Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT

Tharaka Hewa*, An Braeken†, Mika Ylianttila‡, Madhusanka Liyanage§
*‡§Centre for Wireless Communications, University of Oulu, Finland, †Vrije Universiteit Brussel, Brussels, Belgium
§School of Computer Science, University College Dublin, Ireland
Email: *‡§[firstname.lastname]@oulu.fi, †an.braeken@vub.be §madhusanka@ucd.ie

***Abstract*—There is a global hype in the development of digital healthcare infrastructure to cater the massive elderly population and infectious diseases. The digital facilitation is expected to ensure the patient privacy, scalability, and data integrity on the sensitive life critical healthcare data, while aligning to the global healthcare data protection standards. The patient data sharing to third parties such as research institutions and universities is also concerned as a significant contribution to the society to sharpen the research and investigations. The emergence of 5G communication technologies eradicates the borders between patients, hospital and other institutions with high end service standards. In patients' perspective, healthcare service delivery through the digital medium is beneficial in terms of time, costs, and risks. In this paper, we propose a novel Multi-access Edge Computing(MEC) and blockchain based service architecture utilizing the lightweight ECQV (Elliptic Curve Qu-Vanstone) certificates for the realtime data privacy, integrity, and authentication between IoT, MEC, and cloud. We further attached storage offloading capability to the blockchain to ensure scalability with a massive number of connected medical devices to the cloud. We introduced a rewarding scheme to the patients and hospitals through the blockchain to encourage data sharing. The access control is handled through the smart contracts. We evaluated the proposed system in a near realistic implementation using Hyperledger Fabric blockchain platform with Raspberry Pi devices to simulate the activity of the medical sensors.**

***Index Terms*—Elliptic Curve Cryptography, Elliptic Curve Qu Vanstone Certificates, Blockchain, Smart Contracts, 5G, IoT**

I. Introduction

The classical healthcare systems require patients to admit the hospitals and connect to the biomedical equipment including oxygen sensors, blood pressure meters, glucose sensors and so on. However, the classical procedures are challenging to cope with extensive demands of healthcare, which is a vital consideration due to the increase of elderly population as well as an events such as global pandemics. Presently, the global enthusiasm towards the Telehealth techniques is accelerated with the COVID-19 pandemic. Furthermore, the pandemic situation restricts the utilization of healthcare resources to minimize the risk of spreading diseases. A certain amount of the patients, who do not require a robust medical intervention can be connected to the hospitals for monitoring and remote treatments. Elderly people and post-treatment monitoring are potential patient categories. It reduces risk, improves the patient's comfort and satisfaction with eventually cutting the costs.

Telehealth systems [1] include among others the application of robotics to deliver medicines, monitoring of patients and offering remote consultation of the patients. It can seamlessly connect patients with medical professionals including nurses, general practitioners, and consultants through the Internet while are patients in their homes.

The 5G and MEC are identified as prominent technologies to leverage future telehealth systems by satisfying above requirements. The 5G network ecosystem provides seamless connectivity between medical sensors, actuators and the cloud with ultra high speed and extensive bandwidth support. Furthermore, the high reliable high quality video streaming for patient screening and Augmented Reality (AR) assisted consultation are can be provided by utilizing 5G MEC technologies [2]. Connectivity with the MEC elevates the service capabilities of connected IoT (Internet of Things) nodes with offloading some resource intensive computations to MEC nodes.

To realize this setup, we propose a novel MEC and blockchain based secure telehealth system using lightweight Elliptic Curve Qu Vanstone (ECQV) certificates [3] and symmetric keys which connects IoT nodes with the cloud using MEC nodes. The solution utilizes blockchain-based smart contracts in the key establishment, data access and data sharing processes. The blockchain storage is extended with the IPFS (InterPlanetary File System) to reduce blockchain storage growth to support the massive number of connective nodes. The access control to the patients' data and the rewarding scheme for the hospitals and patients for data sharing are handled through the smart contracts. We evaluated the proposed system with a prototype implementation by using Hyperledger blockchain platform.

The rest of the paper is organized as follows. Section II presents a background on Telehealth systems and 5G. Section III presents the proposed architecture. Security of the proposed system is analysed in Section IV. Section V presents the prototype implementation and experimental results. Finally, the Section VI concludes the paper.

II. Background

A. Telehealth systems

The telehealth is defined as a technique which delivers medical services, such as clinical consultation, patient monitoring, and remote treatment over the digital infrastructure. The key distinguishing parties in classical telehealth systems are the patients, interfaced with the digital medium, and the hospitals which operate the system and data storage, typically hosted in cloud computing infrastructure. The telecommunication services are provided by a third party and the data is stored in the cloud. Hence, there are many security considerations for the data in transit and the data stored in the cloud in terms of privacy, integrity and compliance with standards.

1) Benefits of telehealth systems: The telehealth systems enable seamless connectivity with the patients and consultants beyond frontiers with various types of healthcare service delivery. Through the realtime connected telehealth systems, the healthcare response is achievable with minimal time and the healthcare professionals are not unnecessarily exposed to the patients.

2) Key requirements of the telehealth systems:

a) Data security: The data security is a vital concern in telehealth systems and the data security mechanisms must be aligned with ultra low latency requirements and computational resource restrictions associated with the lightweight computing nodes operating in the telehealth domain along with the compliance standards such as Health Insurance Portability and Privacy Act (HIPAA).

b) Authentication and access control: Authentication and access control in telehealth systems should be applicable to the data and services. The data authentication ensures the data in transit is not being tampered and the service access control ensures that the services consumed by the patients are aligned with their subscription plans. However, the importance of authentication is vital since the data exchanged is life critical and the tampering of data could lead the human life at risk.

c) High-end connectivity: The primary anticipations of the connectivity include ultra-low latency with higher bandwidth. Furthermore, the limited and customized operational requirements also exist.

d) Data sharing capability: The data sharing capability is a vital requirement and the privacy must be balanced in-between the applications since the privacy violations will deviate the systems with compliance standards. The shared data will be used in improving accuracy of the future research conducted in disease control.

B. 5G for Telehealth

The 5G communication technologies facilitate to leverage the healthcare context by the distinguishing advancements compared to the previous communication infrastructure. The high throughput, extremely low latency and a vast array of customized techniques including micro operators have potential to expand the usability towards diverse use cases.

The IoT initiatives in the healthcare are widespread in different avenues including treatments in the infectious diseases and adult care, monitoring and remote treatments with 5G connected sensors and actuators.

The MEC based architecture is fostered in different application contexts since the edge computing infrastructure shrinks the gap of cloud-quality computation in contrast with the cloud.

C. Related works

Most of the communications in the telehealth context are performed in a wireless medium, open for a wide range of attackers, the inclusion of sufficient security mechanisms should be guaranteed [4]. In particular, authentication of legitimate IoT devices is very important in the telehealth applications. The advantages of including blockchain in healthcare are discussed in [5]. Xiong et al. [6] highlighted the significance of integrating edge computing nodes for offloading computational resource intensive tasks in the blockchain networks.

Theodouli et al. [7] presented a blockchain based architecture for healthcare data sharing and access permission handling utilizing the smart contracts. Chen et. al [8] presented edge and cognitive computing based healthcare system which monitors and analyzes the physical health of smart clothing users. Pace et al. [9] proposed BodyEdge, which is an edge based novel architecture for human-centric applications in the healthcare industry 4.0. Wang and Zhang [10] proposed homomorphic encryption based data division scheme on the data generated by wireless sensor nodes.

III. Proposed Architecture

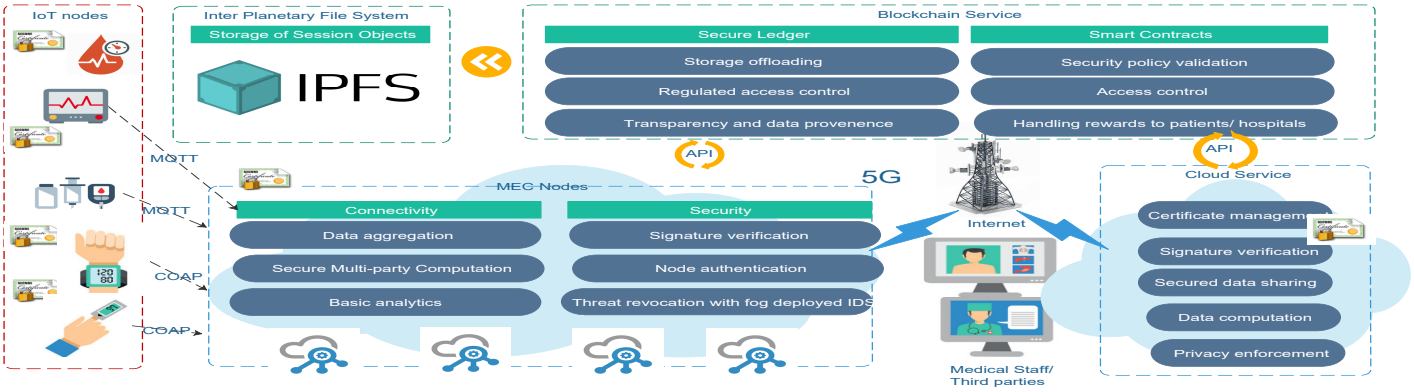
We propose an IoT-MEC-Cloud based architecture as illustrated in Figure 1, linked to the blockchain and Inter Planetary File System (IPFS) to achieve end to end security, scalable data storage, high throughput, and efficient operational capability in the resource restricted computational infrastructure. We utilize the lightweight ECQV certificate based mechanisms to ensure the lightweight cryptographic overheads in the operations.

In the proposed system, we envision seven parties: patient, hospital, device, MEC node, blockchain service layer (BSL), cloud server and trusted third party (TTP). The BSL can be seen as a trusted security utility application, which separates some services from the off-chain invocation. Note that we will further assume that the hospital is responsible for the correct access control to the doctor(s) related to it.

The following nine main phases in the system are distinguished and are illustrated on Figure 2.

1) **System initialization**: Without loss of generality, we can assume the existence of one TTP, who decides on the EC, generator G, hash function $H()$, symmetric key encryption function $E_K(.)$ with symmetric key K, and chooses a random value d_{TTP} as private key. The parameters $EC, G, Q_{TTP}, H(.), E_K(.)$ with public key of TTP, $Q_{TTP} = d_{TTP}G$, are publicly available.

Fig. 1: The System Architecture



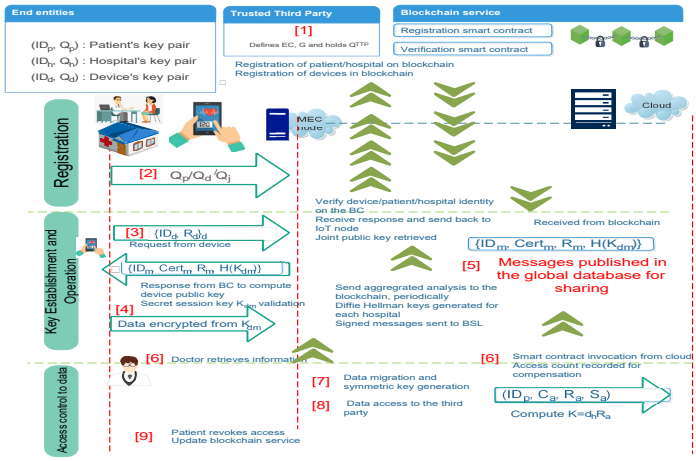


Fig. 2: The message flow

The MEC nodes with identity ID_m obtain a private and public key pair (d_m, Q_m) through ECQV from the TTP with $Q_m = H(ID_m, Q_m) + Q_{TTP}$.

2) **Registration phase of patient, hospital and device**: In this phase, the patient and hospital first obtain a private-public key pair (ID_p, Q_p) and (ID_h, Q_h) through ECQV via the TTP. The hospital publishes on the BC its identity, public key, time of registration, and certificate $(ID_h, Q_h, T_h, Cert_h)$ with $Q_h = H(ID_h, T_h, Cert_h)Cert_h + Q_{TTP}$ invoking the smart contract via blockchain API.
The patient publishes on the BC its identity, identity of the hospital to who (s)he trusts his/her data, public key, time of registration, and certificate $ID_p, ID_h, Q_p, T_d, Cert_p$ with $Q_p = H(ID_p, ID_h, T_p, Cert_p)Cert_p + Q_{TTP}$.
Next, a joint public key pair (d_j, Q_j) for patient and hospital is constructed. For that, using the public key based mechanisms to establish a secret channel, the random numbers r_1, r_2, selected by patient and hospital respectively, are securely shared among them in order to derive the new private key d_j and corresponding public key $Q_j = d_j G$. This joint public key is added to the BC related information of the patient.
Also the devices going to monitor the patient will be registered by the hospital on the BC at time T_d. Therefore, the device receives a private-public key pair (ID_d, Q_d) with certificate $Cert_d$ where $Q_d = H(ID_d, ID_p, ID_h, Q_j, T_d, Cert_d)Cert_d + Q_{TTP}$ through ECQV via the TTP. On the BC, the information $ID_d, ID_p, Q_d, T_d, Cert_d, Q_j$ is published.
3) **Key establishment between IoT and MEC node**: The IoT device sends a request message containing the signed message $\{ID_d, R_d\}_{d_d}$ of its identity ID_d and random value $R_d = r_d G$. Upon arrival of this message, the MEC node verifies the existence of ID_d on the BC, and looks up its corresponding public key Q_d and identifiers ID_p, ID_h, Q_j. It verifies also on the BC if the patient has ID_h as its preferred hospital and corresponding joint public key Q_j. If then also the signature is correct, it verifies in its local database if an analysis of ID_p is already ongoing. If so, it adds the current request to this analysis with identifier ID_a. If not, it creates a new analysis identifier ID_a. Next, the response containing $(ID_m, Cert_m, R_m, H(K_{dm}))$ with $K_{dm} = (r_m + d_m H(R_d, R_m))(R_d + H(R_m, R_d)Q_d)$ is sent to the IoT node and ID_d, K_{dm}, Q_j is securely stored in the database, containing the information related to ID_a. Based on the received response, the IoT device can first compute with ECQV the public key Q_m and verify the correctness of the hash by also computing the secret session key $K_{dm} = (r_d + d_d H(R_m, R_d))(R_m + H(R_d, R_m)Q_m)$. If so, both are mutually authenticated and share the same session key K_{dm}, which is due to construction, secure for perfect forward secrecy and session information leakage attacks.
4) **IoT-Cloud data sharing operation**: Using the session key K_{dm}, all data M from the IoT node can now be securely sent to the MEC node as $(ID_d, E_{K_{dm}}(M))$.
The MEC node first checks the existence of ID_d in its database to find the session key and the corresponding

analysis ID_a to which it belongs. Based on that info, it can decrypt the message and use it for the complete analysis profile of the patient.

5) **Active patient cloud update**: After a fixed period, the different aggregated analyses of all ID_a are sent to the BSL for publication on the BC. For each analysis, it computes a random point $R_a = r_a G$ and Diffie Hellman key $K_a = r_a Q_j$ with the corresponding hospital and patient (using the joint public key). This key is used to encrypt the analysis data M_a, to obtain $C_a = E_{K_a}(M_a)$. Next, the message is signed by $s_a = r_a - h_a d_m$ with $h_a = H(ID_m, ID_p, R_a, C_a)$. The message $ID_m, (ID_p, C_a, R_a, s_a)_a$ is sent to the BSL.
   Upon arrival of all these messages, coming from different MEC nodes, the BSL combines the messages of each MEC and performs an aggregated signature verification by computing $(\sum_a s_a)G = \sum_a R_a - (\sum_a H(ID_m, ID_p, R_a, C_a))Q_m$. If it is correct, the authentication of all messages related to the same MEC is verified at once and each message (ID_p, C_a, R_a, s_a) is stored in the global database, together with a link on the BC by invoking the smart contracts.
6) **Active patient information retrieval**: The doctor and patient are now able to retrieve at any moment the data related to the patient by taking the records (ID_p, C_a, R_a, s_a) stored in the cloud server and computing $K = d_j R_a$ to obtain $M_a = D_{K_a}(C_a)$. The access query is validated by the smart contracts.
7) **Data sharing activation**: When the patient-hospital relationship has been detached, for instance, 3 months after discharging, the patient data will be transformed to a shareable state by revoking the previously joint key pair within the system. Patient data will be decrypted and re-encrypted with a new random generated session key. This session key is shared with the patient by encrypting it with the patient's public key.
8) **Data sharing with third party**: When the third party needs to get the patient's data, the hospital will be contacted and the hospital triggers the patient about the request. When the patient accepts the sharing request, the patient shares the session key and the data can be decrypted. The data will be shared in plain form without revealing the patient's identity to the third party. The key recycling policy is established in the smart contract, for instance by expiring the session key after 1 month or recycle the key after single data sharing operation. Each key expiry will require encryption of the data again from the newly generated session key.
9) **Access revocation**: Suppose the patient wants to change its preferred hospital, then it registers again with the TTP and receives a new private-public key pair, containing the new hospital identifier in its calculation of the public key. It need to create a new joint key and also all devices used by the patient need to renew their certificate. Via a smart contract, the MEC node is made aware of an update of hospital and all ongoing analyses with ID_p involved, change the stored joint public key to which the patient is linked. The smart contract is invoked to flag the access revocation on data.

IV. Security Analysis

The required security features of the proposed system are obtained using well established and secure building blocks like ECQV, Shnorr signature and Diffie DH key, who rely on the security of the ECDLP and ECDHP. A focus on the security features is as follows.

1) Authentication: The authentication of IoT nodes, MEC nodes and cloud is guaranteed by the usage of the Schnorr signature in each message. Through the signature verification, the exchanged messages are secured against impersonations and man-in-the-middle attacks since forging the messages is difficult according to hardness of the Elliptic Curve Diffie Hellman problem (ECDLP).

2) Integrity: The integrity is obtained in the same way as the authenticity since the signature is generated on the complete content of the message by means of a hash operation satisfying protection against collisions, pre-image and second pre-image attacks. Consequently, signatures cannot be forged by any other party.

3) Confidentiality: Thanks to the key establishment between IoT node and MEC node, the data sent from IoT to the MEC is encrypted using the symmetric encryption algorithm such as AES-256. The aggregated data is sent from MEC to cloud, encrypted by means of Diffie Hellman key, constructed using the joint public key of hospital and patient.

4) Anonymity in shared patient data: The patient data is accessible to the third parties after expiring the continuation of the patient with the hospital, for instance 3 months after discharging from the treatments. However, the patient and hospital will be assigned with a new joint key pair and the patients are only mapped in the hospital for the older data to trigger access requests and reward them for the data sharing. The patient's data is migrated to a shareable storage upon permission of the patient through the hospital and no patient identity will be revealed.

5) Access control: The access control to the patient data is enforced with smart contracts. The patient contains ownership of the data and the access to the data is granted to the attached hospital, using the joint key pair, by default in the treatment process. The access of the hospital is revoked automatically using the smart contracts after a predefined period of time when the patient is detached from the treatment. The patient needs to authorize data access after the data converted into a shareable state. The data shared anonymously with the other organizations and the patient and hospital will be rewarded for the number of access attempts and volume of the shared data. The evaluation of the reward is performed through the smart contracts, which handle the access control operation. The explicit access revocation operation is also handled through the invocation of the smart contract.

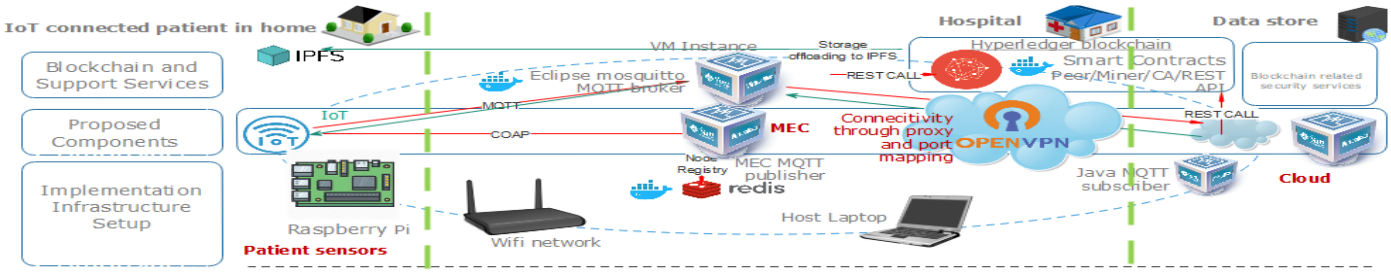


Fig. 3: The implementation setup

V. Experimental evaluation

A. Experimental setup

The computing infrastructure utilized for the implementation consists of a few virtual Machines(VM) and one host machine. The virtual machine operates Ubuntu 18.10 64 bit with 13.2GB RAM and single core allocation. The host machine consists of Intel(R) Core i5 -8250 CPU with four cores and eight logical processors. Figure 3 provides an overview of the implementation setup. The proposed architecture integrates the MEC computing module as an intermediary to establish the connectivity between IoT nodes and the cloud. The IoT-MEC connectivity is established in the implementation with Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) protocols, which are widely used application protocols in the IoT context. We used Raspberry Pi as IoT nodes which represent the medical sensors and actuators in the experimental evaluation.

The experimental environment with Hyperledger Fabric blockchain platform, is connected to the Inter Planetary File System (IPFS) as the extension of storage. The Hyperledger Fabric blockchain platform is connected to the MEC nodes and cloud service via REST API connectivity to submit and retrieve transactions. The IPFS is connected to the smart contracts via REST API in order to store the objects in the distributed storage. The smart contracts are deployed in the Hyperledger blockchain to operate on different steps of intervention of the blockchain. The blockchain service is connected to the BSL which is being invoked by the smart contract via REST API to offload a few cryptographic transactions.

B. Transaction generation

A near realistic transaction generation implemented by making the transactions follow a Poisson arrival with defined mean values corresponding to the transactions per second (tps). The rate parameter λ is defined for the generated tps.

The simulation of transaction traffic is performed by the multi-threaded software codes. The rate parameter is configurable when the test is conducted. The transaction generation follows a Poisson distribution with rate parameter λ and the probability of observing k events in the time period is denoted as

$$P(X = k) = \frac{e^{-\lambda}\lambda^k}{k!}$$

The average of the measuring parameter R for N requests triggered on each λ is denoted as

$$\bar{R} = \frac{1}{N}\sum_{i=1}^{N} R_i$$

C. Experiment

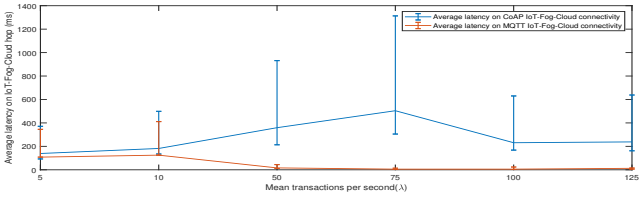


Fig. 4: The IoT registration delay over MQTT and CoAP

1) IoT Device/Hospital/Patient registration delay: The registration process corresponding to IoT device, hospital, and patient registration processes are the same in terms of interaction. Through the MEC based architecture we facilitated MQTT and CoAP IoT protocols. We observed that, there is a performance bottleneck which hinders the scalability due to the smart contract invocation as illustrated in Figure 4. However, the blockchain service scalability is feasible with different specialized approaches. The healthcare use cases usually do not expect to perform a higher number of registrations in realtime.

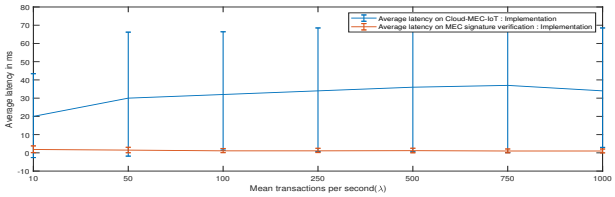


Fig. 5: The IoT to Cloud data upload via MQTT

2) IoT to Cloud Data Upload delay: We evaluated the IoT-Cloud data upload latency over the MEC connectivity. Previously we observed that MQTT is better in terms of latency and therefore we run this experiment through MQTT. We used to publish the data from the IoT nodes into different topics while the subscribing cloud listens to each and every topic with individual thread assigned for processing. The results prove as in Figure 5, that even in 1000 transaction per second, the latency

does not increase drastically indicating the performance optimal design of the proposed architecture.

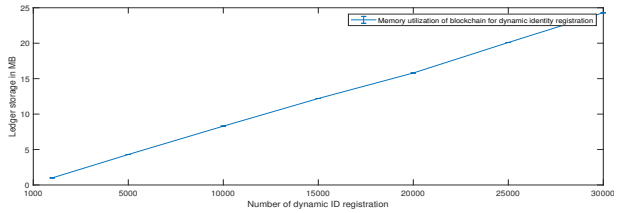


Fig. 6: The blockchain storage utilization for registrations

3) Scalability Analysis Storage utilization in Blockchain : We offload the storage overheads to a manageable distributed storage to improve the scalability of solution. We focused the storage utilization of the Hyperledger fabric blockchain by retrieving the growth of the actual ledger using CouchDB administration tools in Hyperledger. In the evaluation, we observed that around 4MB is utilized for dynamic registration of 5000 objects which is relatively low and makes the system scalable with minimal storage overhead. The results are displayed in Figure 6.

D. Comparison with Related Work

TABLE I: Features Comparison with Key Related Works

Features	[7]	[8]	[9]	[11]	[12]	Proposal
ECQV certificates	No	No	No	No	No	Yes
Remote patient connectivity	No	Yes	Yes	Yes	Yes	Yes
Scalable storage	No	No	No	No	No	Yes
Patient anonymity	Yes	No	No	No	Yes	Yes
Operating on realtime data	No	Yes	Yes	Yes	Yes	Yes
Decentralization	Yes	No	No	Yes	Yes	Yes
Data sharing rewarding	No	No	No	No	No	Yes
Blockchain fees	N/A	No	N/A	No	No	No

VI. Conclusions and Future Work

A global interest towards telehealth systems surged with the pandemics to keep the patients home and connect to the hospital persistently on the treatment process. The growth of global elderly population is also a significant reason for the researchers to investigate on the telehealth systems in depth. We proposed a MEC and blockchain based secure service architecture which provides data privacy, integrity, authentication, and anonymous data sharing capability for the future research using lightweight ECQV mechanisms. We compared our work with a few existing solutions in Table I We incorporated the smart contracts to execute different actions of the proposed systems such as signature verification, access revocation and so on. We performed a near realistic performance evaluation and validated that our system can tolerate high transaction volumes through the MEC nodes, with minimal latency. Furthermore, we optimized the blockchain storage by offloading to the IPFS storage which is extensible. Overall, our solution was designed targeting the lightweight computing nodes and we observed the benefits for performance in the evaluation.

We expect to develop the proposed system towards more scalability by evaluating with other blockchain platform. We further expect to enable on-chain secure multi-party computations on the healthcare data.

Acknowledgement

This work was supported in part by the Academy of Finland Project 6Genesis Flagship (Grant No. 318927), RESPONSE 5G (Grant No: 789658) and the European Unions Horizon 2020 research and innovation programme under the INSPIRE-5Gplus project (Grant No. 871808). The paper reflects only the authors views. The Commission is not responsible for any use that may be made of the information it contains.

References

[1] D. M. West, "How 5G Technology enables the Health Internet of Things," *Brookings Center for Technology Innovation*, vol. 3, pp. 1–20, 2016.

[2] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-access Edge Computing for Internet of Things Realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[3] C. Research, "SEC4: Elliptic Curve Qu-Vanstone implicit certificate scheme, Standards for Efficient Cryptography Group. Version 1.0." *Brookings Center for Technology Innovation*, 2013.

[4] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[5] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2018, pp. 1–7.

[6] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain Meets Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[7] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the Design of a Blockchain-based System to Facilitate Healthcare Data Sharing," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1374–1379.

[8] M. Chen, W. Li, Y. Hao, Y. Qian, and I. Humar, "Edge Cognitive Computing based Smart Healthcare System," *Future Generation Computer Systems*, vol. 86, pp. 403–411, 2018.

[9] P. Pace, G. Aloi, R. Gravina, G. Caliciuri, G. Fortino, and A. Liotta, "An Edge-based Architecture to Support Efficient Applications for Healthcare Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 481–489, 2018.

[10] X. Wang and Z. Zhang, "Data Division Scheme based on Homomorphic Encryption in WSNs for Health Care," *Journal of medical systems*, vol. 39, no. 12, p. 188, 2015.

[11] A. Islam and S. Y. Shin, "BHMUS: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City," in *2019 7th International Conference on Information and Communication Technology (ICoICT)*. IEEE, 2019, pp. 1–6.

[12] H. D. Zubaydi, Y.-W. Chong, G.-S. Ham, K.-M. Ko, and S.-C. Joo, "A Decentralized Consensus Secure and Authentication Framework for Blockchain-Based Healthcare Application," in *Advances in Computer Science and Ubiquitous Computing*. Springer, 2018, pp. 550–556.