (MeDShare) *Consensus*: using consensus nodes *class*: patient [10]	Blockchain system is proposed to provide medical data sharing, auditing, and control over diverse entities	Privacy scalability	Patients Hospitals Research institutions
Private (Hyper ledger fabric) *Consensus*: voting-based approach *class*: patient [11]	Blockchain has been integrated with a tree-based method for medical data sharing between different entities	Privacy scalability	Patients Doctors Insurance companies

unverified blocks, distributes them across the verifiers, triggers the consensus process, and inserts the verified blocks in the blockchain. Hence, the BM acts as the leader, while the verifiers are the followers that cooperate to complete the block verification task. In line with the traditional DPoS consensus scheme, the verifiers take turns to work as BM for a given period of time [12].

For healthcare applications, the blockchain architectures that have been proposed so far can be broadly classified into two categories: patient-based and entity-based. In patient-based architectures, patients participate in the blockchain and transactions are driven by the patient directly. However, such architectures have a limitation in terms of system's scalability. In entity-based architectures, instead, health organizations, hospitals, research institutes, and alike are the main actors, while patients only interact with the health organizations to acquire the service they need. According to our survey, 83% of the systems proposed since 2016 are patient based, while 17% are entity based. Table I reports recent works in this area, highlighting the encryption techniques and consensus algorithms they adopt, as well as some of the limitations they exhibit. In particular, several approaches suffer from poor scalability and slow response. Being swift response a major goal for emergency care, some studies aim to overcome these limitations using an external database, which stores the raw data, and shares only the index or reference to the data in the blockchain [4], [8]. However, the changes in the consensus algorithms that are necessary to deal with such an architecture, may have an impact on privacy level and computational cost. We therefore envision a solution that combines the blockchain-enabled architecture with intelligent processing at the edge so as to support fast, secure and scalable exchanging of medical data.

III. ssHEALTH ARCHITECTURE AND BLOCKCHAIN CONFIGURATION

This section first describes the proposed ssHealth system architecture, then it discusses the blockchain approach we adopt. Finally, it presents a method for optimally configuring the blockchain system for effectively address the challenges and requirements posed by e-health system.

A. ssHealth architecture

The proposed system architecture, shown in Figure 1, includes two main network sub-systems: (a) a Local network and (b) a Blockchain network. For the sake of scalability, it is assumed that the healthcare entities collect health-related information from the local network, process these data, and share important information through blockchain network. The shared data are validated and locally stored by the different entities in the blockchain, which are trusted entities with large storage and computational capabilities [13].

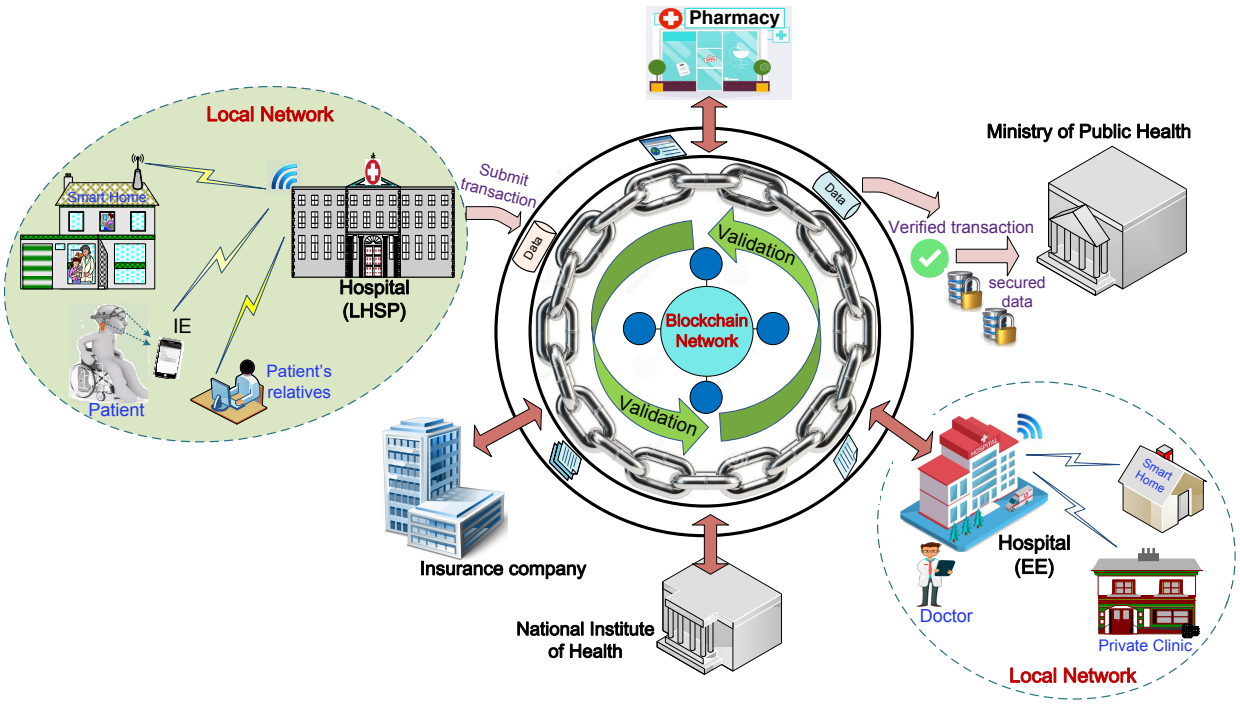


Fig. 1. Proposed ssHealth system architecture.

The local network stretches from the data sources located on or around patients to the Local Healthcare Service Provider (LHSP), e.g., a hospital. It contains the following major components:

a.1) Internet of Medical Things (IoMT): A combination of sensor nodes attached/near to the patients to be leveraged for monitoring health conditions and activities within the smart assisted environment. Examples include: body area sensor networks (i.e., implantable or wearable sensors that measure different biosignals and vital signs), smartphones, IP cameras, and external medical and non-medical devices.

a.2) Internal Edge (IE): This edge node implements local processing functions between the data sources and the LHSP. Specifically, the IE analyzes the gathered medical and non-medical data from different sources, obtains the information of interest, and forwards the processed data/extracted information to the LHSP. Moreover, IE can be a mobile node (e.g., a smartphone) or an infrastructure edge node (e.g., a wireless router or an access point). Importantly, the IE can optimize the medical data delivery based on the context (i.e., data type, supported application, and patient's state) as well as on the conditions of wireless connectivity. Furthermore, different specialized healthcare applications can be implemented at the IE to allow patients to actively participate in their treatment and ubiquitously interact with their doctors anytime and anywhere.

a.3) Local Healthcare Service Provider (LHSP): An LHSP can be a hospital, which monitors and provides the required healthcare services for the local patients, records the patients' state, and puts in place fast emergency services if needed. Importantly, the LHSP plays a significant role in monitoring of patients' state not only inside the hospital (intra-hospital patient care), but also outside (e.g., home patient care). Also, it can be connected with the private-local clinics that may transfer patients to it for more advanced care, or even with patient's relatives to follow up on the patient's conditions.

As far as the blockchain network is concerned (see Figure 1), the core is the blockchain-based data sharing architecture that enables secure access, processing, and sharing of medical data among healthcare entities. Blockchain is suitable for secure medical data sharing because of its immutability and decentralization features, which are perfectly consistent with our proposed ssHealth architecture. Using blockchain, all transaction blocks (i.e., containing health-related information) can be securely shared, accessed, and stored by physicians, decision makers, and other healthcare entities. The latter include, but are not limited to:

b.1) External Edge (EE): In the proposed architecture, a hospital or a LHSP have more advanced tasks than the ones mentioned above: it can act as an EE that is responsible for data storage, applying sophisticated data analysis techniques, population health management, and sharing important health-related information with public health entities. Hence, leveraging the power of edge computing, each entity can verify the authenticity and integrity of the medical data at the EE before sharing it within the blockchain.

b.2) Insurance companies: One important aspect for e-health systems is integrating healthcare providers, patients, and payers into one "digitized community", in order to improve quality

of services and drive down costs. Indeed, to realize a sustainable healthcare-business model, healthcare providers will have to own health plans powered by insurance companies.

b.3) Pharmacies: The main pharmacies' duties include processing prescriptions, storing and providing access to disbursed prescriptions, and ensuring patients' privacy. On top of it, pharmacies have to coordinate with private insurance companies to submit insurance claims, ensure payment, and resolve denials of coverage. Pharmacies may also communicate with prescribers to confirm the dosage and formulation (e.g., liquid or tablet), or to replace prescribed brand name with a generic equivalent. Thus, it is crucial to have a secure communication system to exchange such information with different associated entities.

b.4) National Institutes of Health (NIH): NIH are major players in clinical research and health education. The latter in particular is a process in which all public healthcare institutes, hospitals, and medical care personnel are involved. Thus, NIH should cooperate with healthcare service providers to develop joint educational programs and services for pursuit scientific research and preventive medicine.

b.5) Ministry of Public Health (MOPH): The main role of MOPH is monitoring the quality and effectiveness of healthcare services through coordination with different health entities. MOPH waives the responsibility of healthcare services to the hands of public and private health sectors while regulating, monitoring, and evaluating their healthcare services to guarantee an acceptable quality of care level. Thus, MOPH is committed to establishing an environment that promotes high-quality services by sharing relevant information with its partners such as health insurance companies.

B. Optimal blockchain configuration

Leveraging the above ssHealth architecture, we develop a blockchain-based data sharing scheme that enables medical data access, processing, and sharing among the aforementioned healthcare entities. However, blockchain poses a new challenge, i.e., finding the optimal trade-off among security level, latency, and cost. Indeed, due to the need of coordinating the transactions of multiple entities, public blockchain is slower than traditional databases, implying a service latency that may be unacceptable for several applications (e.g., emergency management). We addresses this challenge by designing a priority-based secure data sharing scheme, as detailed below.

We draw on the BM concept (see [12] and Section II-B, a logical role that any entity in the proposed architecture can take on, possibly by taking turns, or that can be taken by the EE that wants to share its data. In particular, in our scheme the BM is in charge of: (i) collecting the transactions received from the different entities, (ii) preparing and distributing unverified blocks to the verifies (e.g., hospitals, NIH, and MOPH, which have sufficient computation and storage resources), (iii) updating blockchain configuration considering urgency and security level of the collected data, and (iv) interacting with the verifiers to complete the block verification tasks. BM is thus a critical component, which should carefully select the blockchain configuration in terms of number of verifiers and number of transactions per block. These parameters should be dynamically set based on the diverse applications' requirements and data types, and in such a way that the optimal trade-off among security, latency, and cost is established. As an example, Figure 2 illustrates the case where high-priority data are received requiring minimum security, e.g., emergency notifications, and should be dealt with a restricted blockchain, i.e., minimum number of verifiers. On the contrary, for low priority types of data but requiring a high security level (such as video monitoring), fully restricted blockchain mode should be used. In general, the more verifiers participate in the block verification stage, the higher the security level is, but also the larger the latency (due to the verification delay) and the higher the cost (due to verification fees) that are experienced [12]. Instead, as the number of transactions per block grow, the latency increases, while the cost per transaction decreases. We also remark here that data types and priorities are defined at the edge by applying different data classification, event detection, and summarization techniques.

As a case study, we focus on private blockchain framework with DPoS consensus scheme, which performs the consensus process using pre-selected verifiers with moderate cost. Also, we consider that the BM resides at the EE and has to: (i) detect the patient's context (including patient's conditions, data type, and security requirements), and (ii) map the patient's context into different configuration modes of the blockchain. To represent the different conflicting metrics the BM has to play with, namely, latency (L), security (S), and cost (C), we define an aggregate utility U, which combines them into a single function:

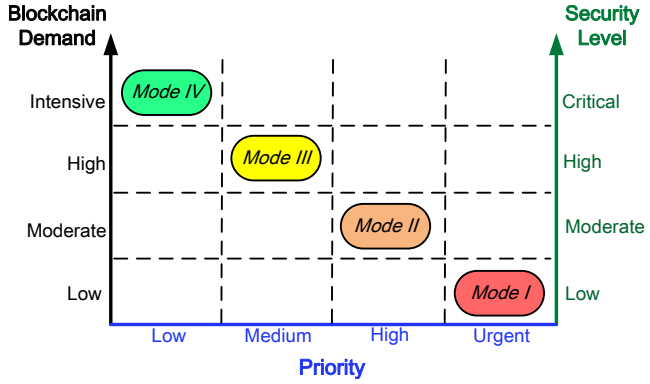
$$U = \alpha \cdot \frac{L}{l_m} + \beta \cdot \frac{s_m}{S} + \gamma \cdot \frac{C}{c_m}, \tag{1}$$

where α, β, and γ are weighting coefficients that represent the relative importance of the considered metrics, such that $\alpha + \beta + \gamma = 1$. However, these metrics has different values and units, which must be normalized with respect to their maximum values (denoted by l_m, s_m, and c_m, respectively) to make them comparable.

The BM can then set the best blockchain configuration, by solving the following problem:

$$\begin{aligned} \underset{m,\theta}{\text{minimize}} \quad & \alpha \cdot \frac{L}{l_m} + \beta \cdot \frac{s_m}{S} + \gamma \cdot \frac{C}{c_m} \\ \text{subject to} \quad & v \leq m \leq M, \\ & t \leq \theta \leq N, \end{aligned} \tag{2}$$

where m is the number of selected verifiers, with maximum and minimum values equal to M and v, respectively, and θ is the number of transactions per block, with maximum and minimum values equal to N and t, respectively. In (1), the security level is defined as $S = \kappa \cdot m^q$, where κ is a coefficient given by the system, and $q \geq 2$ is an indicator factor representing the network scale [12]. L refers to the verification latency, which includes the four steps of the block verification process: (i) unverified block transmission from the



Priority	Data type	Security Level
Urgent	Emergency notifications	Low
High	Physiological signals	Moderate
Medium	Vital images	High
Low	Video monitoring	Critical

Fig. 2. Blockchain modes based on the data priority and required security level.

TABLE II
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
M	10	N	20
v	2	t	2
r_d	1.2 Mb/s	r_u	1.3 Mb/s
O	0.5 Mb	B	1 kb

BM to verifiers, (ii) block verification time, (iii) verification result broadcasting and comparison between verifiers, and (iv) verification feedback transmission from the verifiers to the BM. Hence, the normalized latency is defined, according to [12], as

$$L = \frac{\theta \cdot B}{r_d} + \max_{i \in \{v, \cdots, M\}} \left(\frac{K}{x_i}\right) + \psi \cdot \theta \cdot B \cdot m + \frac{O}{r_u}, \quad (3)$$

where B is the transaction size, K is the required computational resources for block verification task, x_i is the amount of available computational resources at verifier i, O is the verification feedback size, and r_d and r_u are, respectively, the downlink and the uplink transmission rate, from the BM to the verifiers and vice versa. In (3), ψ is a predefined parameter that can be defined leveraging the statistics on previous processes of block verification [12]. Finally, the cost function is defined as $C = \frac{\sum_{i=1}^{m} c_i}{\theta}$, where c_i is the computational cost of verifier i, which is given by $c_i = \rho_i \cdot x_i$. Therein, ρ_i represents the payment from verifier i to a cloud service provider, in order to acquire the needed resources for the verification process.

By defining the weighting coefficients α, β, and γ as functions of data types and application's requirements, the optimal number of verifiers m^* and transactions per block θ^* are obtained by solving (2). However, the above optimization problem is an integer programming optimization, which is NP-complete problem [14]. In light of the problem complexity, we propose Algorithm 1 for an efficient and swift solution. In this algorithm, verifiers are selected in an ascending order based on their associated latency, i.e., those verifiers that finish block verification faster will be selected first.

Figure 3 depicts the variations in the objective U as the number of verifiers m and number of transactions per block θ vary, for applications with similar requirements in terms of security, latency, and cost ($\alpha = \beta = \gamma$). Other simulation parameters are reported in Table II. Furthermore, Figure 4

Algorithm 1 Blockchain Mode Optimization

Input: x_i, ρ_i, v, M, t, N.
Initially: set $m = v$, $\theta = t$, and compute U as in (1).
for $m = v : M$ **do**
  for $\theta = t + 1 : N$ **do**
    Update U based on (1).
    if $U(\theta) > U(\theta - 1)$ **then**
      $\theta^* = \theta - 1$.
      Break % θ^* is obtained
    end if
  end for
  if $m > v$ & $U(m) > U(m - 1)$ **then**
    $m^* = m - 1$.
    Break % m^* is obtained
  end if
end for
Output: m^*, θ^*.

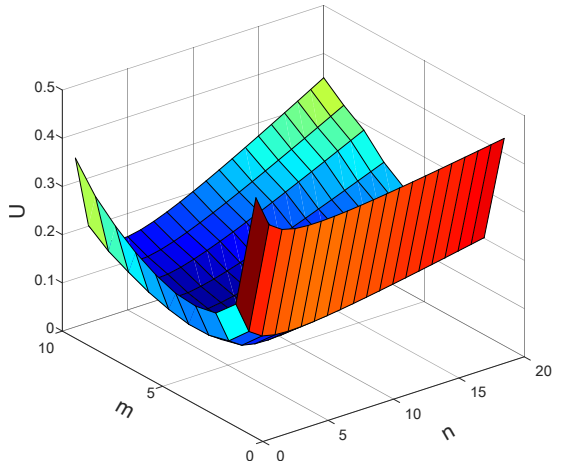


Fig. 3. The proposed utility function as the number of verifiers (m) and the number of transactions per block (θ) vary.

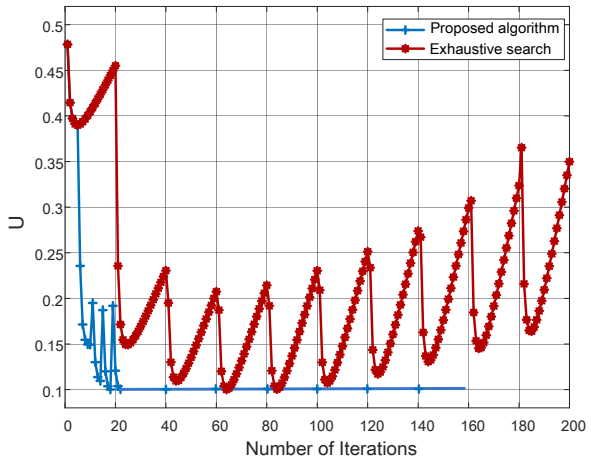


Fig. 4. Convergence behavior of the proposed algorithm compared to the solution obtained through exhaustive search.

shows the convergence behavior of the proposed algorithm to the optimal solution obtained by exhaustive search (or brute-force search) [15], given $M = 10$ and $N = 20$. We observe that our algorithm requires only 23 iterations to reach the optimal solution compared to exhaustive search that still does not converge after 200 iterations.

IV. Benefits of ssHealth

Given the requirements of e-health applications discussed in Section II, we now highlight the effectiveness of our ssHealth system in fulfilling such requirements.

Privacy and security: Slicing the overall system into local and blockchain network facilitates medical data processing, accessing, sharing, and storage while dealing with encrypted data throughout the entire process. The proposed ssHealth system enhances accessibility and information sharing between patients and hospitals to provide effective and safe healthcare services, while protecting healthcare systems from cybersecurity threats. It also allows for preventing privacy threats that data sharing entails leveraging blockchain technology, which provides secure access to patients' health records across distributed entities. Moreover, edge computing capabilities enables each entity (at the EE) to verify the authenticity and integrity of the medical data before sharing it within the blockchain network.

Scalability and management: For implementing an effective healthcare system, various entities should collaborate, and a global health system should be created. The proposed ssHealth system realizes such collaboration efficiently by: managing workloads between different entities, enabling secure data exchange, avoiding the hurdles of managing the available resources or data warehouse. Furthermore, it enables building a scalable and reliable healthcare system by: (i) connecting different physician groups and health entities, which facilitates implementing clinically-integrated, high-value networks for better patient care; (ii) enabling secure medical data sharing, which helps health institutes and pharmacies to anticipate and manage resources across their health systems (e.g., hospital capacity and drugs).

Fulfilling diverse QoS requirements: The proposed ssHealth system can not only transfer massive amounts of data securely, but also analyze data efficiently at the EE to extract meaningful and concise information to be shared with the different entities. Moreover, it efficiently supports different types of applications and data according to their QoS requirements, e.g., demands for high data rates and swift response.

At last, we remark that the proposed system allows for improved healthcare services by developing a patient-centric, physician-aligned healthcare management model. Such architecture can be leveraged to avoid visits to the hospital emergency ward in non-critical situations, thus reducing costs and improving health-case services for patients with serious conditions.

V. Conclusions and Future Directions

In this paper, we envisioned a novel e-health system for creating effective, large-scale and collaborative systems able to provide high-quality patients' care and to make significant advancements in disease treatments through secure data sharing. The proposed ssHealth system integrates edge computing and blockchain to enable the exchange of large amount of medical data generated by different healthcare entities, while preserving the patients' privacy. Additionally, we defined a novel mechanism that can be implemented within the blockchain network to ensure fast response, scalability, and secure transmission of medical data. It is shown that mapping the characteristics of the collected data onto appropriate configurations of the blockchain can significantly enhance the performance of the overall ssHealth system, while satisfying diverse applications' requirements.

In this context, several promising directions for future research emerge, which include:

(i) Developing various cyber security schemes at the IE and EE to achieve a robust privacy protection of medical data and patients' profiles. Maximizing security level for health applications may substantially degrade QoS and cause service disruption. Thus, considering the concept of quality of protection (QoP) while providing security and privacy is mandatory. In this regard, developing QoP-aware schemes can ensure different levels of anonymity and privacy, and optimize misbehavior detection and encryption, according to the type of the collected data and the level of emergency of the situations we have to deal with.

(ii) Further optimizing the blockchain parameters, such as block size, transaction size, and number of blockchain channels. With the evolution of the blockchain frameworks, new features are added for enhancing security and scalability. One important feature is the multi-channel blockchain network. Here channels refer to the state store of the blockchain network which holds the shared data. For instance, in the Hyperledger Fabric framework, there can be multiple channels in the same blockchain to provide privacy and security to different participating entities. By leveraging such concept, specific

geographical areas or group of patients and hospitals can share their data only between them so as to increase the system scalability while still ensuring secure data sharing among the entities that need to access them.

REFERENCES

[1] C. Thuemmler and C. Bai, "Health 4.0: Application of industry 4.0 design principles in future asthma management," 2017, pp. 23–37.

[2] "Healthcare report for 1st half of 2018," https://www.cryptonitenxt.com/resources, accessed: 2019-03-05.

[3] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, vol. 42, no. 7, 2018.

[4] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.

[5] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 99, pp. 1–9, 2018.

[6] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[7] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, 2019.

[8] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems*, vol. 42, no. 8, 2018.

[9] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BLOCHIE: a blockchain-based platform for healthcare information exchange," *IEEE International Conference on Smart Computing*, pp. 49–56, June 2018.

[10] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[11] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–5.

[12] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, March 2019.

[13] 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.

[14] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. cambridge university press, 2003.

[15] A. Puntambekar, *Analysis And Design Of Algorithms*. Technical Publications, 2008. [Online]. Available: https://books.google.it/books?id=NUW_5rs6K-wC