Blockchain-based Mobile Edge Computing Framework for Secure Therapy Applications

Md. Abdur Rahman[1], *Senior Member*, *IEEE*, M. Shamim Hossain[2], *Senior Member*, *IEEE*, George Loukas[3], *Member*, *IEEE*, Elham Hassanain[1], *Member*, *IEEE*, Syed Sadiqur Rahman[1], Mohammed F. Alhamid[2], *Member*, *IEEE*, and Mohsen Guizani[4], *Fellow*, *IEEE*

[1]Forensic Computing and Cyber Security Department, University of Prince Mugrin, Madinah

[2] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

[3]School of Computing and Mathematical Sciences, University of Greenwich, London, UK

[4]Dept. of Electrical and Computer Engineering, University of Idaho, Moscow, ID 83844-1023, USA

{m.arahman, e.hassanain, s.syed}@upm.edu.sa, {mshossain, mohalhamid}@ksu.edu.sa, g.loukas@gre.ac.uk, mguizani@ieee.org

Corresponding author: M. Shamim Hossain (mshossain@ksu.edu.sa)

Acknowledgement:

The authors extend their appreciation to the International Scientific Partnership Program (ISPP) at King Saud University, Riyadh, Saudi Arabia for funding this research work through ISPP-121.

Abstract— Mobile edge computing (MEC) is being introduced and leveraged in many domains, but few studies have addressed MEC for secure in-home therapy management. To this end, this paper presents an in-home therapy management framework, which leverages the IoT nodes and the blockchain-based decentralized MEC paradigm to support low-latency, secure, anonymous, and always-available spatiotemporal multimedia therapeutic data communication within an on-demand data-sharing scenario. To the best of our knowledge, this non-invasive, MEC-based IoT therapy platform is first done by our group. This platform can provide a full-body joint range of motion data for physically challenged individuals in a decentralized manner. With MEC, the framework can provide therapy diagnostic and analytical data on demand to a large portion of humanity who are either born with disabilities or became disabled due to accidents, war-time injuries, or old age. For security, the framework uses blockchain–Tor-based distributed transactions to preserve the therapeutic data privacy, ownership, generation, storage, and sharing. Our initial test results from a complete implementation of the framework show that it can support a sufficiently large number of users without considerable increase in mean processing time.

Index Terms— Blockchain; mobile edge computing; therapy; IoT.

I. Introduction

ALTHOUGH mobile edge computing (MEC) has been implemented in many domains, its application in the therapy field has gained minimal attention. The recent advancements in the IoT devices have provided gesture-tracking devices with great power and capability. Thus, existing therapeutic IoT devices for cloud communication architecture need to be redesigned to leverage the MEC. MEC works as an intermediary between entities related to the physical world, such as therapeutic sensory media and IoT nodes, and the cloud in the cyber world [23] [24][26][27][47]. With the help of disruptive decentralized technologies (e.g. Tor, Blockchain), MEC can provide anonymity, privacy and secrecy of therapeutic data [4][6][7]. Therefore, the MEC for therapy applications need to be carefully designed. Accordingly, the therapeutic IoT data will be secured and anonymized although the IoT hardware API is being designed and maintained by any third party. The incorporation of blockchain and Tor will bring robustness to security implementation. A patient can perform any therapy activity or a transaction without the need for a central or a middleman. The chain of blocks will contain the time-stamped history of therapeutic activities and transactions [1][2][3]. The health data can then be secured [49] from cyber-attacks or unauthorized access from medical institution personnel or anyone in the middle, thereby protecting the medical institutions from financial fines or worse [5].

An in-home therapy environment is composed of numerous gesture-tracking IoT devices, such as Leap Motion, Myo, and Kinect2, and other in-home smart sensors for ambient therapeutic context collection [45][46]. For real-time therapeutic applications, such spatiotemporal multimedia data generated by each therapy session comprise a large volume of data to be shared with the cloud [45][50]. Health therapeutic IoT

sensory data at the MEC layer can be processed at the edge to save bandwidth and to add appropriate security solutions [9].

Recently, Blockchain has gained attraction for therapeutic applications [12][13]. In particular, decentralized yet secure and seamless integration and interaction with the therapy profile are necessary when a therapy patient is mobile, i.e., has to go to different medical institutions or disability hospitals, as a result of moving among inter-MEC nodes [18].

Although blockchain supports strong security, it suffers in terms of anonymity because each transaction added to the block enforces blockchain addresses related to the block, which is visible to the public [3]. Researchers have proposed a multitude of solutions, such as using Tor, a one-time pad address for each transaction, secure wallets, TumbleBit, and Zcash, to add anonymity to blockchain transactions [5]. Raw IoT data from therapy applications can thus be anonymized. The MEC node is assumed to host a cloudlet that acts as a high-end computing platform that can run blockchain nodes or Tor virtual machines.

In addition to security and privacy, a MEC node can be used in tandem with other scalability solutions, such as 5G inter-IoT node and IoT-to-MEC node communication [20][25]. In the context of therapy in which a patient can perform therapy transactions on demand, MEC nodes can be deployed at each user physical proximity to provide therapeutic data a ubiquitous access to cloud services. In this study, we propose a novel mobile edge network that uses blockchain, an anonymous Tor tier, and a secure distributed DB to make therapy applications immutable, always available with service quality, and interoperable. To the best of our knowledge, this therapy application is one of the first to propose a secure mobile edge network solution.

The rest of this paper is presented as follows. Section II reports the related work. Section III illustrates our proposed framework. Section IV describes the implementation. Section V elaborates the conclusions and future work.

II. Related Work

Authors of [1] have proposed a blockchain-based electronic medical record management system. A pervasive social network-based healthcare management system has been shown in [2], in which sensory data from body area network have been secured using blockchain. Authors in [3] have proposed an anonymous key management scheme to provide blockchain privacy. Authors in [5] present a blockchain-based cloud medical data-sharing framework, in which smart contracts are used for the secure access of the data. A multiparty blockchain that targets supply-chain management [6] has been designed to secure IoT data. The availability in terms of the number of transactions per minute the state-of-the-art Ethereum public blockchain can commit has been presented in [10]. An important usage of blockchain, which is digital identity management in the context of smart city applications [50], has been shown in [11]. A secure medical sensory health data-sharing web application designed by leveraging blockchain has been portrayed in [12]. In [15], programmable DApp Blockchain have been evaluated with healthcare quality-of-service delivery metrics. An advanced e-Health blockchain has been implemented in the context of medical data storage and exchange within medical institutions [16].

An attribute-based signature scheme in a multiparty authority blockchain has been shown in the context of an electronic healthcare delivery system [17]. Authors in [18] have designed a mobile application that can securely collect health data, share them with healthcare and insurance providers, and synchronize them with cloud services. Blockchain has been studied and evaluated to be used as cloud healthcare data security by the authors in [19]. Different types of security attack landscapes that may compromise mobile edges and 5G communication networks have been surveyed by the authors in [20]. A comprehensive survey on blockchain for IoT applications can be found in [21].

Authors in [7] have demonstrated the use of a permissioned blockchain, named Multichain, and to secure IoT data. This system can be hosted in mobile edges[9] [52]. The work presented in [13] scrutinizes the pros and cons of existing edge-centric IoT applications with respect to blockchain consensus mechanisms. A real-time IoT-based patient-monitoring framework has been shown to leverage data mining and distributed services at mobile edges for a high quality of service [34]. User privacy and protection against malicious users that may compromise edge networks have been studied and a novel solution has been proposed in [22].

A comprehensive survey on MEC can be found in [8]. An IoT-based smart healthcare management system has been outlined [4][51]. In this work, fog nodes are used to support scalability of healthcare data and blockchain is used to secure them. An offloading of task and computation from mobile terminals to fog nodes has been illustrated in [14] with a cost model to optimize the task execution

delay and energy. A joint offloading of task and data between a set of mobile devices and a set of mobile edge servers has been shown in [23][24] with a game-centric pricing mechanism. A virtualization model for offloading tasks at a mobile edge-based 5G network has been proposed [25]. While other architectures use a flat offloading model from mobile terminal to the MEC base station, authors in [26] envision an inter-MEC base station offloading when one MEC base station is overloaded with tasks. A fair resource allocation scheme for mobile users, which will optimize mobile edge resources, has been illustrated in [27].

A novel crowd-sourcing-based MEC model has been proposed as a dynamic edge proxy [28]. Authors in [29] have proposed a novel 5G edge resource maximization technique that can handle numerous concurrent offloading requests from mobile clients. While the existing literature attempts to optimize the offloading to MEC from the technical perspective, authors in [30] take the stance of modeling human behavior within a game theory to optimize the MEC offloading process. In [31], MEC solution has been studied to provide fast and real-time delivery of automatic driving services. In [32], authors have leveraged the MEC architecture for crowd-sensing applications, in which raw sensory data of large volume can be shared and saved in clouds with improved scalability. An energy-efficient task offloading in a 5G MEC network has been outlined in [33]. MEC paradigm has been evaluated for its suitability in IoT-based interactive games, which require a heavy server-side interaction. Authors have found that the MEC outperforms traditional cloud-only solutions [35]. A task caching framework, which leverages mobile edges for offloading tasks, has been proposed in [36].

In the context of the Internet of connected vehicles, the authors of [37] have shown the benefit of using MEC coupled with cloud solutions for the life cycle of auto-charging electric vehicles. The authors have proposed an energy-harvesting model by allowing mobile nodes to offload tasks to nearby mobile edge towers for obtaining energy efficiency at the mobile nodes [38]. The authors of [39] have attempted to use an edge-centric approach to multimodal authentication for deciding the optimum amount of load balancing between edges and cloud biometric templates. The authors have used [40] spatiotemporal Markov decision process to optimize energy consumption, processing time, and transmission cost for a synchronous task offloading among a mobile device, the edge network, and the cloud. The work outlined in [41] uses a mobility-aware hierarchical MEC framework. The work in [42] supports user mobility within the fog layer by leveraging the SDN approach. [43][53] uses machine-to-machine communication at the MEC layer to maximize computer resources and minimize the energy at the edge network. An edge network suitable for healthcare 4.0 has been designed in [44].

Although numerous existing works have been proposed in literature, none of them have studied physiotherapy applications for secure MEC applications. A growing body of blockchain applications in healthcare have shown that it is a technology that can offer tangible benefits in the sector. However, existing research has focused on services that do not have strict privacy, anonymity, and real-time requirements simultaneously, as in the case of IoT-supported therapy. In the next section, we detail the design of a framework that leverages the real-time benefits of MEC and has the anonymity benefits of Tor and the decentralized privacy and security of blockchain that remove the need for a central authority.

III. Secure IOT Framework Architecture

Design Considerations

Before we discuss the system design, we first indicate the need for blockchain and Tor for the IoT-based therapy system. Blockchain is attractive for applications in which a set of distributed copies are required for redundancy. Another important characteristic of the system is that the IoT nodes that are involved in the therapy process cannot trust the third party system that receives the health data. Whether the IoT nodes may be deployed in an untrusted network, controlling who can regulate the blockchain framework is necessary. In other words, if an IoT device is compromised, then the rest of the IoT devices will have no effect on it because the signature of each IoT device is different and governed by a one-time address. The health data once created or captured by the IoT nodes are not allowed to be altered or modified in their future lifetime; therefore, saving the data in blockchain makes perfect sense. All these requirements make the combination of blockchain and Tor a candidate security application [5].

High-Level Framework

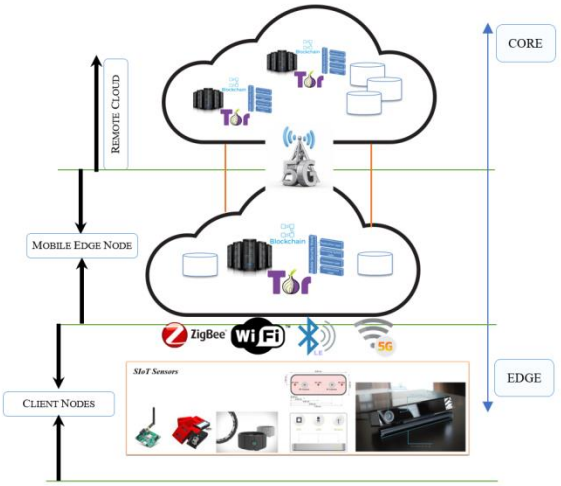


Fig. 1. IoT, mobile edge/cloudlet, Tor, blockchain, and cloud environment for the proposed therapy application

Figure 1 shows that therapy-related IoT devices forward their traffic to MEC nodes, which conduct the security handling and small-scale analysis and then share the final results with the cloud. The task of decentralization and anonymity of therapy data also occurs in the MEC nodes. Through the advancements in 5G technologies, the MEC nodes can provide many IoT-edge-centric services to therapy applications, thereby reducing the load on cloud. The MEC node supports security and anonymity of therapy and IoT data; once deployed near public places, it can securely support therapy applications with mobility of the users [29][33].

As shown in Figure 1, a cloudlet server can be hosted at the house of a patient or at the medical institutions or at the premises of the base station [42]. The cloudlet server acts at the IoT edge network to support the IoT data processing, securing, storage, and analytics at the edge. This feature will allow high-data-rate IoT gesture-tracking sensors to be processed with low latency and high security in a decentralized manner. In the absence of a mobile edge tower, a smaller server, such as a laptop, a smartphone that can intake the sensory data and share them with the cloudlet, or a mobile edge network, can be used as an edge router for further processing [14].

In case of a therapy application, a therapist creates a high-level therapy that targets a particular type of disability. The therapist can then map the therapy to a particular disabled patient. The therapist can also create a 3D game in augmented or virtual reality mode to save a model therapist for assisting a patient at home. The model therapy can be played by the patient at home, while the gesture-tracking sensors and other ambient sensors capture different motions and the quality of the therapy as the patient records the therapy. At the end of each therapy session, the complete multimedia session can be saved to the user session in the repository for further analysis of the session data. The user-submitted session is then parsed by an analytic engine to extract the quality of information for report generation and sharing with the therapist. The therapist can review the online multimedia and test results and can approve or change the therapy or complexity levels. The therapy results can be shared with the community of interest or other therapists or institutions.

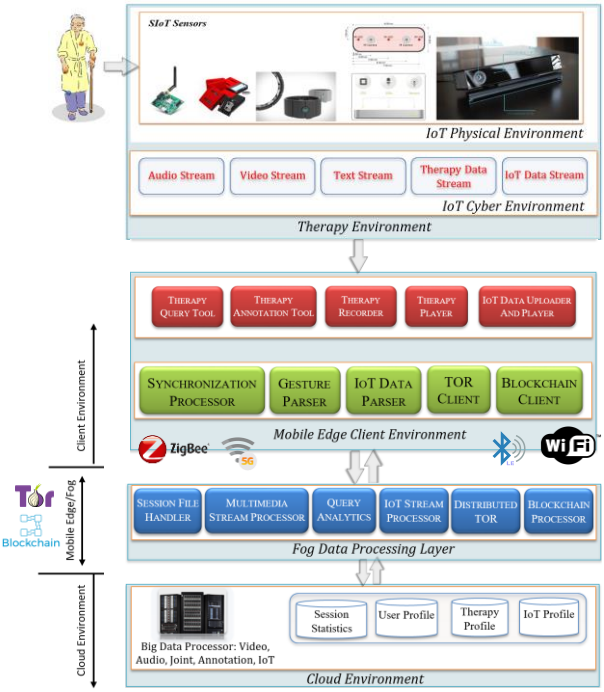


Fig. 2. Cyber physical high-level block diagram of the proposed secure, decentralized therapy application

Another important aspect is the possibility of sharing health data seamlessly among different entities [5][18]. For example, a patient can visit different therapists that work at different institutions and go through various types of paperwork and medical tests. All of the above-mentioned types of interactions actually demand a large amount of therapeutic multimedia data that can be captured, analyzed, stored, processed, and shared with a community of interest. Thus, securing patient data with proper privacy and integrity of the captured data is of utmost priority of such a therapy system. Electronic therapy records will need a portable data structure, which will allow the therapy history to be shared across the geographic boundary. Figure 2

shows the necessary software components to support the aforementioned scenario.

Software Components

With the help of multiple non-invasive gesture-tracking and IoT sensors at the vicinity of the patient, the framework collects the therapeutic data and securely shares them with big-data repository and its stakeholders. The blockchain for the therapy application uses a set of trustless MEC and cloud nodes for storing the committed blocks that contain therapy transactions. The therapy application block consists of the time of its creation, the hash of the previous block, the hash of the current transactions and block data, the patient's therapy profile, the user profile, and the healthcare provider/therapist information. Every time a new patient profile is created, a new therapy is assigned to a patient, a new prescribed therapy is provided, or a new therapy session is added to the system, a new block needs to be inserted into the blockchain. Once a majority of the consensus peers accept the new block, it is added to the blockchain. The longest-chain rule is maintained by the nodes to avoid any attack.

Sidechains, off-chains, and altchains are assumed to be loosely coupled with the chain and will not be part of a main blockchain consensus mechanism within the permissioned consensus mechanisms in the proposed private or public shared blockchain ledger system to support scalability and avoid latency problems [21]. However, a sidechain can be maintained to support offloading of many non-transactional activities, such as multimedia data, including images, audios, and videos related to the therapy, which can be stored in the sidechains linked with a transactional block that is saved in the main blockchain. A bridge among different therapy applications running on different types of blockchain models can be maintained to support altchains [21].

A set of trusted nodes participates in the consensus mechanism of adding a therapy transaction within the set of blocks. As a result, the IoT-based transactions become fast. Block creation rate and the size of each block can be customized depending on the therapeutic needs to support scalability. As for the underlying transaction model, the framework supports an UTXO model for financial transactions and a smart contract for the spatiotemporal activity log of a patient [21]. For example, a therapist can design a smart contract and add to the block; in this way, the contract will be activated, completed, and added to the block through a closed consensus mechanism when the patient does that therapy activity with the stipulated time duration [13]. The smart contract can embed logic, such as whether the required times of therapy action have been performed in a day with certain frequency per session. The therapy monitoring and supervising system is costly to maintain due to the involvement of professional therapists; therefore, a transaction fee-based mining of the blocks is assumed either using proof-of-work or delegated proof-of-stake consensus model.

Smart Contract

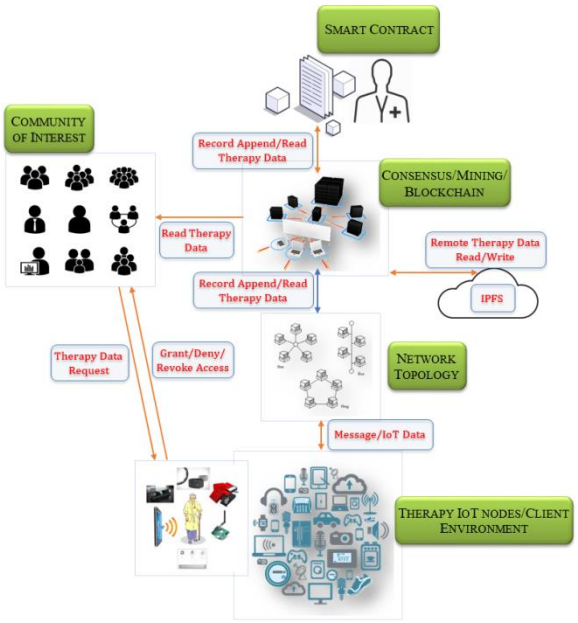


Fig. 3. High-level diagram to obtain permission from the patient, read/write to blockchain/edge network, and remote cloud big-data repository

Figure 3 depicts a therapy patient surrounded by a set of gesture-tracking sensors and ambient intelligent IoT sensors that support in-home therapy sessions [46]. The IoT nodes and gesture-tracking sensors are made secure by private/public keys. A patient can give access to his/her therapeutic data to anyone in the community of interest, such as caregiver, therapist, insurance company, medical doctor, and hospital authority. Moreover, the patient-related data can be digitally signed and saved into the blockchain by trusted parties, such as a physio-therapy center, a therapist, the patient, and the caregiver. The patient can also authorize a subset of his/her therapy data on an ad hoc basis. The therapist can create a smart contract, which provides metadata related to a therapy that needs to be performed, and save it for further execution. The smart contract embeds the access policy of the patient. Any transaction that enters the edge network is parsed by the geographically distributed permissioned

mining/consensus nodes to be approved and added to the blockchain.

Each therapy session results in a large amount of multimedia data in the form of text, image, audio, and video [45][46]. Thus, an offline centralized cloud or decentralized cloud storage can be used to store the multimedia data, while the transaction in the blockchain stores the hash of the pointer or the files distributed in the cloud storage. While reading or querying the file, the patient has to first authenticate with the private key to obtain the hash of the distributed file pointers and then acquire the actual file by providing the distributed hash to the cloud controller [21]. The cloud storage pointer hash is saved in the blockchain and then goes through a Tor network anonymity; the security, immutability, integrity, and backup of the hash are therefore guaranteed. A distributed cryptographic P2P cloud storage architecture, such as StorJ, BigchainDB, or IPFS, can be adopted to improve the security and backup of the files. The patient is in the center of ownership of their therapeutic data stored in different autonomous and private health institutions' computer systems and can share their data on demand with any institution through the cryptographic signature in the blockchain [5].

In summary, the smart contract stores the cryptographic public ID of the patient, therapist, hospital, caregiver, and other community of interest and their relationship, the permission, and the authorization level by different entities. When anyone wants to access a particular therapy profile or historical therapy data, the smart contract is used to validate the access control, permission, and relationship among the entities and share the hash of the actual off-chain health data that belong to the joint ownership [17]. The off-chain health data can be queried with the session key obtained from the smart contract execution.

Setting up of the Key

IoT, mining, consensus or approval, and Tor nodes form a P2P network to set up the environment. Each IoT node in a therapy application uses a local web server to act as an IoT node, in which a key pair is generated. Similarly, other nodes in the P2P network generate a private key and a public key. The private key is saved in a wallet, and the public key is shared with other peers. The private key is used for signing/approving blocks or transactions within the blocks and reading the encrypted messages. The public key used as a unique key is adopted by peers to send any message or perform any transaction. The private key can also be used to generate a set of stealth keys as public addresses, which can be utilized for performing transactions, without revealing any identity of wallet information [3].

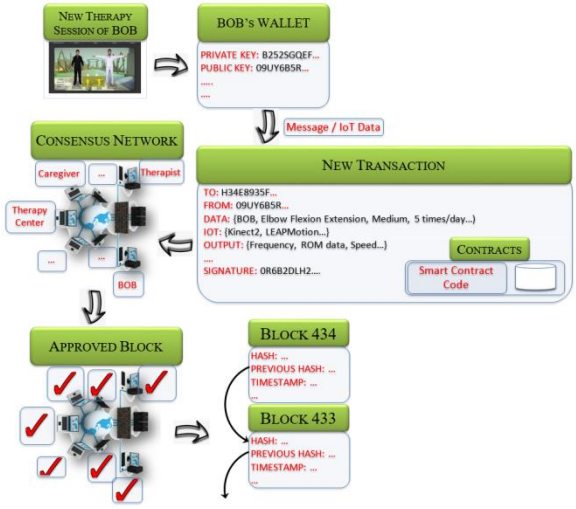


Fig. 4. Therapy data and smart contract execution process within the blockchain.

Approval of Block in the Chain

After signing by an IoT client node, the data enters into the edge peer network for further verification by one-hop edge nodes. The permissioned edge nodes, a part of the consensus or approval network (Figure 4), verify the keys, approve the transaction, and add the block into the blockchain. After approval, they are subjected to any anonymization process by passing at least N+1 levels of Tor nodes. The value of N is variable and depends on the need and available resources at the edge network. At the Tor exit node, the therapy packets are saved to the cloud as the next-hop destination node. In this mechanism, the patient's identity and the therapist or hospital authority's identity are hidden. An attacker has no way to de-anonymize any entity from the obfuscated public addresses.

Figure 5 shows a sample scenario with a 2D blockchain. A patient BOB can visit different therapists and therapy centers over a time span. Each independent center or therapist has its own blockchain, in which the patient therapy session can be added. The vertical chain corresponds to one independent chain, and a patient can be added horizontally or vertically with existing chains. The design pattern will build trust among healthcare providers although their provided services are incompatible with one another yet support a mobile patient with industry and government compliance policies, such as HIPAA.

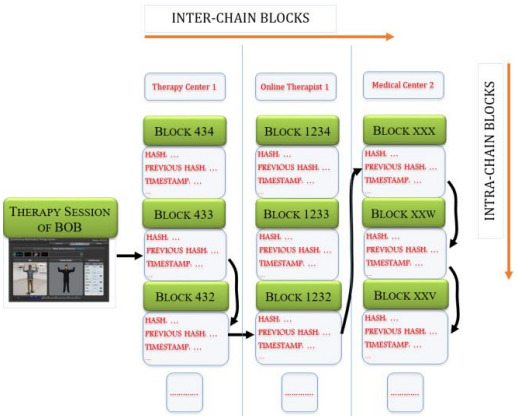


Fig. 5. Scenario in which a therapy session is stored in multiple independently maintained Blockchain by different service provider entities related to a particular disabled subject

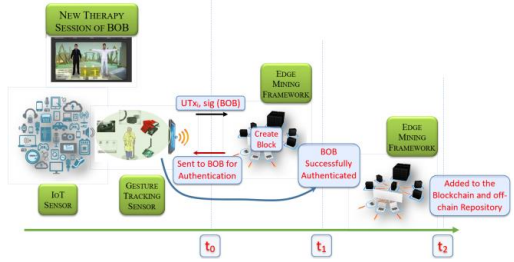


Fig. 6. Timeline perspective of the spatiotemporal addition of a set of therapy transactions to the chain

Different data types associated with the therapy framework are stored in main and off chains for immutable and secure storage. Other types of therapy scenarios follow a similar flow of the process. For example, when a disabled patient visits a therapist, the detailed activity and prescriptions are inserted into a new block. In other words, every therapist visit, every new therapy assigned, every new assessment made, and every therapy session performed at different instances will be recorded as a new block in the chain.

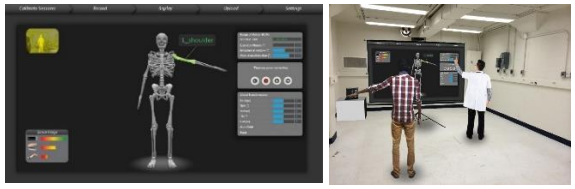
Figure 6 shows a sample scenario of the addition of on- and off-chain therapy data to the blockchain. The therapeutic sensory IoT data is first parsed and made available to the smartphone gateway as a transaction. The gateway then sends the transactions to be included in the next block for committing. The edge gateway waits until a time threshold t_0, packs all the transactions into a block, and sends them back to the smartphone application for authentication. Once the block is signed with the private key of the patient and is verified, it is distributed to the mining/approval nodes in the edge. Once more than a threshold number of consensuses are being obtained, the block is added to the chain and further propagated to MEC nodes.

IV. PROOF OF CONCEPT IMPLEMENTATION

Use Case: Secure ROM BOT - A Virtual 3D ROM Avatar

We develop a secure therapy tool called Range of Motion (ROM) BOT to provide solutions, such as real-time measurement of a human skeletal ROMs and creating model therapy exercises. These types of data serve as the backbone of benchmarking with a model ROMs. A secure ROM BOT algorithm is crucial in guiding the physiotherapy sessions by patients, driving exercise game actions, generating model therapy ROM, and thus helping with analytics and progress visualizations.

A secure ROM BOT engine is beneficial during the actual therapy session by patients by displaying a virtual skeleton that mimics the patient's action. Figure 7 (a) shows the secure, live skeletal kinematic ROM data by using three gesture-tracking sensors. Figure 7 (b) presents a therapist who diagnoses the joints of interest for a subject. Figures 7 (c) and 7 (d) show an online remote sharing of skeletal data, in which a patient shares the live therapy session with a therapist at home or at a therapy center. Data from the therapy session are secured and anonymized by the secure MEC node before they go to the cloud.



(a) (b)

(c) (d)

Fig. 7. Secure institutional and in-home therapy management scenario

Use Case: Secure Therapist On Demand

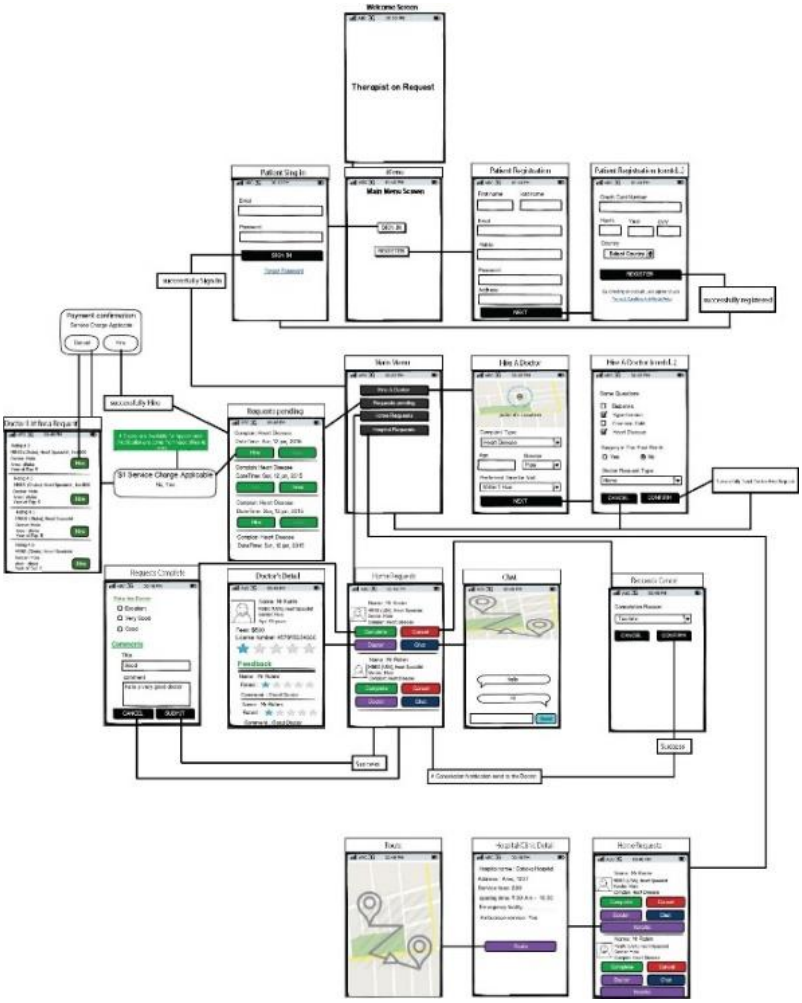


Fig. 8. On-demand secure therapist finding a module for a patient

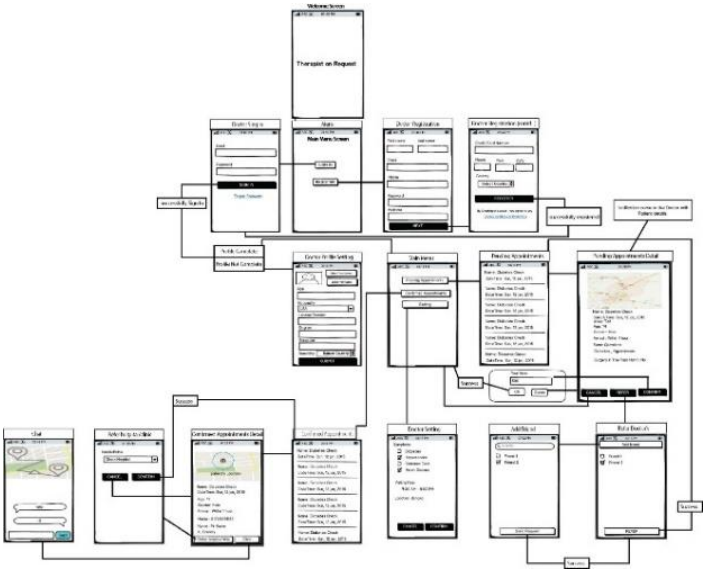


Fig. 9. On-demand secure patient management module

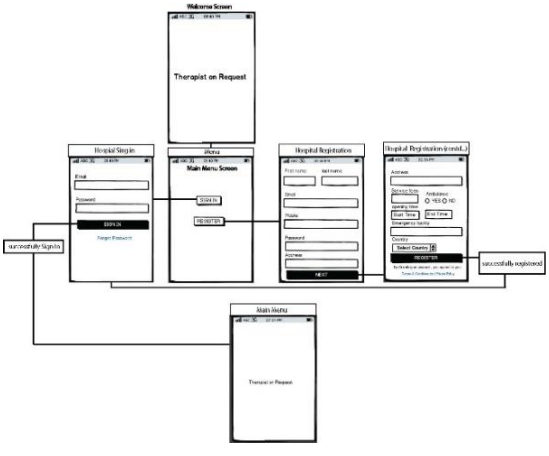


Fig. 10. Secure therapy center user interface

Figures 8–10 depict a scenario in which a disabled patient can post his/her disability; search for a therapist on demand; hire a therapist or a medical institution based on the type of disability, and the

expertise of the therapist, and the location of the hospital or in-home service; and negotiate on the per-hour or per-visit charges through the blockchain-based secure communication channel. Once a patient establishes a smart contract with a specialist, both parties can share their location and the physiological health record or previous blocks of therapy history securely. In case a hospital is referred to within the loop, a hospital is also added as a signing authority.

Test Bed Implementation Details

In both scenarios, a permissioned private blockchain mining node is assumed to be available at the MEC node, which will commit the private blockchain, with an incentive mechanism. The mining nodes can be set up at the patient or his/her community of interest's premises or by the medical institutions. We use only a soft version of mining, i.e., the consensus algorithm is only run by a selective set of trusted nodes; thus, the transactions are completed rapidly. Although the concept of "a set of trusted mining nodes" makes a weak point in the process, a physical trust and relation grow between a disabled patient and a therapist or a therapy institution in the therapy domain. The mining nodes are assumed to be part of the incentive network given that each visit to a therapist or a therapy institution is a paid service.

The mining node executes the smart contract that contains the script of the prescribed therapy. The script will allow each IoT node related to the therapy application to obtain its access read/write policy and accordingly activate the sensors. The therapeutic multimedia sensory data are first stored and processed by the off-chain MEC node, and the session metadata are stored in the blockchain for permanent storage. The transactions for storing therapy data, accessing therapy data, and monitoring or annotating the therapy data are programmed in the smart contract script. The smart contract can also use spatial predicates to enable the MEC node within the patient's home to access and store the off-chain data into a local repository or an IPFS distributed repository. This utilization allows a patient to retain a copy of his/her therapy records. The strict mining restrictions are relaxed because the framework only requires the metadata transactions related to therapy applications.

As for blockchain, we have implemented permissioned Ethereum and Hyperledger private Blockchain. The off-chain therapy solution has been implemented using IPFS [45][46]. For example, a particular therapy assigned to a patient becomes an immutable prescription in the patient profile. Once the patient does the therapy in multiple instances, the metadata of the session analytics are added to the particular therapy profile. The same therapy session may be annotated by the therapist with further comments and suggestions. All these works serve as append operation on the BigchainDB. However, whenever someone in the community of interest sends any query to the BigchainDB or intends to append any data to any particular asset or block, the patient and the interested entity have to authenticate and digitally sign using their private keys.

The web and client servers are implemented with Laravel and Angular JS, respectively. The Ethereum and Hyperledger client communicates with the node.js for acquiring the IoT data. As for the IoT data, we use three gesture-tracking sensors, namely, Kinect2, Leap Motion, and Myo sensors. As shown in Figure 6, different data types are harvested and synchronized before being sent to the blockchain. A private Tor is set up with four nodes, including two onion routers. The third one acts as onion router and authority and HTTP server. The fourth node acts as an onion client that sends the blocks by using the Tor. As for edge and cloudlet solutions, we port an extended version of the open-source cloudlet-based edge computing solution, Elijah [48]. Figure 11 shows the overall delay in capturing different types of therapeutic multimedia data, adding them to a block, and saving them to the distributed repository or at the edge network repository.

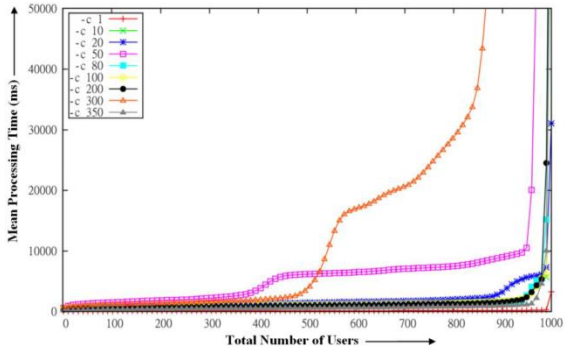


Fig. 11. Delay in accessing therapy services by using the edge network

We calculate the delay as follows:

Mean processing time = processing delay at client + network delay to upload to MEC + Blockchain processing delay at MEC + network delay at MEC to upload to IPFS and decentralized cloud + processing delay at IPFS + processing delay to add off-chain Hash to Blockchain.

As shown in Figure 11, the mean processing time increases as the number of users increases. Among different data types, c300 represents very-high-resolution hand video frames captured from the Leap Motion device, which requires much bandwidth and hence considerable time to add to the off-chain repository at the edge and cloud. Accordingly, as the number of users increases, the mean processing delay increases at a rate higher than that of other types of therapeutic data. In our future endeavor, we will look at ways to reduce the off-chain data storage time.

V. CONCLUSION

In this paper, we present a secure therapy framework that will allow a patient to own and control his/her personal data without any trusted third party, such as a therapy center. With the support of blockchain, the framework will be immune to a single point of failure or unauthorized access. The therapeutic data will be immutable, anonymous, secure, and transparent to the community of interest. The patient can share the therapy history and quality-of-improvement data with anyone he or she wants. Through a MEC network, the therapy framework can avoid the shortcomings of the high bandwidth and analytical processing need of the cloud by supporting considerable processing at the edge network. Although the blockchain only stores the immutable hashes of the therapy metadata, the actual multimedia data that contains the images, audios, videos, and other augmented reality therapy data is stored off-chain in a distributed or a centralized DB depending on the application need. This feature allows leveraging the immutabilities of metadata and annotating or updating multimedia big data.

REFERENCES

[1] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30.

[2] J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," in *IEEE Access*, vol. 4, pp. 9239-9250, 2016.

[3] H. Zhao, Y. Zhang, Y. Peng and R. Xu, "Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys," *2017 IEEE ISADS*, Bangkok, 2017, pp. 229-234.

[4] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib and F. Sallabi, "Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare," in *Computer*, vol. 50, no. 7, pp. 74-79, 2017.

[5] Q. 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," in *IEEE Access*, vol. 5, pp. 14757-14767, 2017.

[6] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," *2017 International Conference on Service Systems and Service Management*, Dalian, 2017, pp. 1-6.

[7] M. Samaniego and R. Deters, "Internet of Smart Things - IoST: Using Blockchain and CLIPS to Make Things Autonomous," *2017 IEEE International Conference on Cognitive Computing (ICCC)*, Honolulu, HI, 2017, pp. 9-16.

[8] N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[9] M. S. Hossain, G. Muhammad, and S. U. Amin, “Improving Consumer Satisfaction in Smart Cities Using Edge Computing and Caching: A Case Study of Date Fruits Classification," Future Generation Computer Systems, vol. 88, no. (2018), pp. 333-341, Nov. 2018

[10] I. Weber *et al*., "On Availability for Blockchain-Based Systems," *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, Hong Kong, 2017, pp. 64-73.

[11] R. Rivera, J. G. Robledo, V. M. Larios and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," *2017 International Smart Cities Conference (ISC2)*, Wuxi, 2017, pp. 1-4.

[12] N. Rifi, E. Rachkidi, N. Agoulmine and N. C. Taher, "Towards using blockchain technology for eHealth data access management," *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, Beirut, 2017, pp. 1-4.

[13] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," in *IEEE Access*, vol. 6, pp. 1513-1524, 2018.

[14] L. Liu, Z. Chang, X. Guo, S. Mao and T. Ristaniemi, "Multiobjective Optimization for Computation Offloading in Fog Computing," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 283-294, Feb. 2018.

[15] P. Zhang, M. A. Walker, J. White, D. C. Schmidt and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," *2017 IEEE Healthcom*, Dalian, 2017, pp. 1-4.

[16] W. Liu, S. S. Zhu, T. Mundie and U. Krieger, "Advanced block-chain architecture for e-health systems," *IEEE Healthcom*, Dalian, 2017, pp. 1-6.
[17] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," in *IEEE Access*, vol. 6, pp. 11676-11686, 2018.
[18] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," *2017 IEEE PIMRC*, Montreal, QC, 2017, pp. 1-5.
[19] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37, Feb. 2018.
[20] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, MARCH 2018.
[21] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in *IEEE Access*. doi: 10.1109/ACCESS.2018.2842685.
[22] L. Ma, X. Liu, Q. Pei and Y. Xiang, "Privacy-Preserving Reputation Management for Edge Computing Enhanced Mobile Crowdsensing," in *IEEE Transactions on Services Computing*. doi: 10.1109/TSC.2018.2825986
[23] T. Zhang, "Data Offloading in Mobile Edge Computing: A Coalition and Pricing Based Approach," in *IEEE Access*, vol. 6, pp. 2760-2767, 2018.
[24] F. Wang, J. Xu, X. Wang and S. Cui, "Joint Offloading and Computing Optimization in Wireless Powered Mobile-Edge Computing Systems," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1784-1797, March 2018.
[25] M. Liu, Y. Mao, S. Leng and S. Mao, "Full-Duplex Aided User Virtualization for Mobile Edge Computing in 5G Networks," in *IEEE Access*, vol. 6, pp. 2996-3007, 2018.
[26] W. Fan, Y. Liu, B. Tang, F. Wu and Z. Wang, "Computation Offloading Based on Cooperations of Mobile Edge Computing-Enabled Base Stations," in *IEEE Access*, vol. 6, pp. 22622-22633, 2018.
[27] Z. Zhu *et al*., "Fair Resource Allocation for System Throughput Maximization in Mobile Edge Computing," in *IEEE Access*, vol. 6, pp. 5332-5340, 2018.
[28] P. Bellavista, S. Chessa, L. Foschini, L. Gioia and M. Girolami, "Human-Enabled Edge Computing: Exploiting the Crowd as a Dynamic Extension of Mobile Edge Computing," in *IEEE Communications Magazine*, vol. 56, no. 1, pp. 145-155, Jan. 2018.
[29] A. Kiani and N. Ansari, "Edge Computing Aware NOMA for 5G Networks," in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1299-1306, April 2018.
[30] L. Tang and S. He, "Multi-User Computation Offloading in Mobile Edge Computing: A Behavioral Perspective," in *IEEE Network*, vol. 32, no. 1, pp. 48-53, Jan.-Feb. 2018.
[31] Q. Yuan, H. Zhou, J. Li, Z. Liu, F. Yang and X. S. Shen, "Toward Efficient Content Delivery for Automated Driving Services: An Edge Computing Solution," in *IEEE Network*, vol. 32, no. 1, pp. 80-86, Jan.-Feb. 2018.
[32] M. Marjanović, A. Antonić and I. P. Žarko, "Edge Computing Architecture for Mobile Crowdsensing," in *IEEE Access*, vol. 6, pp. 10662-10674, 2018.
[33 Y. Hao, et al. "Energy Efficient Task Caching and Offloading for Mobile Edge Computing," in IEEE Access, vol. 6, pp. 11365-11373, 2018
[34] P. Verma and S. K. Sood, "Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1789-1796, June 2018.
[35] G. Premsankar, M. Di Francesco and T. Taleb, "Edge Computing for the Internet of Things: A Case Study," in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1275-1284, April 2018.
[36] Y. Hao, et al. “Energy Efficient Task Caching and Offloading for Mobile Edge Computing,” IEEE Access, vol. 6, pp. 11365-11373, 2018
[37] Y. Cao *et al*., "Mobile Edge Computing for Big-Data-Enabled Electric Vehicle Charging," in *IEEE Communications Magazine*, vol. 56, no. 3, pp. 150-156, MARCH 2018.
[38] L. Liu, Z. Chang and X. Guo, "Socially Aware Dynamic Computation Offloading Scheme for Fog Computing System With Energy Harvesting Devices," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1869-1879, June 2018.
[39] Z. Ali et al., “Edge-centric multimodal authentication system using encrypted biometric templates," Future Generation Computer Systems, vol. 85, no. 2018, pp. 76-87, August 2018
[40] H. Ko, J. Lee and S. Pack, "Spatial and Temporal Computation Offloading Decision Algorithm in Edge Cloud-Enabled Heterogeneous Networks," in *IEEE Access*, vol. 6, pp. 18920-18932, 2018.
[41] K. Zhang, S. Leng, Y. He, S. Maharjan and Y. Zhang, "Mobile Edge Computing and Networking for Green and Low-Latency Internet of Things," in *IEEE Communications Magazine*, vol. 56, no. 5, pp. 39-45, May 2018.

[42] Y. Bi, G. Han, C. Lin, Q. Deng, L. Guo and F. Li, "Mobility Support for Fog Computing: An SDN Approach," in *IEEE Communications Magazine*, vol. 56, no. 5, pp. 53-59, May 2018.
[43] M. Li, F. R. Yu, P. Si and Y. Zhang, "Green Machine-to-Machine Communications with Mobile Edge Computing and Wireless Network Virtualization," in *IEEE Communications Magazine*, vol. 56, no. 5, pp. 148-154, May 2018.
[44] 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," in *IEEE Transactions on Industrial Informatics*. doi: 10.1109/TII.2018.2843169
[45] M. A. Rahman and M. S. Hossain, "m-Therapy: A Multisensor Framework for in-Home Therapy Management: A Social Therapy of Things Perspective," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2548-2556, Aug. 2018.
[46] M. A. Rahman, and M. S. Hossain, "A Cloud-based Virtual Caregiver for Elderly People in Cyber Physical IoT Systems", Cluster Computing, Springer Nature, 2017, Online View Available - http://rdcu.be/GtCc
[47] M. A. Rahman, E. Hassanain, M. S. Hossain, "Towards A Secure Mobile Edge Computing Framework for Hajj", IEEE Access, vol. 5, Issue: 99, 16 June 2017.
[48] M. Satyanarayanan, "The Emergence of Edge Computing", IEEE Computer, vol. 50, no. 1, January 2017.
[49] M. Masud et al., "Data Interoperability and Multimedia Content Management in e-Health Systems," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1015-1023, Nov. 2012.
[50] M. S. Hossain et al. "Cloud-assisted secure video transmission and sharing framework for smart cities," Future Generation Computer Systems, vol. 83, no. 2018, pp. 596-607, June 2018.
[51] M. S. Hossain, G. Muhammad, and A. Alamri, "Smart Healthcare Monitoring: A Voice Pathology Detection Paradigm in Smarter Cities" ACM/Springer Multimedia Systems, 2017, DOI: 10.1007/s0053
[52] M. Chen et al."Edge-CoCaCo: Toward Joint Optimization of Computation, Caching, and Communication on Edge Cloud," IEEE Wireless Communications, vol. 25, no. 3, pp. 21-27, JUNE 2018
[53] K. Lin, et al. "Green Video Transmission in the Mobile Cloud Networks," IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 1, pp. 159-169, Jan. 2017.

Md. Abdur Rahman [SM'17] is an Assistant Professor in the Department of Forensic Computing and Cyber Security, University of Prince Muqrin (UPM), Madinah Al Munawwarah, Kingdom of Saudi Arabia. Dr. Md. Abdur Rahman is currently the Chairman of Computer Science (CS) and Forensic Computing and Cyber Security (FCCS) Department of UPM. Dr. Abdur Rahman received his Ph.D. degree in Electrical and Computer Engineering from the University of Ottawa, Canada in 2011. His research interests include serious games, cloud and multimedia for healthcare, IoT, smart city, secure systems, multimedia big data, and next generation media. He has authored and co-authored around 100 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He has 7 US patents and several are pending. Dr. A. Rahman has received more than 12 million SAR as research grant. Dr. A. Rahman has been awarded the best researcher award by the UPM for the year 2018. Recently, he received three best paper awards from ACM and IEEE Conferences. Dr. Abdur Rahman is a member of both IEEE and ACM.

M. Shamim Hossain [SM'09] is a Professor at the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an adjunct professor at the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. He received his Ph.D. in Electrical and Computer Engineering from the University of Ottawa, Canada. His research interests include cloud networking, smart environment (smart city, smart health), social media, IoT, edge computing and multimedia for health care, deep learning approach to multimedia processing, and multimedia big data. He has authored and coauthored approximately 200 publications including refereed journals, conference papers, books, and book chapters. Recently, his publication is recognized as the *ESI Highly Cited Paper*. He has served as a member of the organizing and technical committees of several international conferences and workshops. He has served as cochair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. Currently, he is the cochair of the 2nd IEEE ICME workshop on Multimedia Services and Tools for smart-health (MUST-SH 2019). He is a recipient of a number of awards, including the Best Conference Paper Award and the **2016 *ACM Transactions on Multimedia Computing, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award*** and the Research in Excellence Award from the College of Computer and Information Sciences (CCIS), King Saud University (3 times in a row). He is on the editorial board of *IEEE Network*, *IEEE Multimedia*, *IEEE Wireless Communications*, *IEEE Access*, Journal of Network and Computer Applications (Elsevier), Computers and Electrical Engineering (Elsevier), Human-centric Computing and Information Sciences (Springer), Games for Health Journal, and International Journal of Multimedia Tools and Applications (Springer). He also presently serves as a lead guest editor of IEEE Network, Future Generation Computer Systems (*Elsevier*), and IEEE Access. Previously, he served as a guest editor of *IEEE Communications Magazine*, *IEEE Transactions on Information Technology in Biomedicine* (currently *JBHI*), *IEEE Transactions on Cloud Computing*, International Journal of Multimedia Tools and Applications (*Springer*),

Cluster Computing (*Springer*), Future Generation Computer Systems (*Elsevier*), Computers and Electrical Engineering (*Elsevier*), Sensors (*MDPI*), and International Journal of Distributed Sensor Networks. He is a senior member of both the IEEE, and ACM.

George Loukas is an Associate Professor in Cyber Security at the University of Greenwich. He received his PhD degree in Network Security from Imperial College London. Dr. Loukas currently serves on the editorial boards of Elsevier's Simulation Modelling Theory and Practice, and BCS' The Computer Journal. He is currently the P.I. of three international research projects related to IoT security, as well as founding member of the IEEE working group on IoT and Cultural Heritage. His book *"Cyber-physical attacks: a growing invisible threat"* has been chosen by ACM in the top 10 in the Computing Milieux category of the 2015 annual list of notable books and articles published in computing. Dr. Loukas has authored or co-authored more than 70 publications.

Elham Hassanain is an Assistant Professor in the Department of Forensic Computing and Cyber Security, University of Prince Muqrin (UPM), Madinah Al Munawwarah, Kingdom of Saudi Arabia. Dr. Elham served as the Vice Dean of College of Computer and Information Systems at Umm Al-Qura University. Dr. Elham also served as a member of Saudi Parliament for a duration of 4 years. Currently she is as the Deputy Rector for Academic Affairs of University of Prince Mugrin. Her research interests include e-Health, cloud and multimedia for healthcare, IoT, and smart city. She has publications in refereed IEEE/ACM journals and conferences. Recently, she has been awarded 1 US patent on Vision Therapy. She has served as a member of the organizing and technical committees of several workshops.

Syed Sadiqur Rahman is an Assistant Professor in the Department of Forensic Computing and Cyber Security, University of Prince Muqrin (UPM), Madinah Al Munawwarah, Kingdom of Saudi Arabia. Dr. Rahman received his Ph.D. degree in Computer Science (Cyber Security Group) from the University of Warwick, UK in 2015. Prior to Joining UPM, Dr Rahman has worked in various prestigious universities including University of Oxford, and University of Birmingham in the UK. His research interests include Cyber Security, Information Trustworthiness (particularly generated from Smartphones in the context of Human as a Sensor Scenario) and Open Source Intelligence.

Mohammed F. Alhamid [M'10] Mohammed F. Alhamid is an Assistant Professor at the Software Engineering Department, King Saud University, Riyadh, KSA. Alhamid received his Ph.D. in Computer Science from the University of Ottawa, Canada. His research interests include recommender systems, social media mining, big data, and ambient intelligent environment.

Mohsen Guizani (S'85–M'89–SM'99–F'09) is currently a professor and the ECE Department chair at the University of Idaho. He currently serves on the editorial boards of several international technical journals including IEEE