IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 30, 2018, accepted January 10, 2019, date of publication January 30, 2019, date of current version February 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2896065

Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City

MD. ABDUR RAHMAN[1], (Senior Member, IEEE), MD. MAMUNUR RASHID[2], (Member, IEEE), M. SHAMIM HOSSAIN[3], (Senior Member, IEEE), ELHAM HASSANAIN[1], (Member, IEEE), MOHAMMED F. ALHAMID[3], (Member, IEEE), AND MOHSEN GUIZANI[4], (Fellow, IEEE)

[1]Department of Cyber Security and Forensic Computing, University of Prince Mugrin, Medina 41499, Saudi Arabia
[2]Consumer and Organizational Digital Analytics Research Centre, King's Business School, King's College London, London WC2B 4BG, U.K.
[3]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[4]Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID 83944 1023, USA

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

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

ABSTRACT In this paper, we propose a Blockchain-based infrastructure to support security- and privacy-oriented spatio-temporal smart contract services for the sustainable Internet of Things (IoT)-enabled sharing economy in mega smart cities. The infrastructure leverages cognitive fog nodes at the edge to host and process offloaded geo-tagged multimedia payload and transactions from a mobile edge and IoT nodes, uses AI for processing and extracting significant event information, produces semantic digital analytics, and saves results in Blockchain and decentralized cloud repositories to facilitate sharing economy services. The framework offers a sustainable incentive mechanism, which can potentially support secure smart city services, such as sharing economy, smart contracts, and cyber-physical interaction with Blockchain and IoT. Our unique contribution is justified by detailed system design and implementation of the framework.

INDEX TERMS Sharing economy, cognitive processing at the edge, mobile edge computing, Blockchain, smart city.

I. INTRODUCTION

Current advancements in 5G networks for IoT data, mobile edge computing (MEC), fog computing, cognitive capability at the edge, cognitive machine-to-machine (M2M) connectivity, IoT for cyber-physical systems, decentralized data storage computing through cloudlets, and Blockchain-based decentralized security enable the provision of context-aware, personalized, and intelligent sharing economy services to a massive smart city crowd. Next generation smart cities will face the challenge of the convergence of these advancements wherein a massive amount of data will be generated by the mass crowd [17] and IoT devices on a daily basis. These data must be digested, processed, and responded to in a secure and cognitive manner. After the invention of WWW, the disruptive technologies that have touched almost every aspect of the computing domain include the introduction of decentralized data transactions using Blockchain, IoT, and machine intelligence at the mobile edge. All of them work together to provide smart city sharing economy solutions wherein two entities perform a transaction in a complete decentralized manner without any middle trusted party [1].

With the recent advancements, additional IoT devices with great processing power are used to support sharing economy services. For example, recent medical equipment, such as Computed Tomography (CT) Scan machine, comes with embedded IoT devices, which can process diagnosed data at the edge [2]. Moreover, the MEC layer could incorporate decentralized security mechanisms, such as Blockchain and The Onion Router (Tor), to ensure data security and privacy before the health IoT data are shared with the stakeholders [3]. For example, the Tor network allows disguising the transaction parties' identity by encrypting the traffic and then randomizing the medical equipment terminals so that

The associate editor coordinating the review of this manuscript and approving it for publication was Yin Zhang.

the traffic looks like coming from random nodes on the Tor network [4]. An entity can complete any business activity, perform any financial or business transaction, or securely save the raw IoT or multimedia data without requiring a middleman [5]–[7]. In the context of health IoT-based sharing economy application wherein a patient can perform therapeutic activities at different locations, such as at home or in a medical institution, MEC nodes can support ubiquitous access to the therapeutic services [8].

These solutions will ensure a scalable big data generation, transmission to the remote cloud [32], centralization or decentralization in a smart city. However, data processing and event detection in different scenarios are a daunting task as the amount of data is at a massively large scale [9]. Analyzing such a sheer volume of data and determining the phenomena of interest [10] at the edge and cloud are possible due to the advancement in high speed transaction capability as an overlay on top of existing Blockchain networks, cognitive computing capabilities with Artificial intelligence (AI), with the support of multi-tier machine learning, deep learning, and other types of data science advancements.

For example, Lightning Network (LN) shows promising potential of scalability by supporting a massive number of concurrent transactions and multi-signature wallet, which is a need of smart city sharing economy services. LN network provides the scalability by opening overlay channels between two transaction-parties, and instead of writing each micro sharing economy transaction, the underlying blockchain only stores the summary of the transactions performed within a temporal dimension or upon closing the channel. Another massively scalable framework named IOTA has been designed to support IoT-based sharing economy data sharing services with no fee and improved Winternitz signature based security. On the other hand, AI and Cognitive computing have been successful in automatic reasoning by following predefined work-flows, the big data set to work on, and the output types to deal with. These technologies show the promising prospect of different smart city sharing economy challenges that the world is facing.

Given the industrial revolution of IoT and its business values, sharing economy services are relying increasingly on IoT data. In this study, we address the challenge of bringing intelligent and cognitive processing at the edge wherein the massive amount of IoT data is generated and processed by the MEC nodes, wherein key transactions are anonymized and securely saved at the Blockchain, and wherein multimedia big data are securely saved at the decentralized off-chain solutions for immutable registry. By using our proposed framework, the sharing economy services wherein two parties can securely perform any number of transactions without requiring any trusted third party can leverage the intelligence at the edge to coordinate seamlessly with the IoT data processing framework. This process will help in understanding the need of transaction parties, their historical profiles, and the data saved within the decentralized repositories.

The remainder of the paper is organized as follows. In Section II, we present the related works. In Section III, we describe different sharing economy scenarios. In Section IV, we discuss the design and components of the framework. In Section V, we share our implementation details. In Section VI, we conclude the paper with the summary and future directions.

II. RELATED STUDY

Although considerable work has been conducted in the areas of Blockchain, sharing economy and IoT, the study and use of IoT data and Blockchain in the context of sharing economy services have not been explored much. The next generation of sharing economy services will face the challenge of the convergence of technological advancements wherein a massive amount of data [33] will be generated by the mass crowd [17] and IoT devices on a daily basis. These data must be digested, processed, and responded to in a secure manner. Recent advancements in decentralized data transactions via Blockchain [5], [11], IoT [12], MEC and Fog Computing [2], [7], [30] and 5G device-to-device (D2D) communication capability [27] will allow secure sharing economy services wherein any number of entities within a mass crowd, such as in a smart city, can perform a multiparty transaction in a decentralized manner [6], [7], [24], [25]. For example, recent medical equipment, such as CT Scan machine, has embedded IoT devices that enable data processing locally and upload the results to Blockchain and off-chain nodes running at the nearby edge [3], [7], [9], [22], [24], [28], [31]. Two parties can securely perform any online activity or financial or business transaction [3], [13], [26], [37]. In the context of a sharing economy application [1], a person can perform health checkups on demand in different mobile edge locations, thereby providing ubiquitous sharing economy service access of health data [10], [13], [18], [19], [25], [26], [29], [38].

However, data processing and event detection in different scenarios of a mass crowd are daunting tasks as the amount of data is at a massive scale [17]. Analyzing massive volumes of data and finding the phenomena of interest are possible through the advancement in AI, with the support of multitier machine learning, deep learning and other types of data science advancements [10].

Building trust through transparent and accurate data transactions and contract agreements is key in a sharing economy service [6]. This case requires developing a framework wherein parties can trust a shared record of events, related to sharing economy policies, despite not knowing each other [21]. The advantage of Blockchain is that it has the potential to eliminate faults and errors as well as detect fraudulent activity associated with falsified IoT data [4], [5], [10]–[12], [19]–[21].

Sharing economy can leverage numerous dimensions of the proposed research. In the context of transportation services, Blockchain can store the driver and car profile with the history of maintenance, accident, transfer, and other types of immutable data [23], [25], [26]. In addition, it can also

connect the stakeholders of a car through a shared chain, providing help in car sharing economy scenario [11].

Blockchain and medical IoT have the potential to interconnect all the communities of interest of ad-hoc health-based sharing economy social media services [34]. For example, they will allow the electronic health record (EHR), electronic medical record (EMR), user profile, health insurance profile, individual medical test history, details of visits to different hospitals, and profiles of physicians and hospitals to be saved in a decentralized and secure repository [13].

One of the major problems faced by the sharing economy is the unique identity management and verification of each stakeholder in a secure and anonymous way [25]. Blockchain offers a promising solution by providing secure identity management; validation of IoT device profiles, user profiles, and other public profiles; and digital signatures, thereby allowing global identity for sharing economy scenarios [14], [19], [35], [36]. Blockchain's smart contracts can automate self-executing agreements that were largely theoretical before the introduction of Blockchain [15].

Although considerable work has been conducted, this study is first to support sharing economy services with the aid of cognitive computing and secure blockchain- and off-chain-based decentralized data storage for a massive crowd. In the next section, we provide the key terminologies and preliminary knowledge areas related to the study.

III. COGNITIVE COMPUTING, BLOCKCHAIN, AND SHARING ECONOMY PRELIMINARIES AND CHALLENGES

Cognitive computing is based on the human thought processes, and it imparts this intelligence to different computerized systems. Cognitive computing is composed of automatic machine learning techniques that use data analytics, pattern recognition, and natural language processing to think like humans. When trained, these systems do not require human assistance. The cognitive engine is similar to powerful brains that drive the distributed IoT devices. This new brain can scan through vast data resources and build intelligence that is required for decision-making and future initiatives. These cognitive engines possess powerful analytics capability and data processing power that imparts human like intelligence into Blockchain frameworks.

A cognitive engine has different models for analytics and prediction tasks and is authorized to record and check changes in physical, functional, and operational properties of the IoT sensors and devices. This affirmation operation is performed in the Blockchain ledger. The cognitive engine and IoT devices also have private key hashing between them, which will help in validate and identify changes. Hence, the cognitive engines will enhance security and integrity of data from IoT devices.

Numerous companies have already combined Blockchain and cognitive computing to build advanced AI platforms, such as IBM Watson. At present, most of the big data collected by the IoT devices, which are previously unused, have become disruptive. Such data provide significant insights that are being converted into actionable intelligence.

In the coming years, the number of IoT devices worldwide could reach 30 billion. No other option to manage and process such huge number of IoT devices and their data in a secure manner unless we leverage the integration of cognitive computing and Blockchain. Hence, such an integration could help build intelligent and independent systems in which data can be harmoniously utilized with enhanced security and reduced wastage.

Several financial institutions have already switched to this technology to provide streamlined and secure transactions give their customers. The users are paid in real time and Blockchain provides unprecedented security to all the stakeholders. The blockchain ledgers are distributed and made transparent, whereas the cognitive systems use the user data and responds to the requests in real time.

Thus, in automated Blockchain-based sharing economy services, the financial transactions and services are automated and intelligently managed by the cognitive engine. The stakeholders participate in trusted operations in which the agreement is studied by the cognitive system, and the obligations are executed automatically without human involvement. Such smart agreement or contract is composed of secure codes, which deals with other similar smart contracts. Such a system can make intelligent decision, perform data analytics, and use Radio-Frequency IDentification (RFID), Near-field communication (NFC), or location information for IoT devices to transmit their data to distributed shared Blockchain ledgers. AI agents are available to manage such autonomous systems with distributed IoT devices. Thus, Blockchain-based sharing economy services and AI agents make business sharing by using smart contracts.

A Blockchain system [18] has the potential to facilitate and coordinate M2M communications among IoT devices and user's mobile devices, which can increase data correctness. As Blockchain is a decentralized digital repository managed by a network of globally distributed computers that independently perform the task of authenticating, validating, and relaying each transaction within the network, it provides a credible architecture to the sharing economy for quickly differentiating a valid data transaction from a duplicate data transaction, or a data transaction involving suspicious activity. Recent advancement in managing the scalability of the Blockchain network has allowed the new generation of Blockchain frameworks to handle a large number of transactions per second. Scalability is no longer a major concern when applying the technology to an IoT platform, wherein the data collected by connected devices and objects will exponentially increase the number of M2M transactions. Several solutions have been proposed to address the current network inefficiencies, including Lightning Network (LN), and scalable distributed ledger architecture IOTA. We define some sharing economy scenarios that will be considered in this literature.

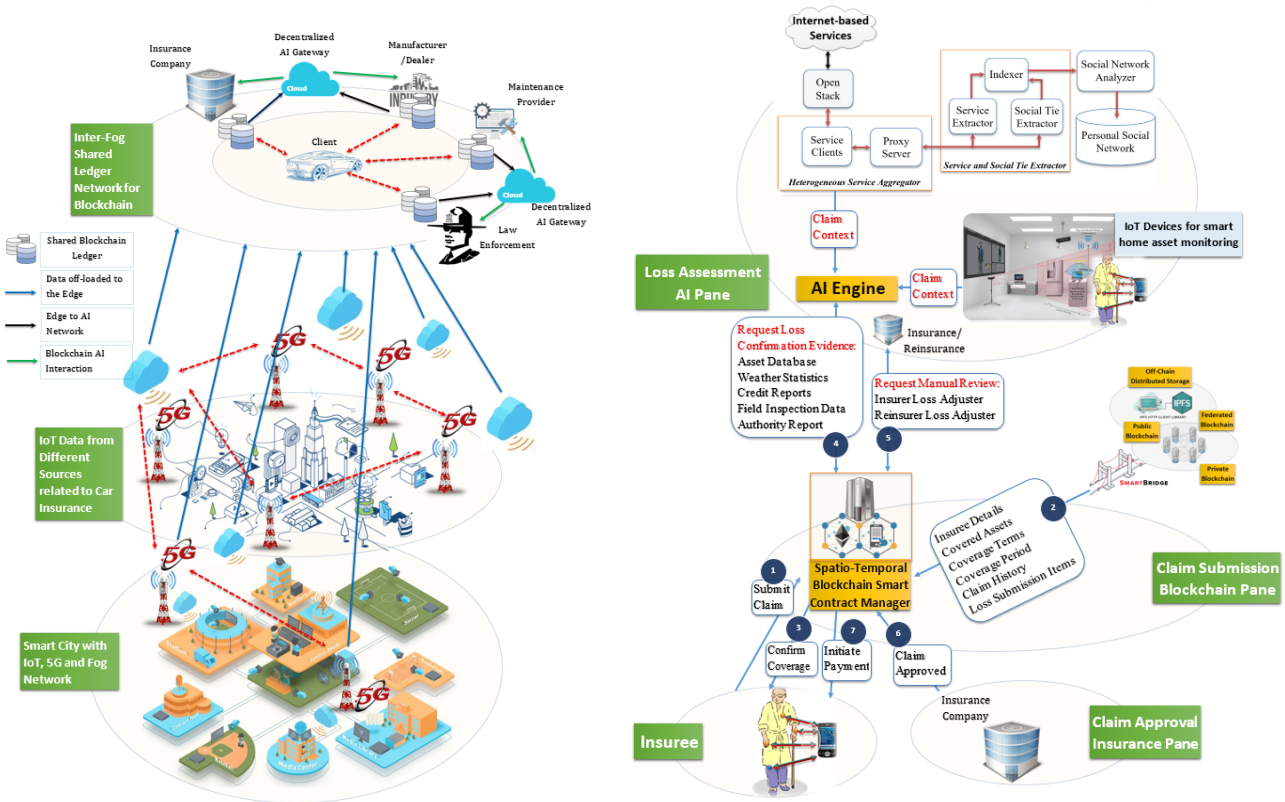


FIGURE 1. Sharing economy scenarios (Left) on demand car rental, and (Right) on demand insurance claim process.

• Transportation Services: Blockchain can store the driver and the car profile with the history of maintenance, accident, transfer and other types of immutable data. Blockchain can also connect the stakeholders of a car through a shared chain and provide help in car sharing economy scenarios. Moreover, the shared ledger can help any ad-hoc query about the car, or the insurance claim can be automated and processed quickly with the help of smart contracts. Figure 1 (a) shows a car rental scenario where IoT, On-board diagnostics (OBD), and other car-rental related data are sent to the nearby mobile edge node, which uses Blockchain and off-chain network to store and then share key information with AI network and other car stakeholders [11].

• Insurance Services: Figure 1(b) shows a sharing economy scenario where Blockchain has been at the center of secure data sharing. Any claim process can be catered by incorporating medical facilities, government agencies, smart contracts, and IoT data with the assistance of AI and would allow automatic payouts to different beneficiaries [12].

• Health Services: Blockchain and medical IoT have the potential to interconnect all the communities of interest of ad-hoc health-based sharing economy services. For example, they will allow the EHR, EMR, user profile, health insurance profile, individual medical test history of each patient, details about the visit to different hospitals, the profile of physicians and hospitals to be saved in a decentralized and secure repository. As shown in Figure 1(b), the sharing economy in health services can be secured and can go across the boundary through the Blockchain of IoT-health data [13].

• Identity Management Services: One of the major problems faced by the sharing economy is unique identity management and verification in a secure and anonymous way. Blockchain shows a promising solution as it can provide secure identity management, validation of user and other public profiles, and digital signatures, thereby allowing global identity for sharing economy scenarios [14].

• Decentralized On- and Off-Chain Storage Services: Sharing economy services require an immutable history of constantly available data. To support such data guarantee, Blockchain allows a short amount of data to be saved in blocks as a secure chain. Recent advancements in decentralized big data repository, such as InterPlanetary File System (IPFS), allows spatio-temporal multimedia big data to be saved into a decentralized storage. Raw data stored in such big data repository can be linked with a sharing economy transaction stored in a blockchain via file hashes.

• Smart Contract Services: Blockchain's smart contracts can automate location-aware agreement logic [15]. For instance, a health insurance smart contract could automatically incorporate the policy, coverage, and evidence available from health IoT devices.

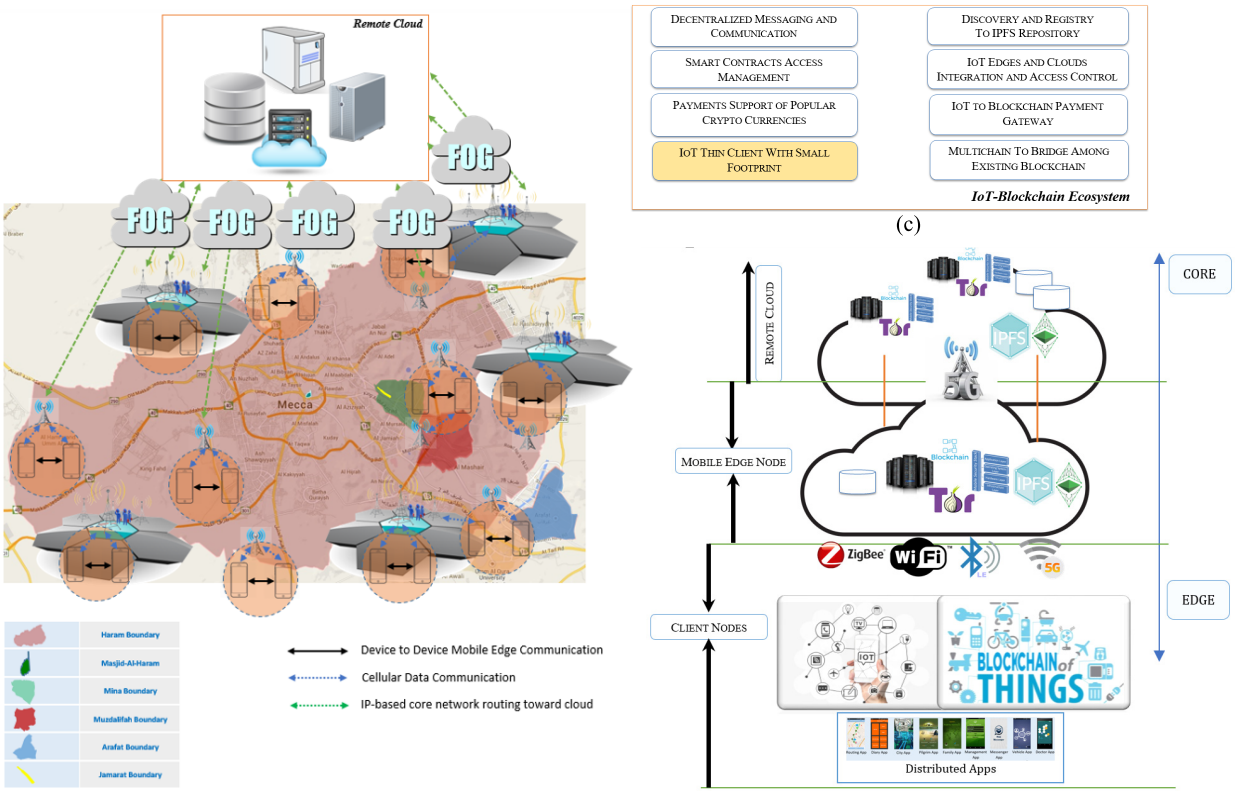


FIGURE 2. (a) Boundary model showing 5G-based D2D communication paradigm using Fog, (b) Three-tier protocol architecture, and (c) protocol stack of collecting, analyzing and visualizing IoT data.

IV. SYSTEM DESIGN

With the release of a large amount of big data from diversified domains, continuously collecting, analyzing, and utilizing such data to autonomously predict, alert, and prevent risky transactions and proactively warn about an event that might occur help in shaping the design of next generation sharing economy services. Figure 2 shows our envisioned sharing economy infrastructure that can manage transactions of a mass crowd. We assume the city has deployed 5G cell towers (see Figure 2(a)) with licensed spectrum for D2D communication and onsite fog nodes for running Blockchain and off-chain operations. Figure 2(b) illustrates a three-tier architecture for supporting scalable sharing economy services in a smart city. Client tier consists of smartphone applications, IoT nodes, and infrastructure associated with the sharing economy services. The client nodes communicate with the mobile edge tier through different communication means, such as Wi-Fi, Bluetooth Low Energy (BLE), Zigbee or 5G. The MEC tier is envisioned to host Blockchain nodes, decentralized data repository client, Tor clients, and other legacy databases and cloudlet applications. The MEC tier is responsible for synchronizing the load with the backend cloud tier, depending on the load experienced by the MEC tier. Figure 2(c) shows the protocol stack of collecting, analyzing, and visualizing IoT data. As IoT devices are thin, we assume that they only has a limited capacity of connecting with edge devices running full Blockchain nodes. The framework allows an IoT node to communicate with nearby edge nodes running smart contract, to use decentralized messaging services, to save raw IoT sensory data into a decentralized repository via edge networks, to add IoT data of interest to the Blockchain, and to connect to cryptocurrency exchanges and gateways.

Data from the IoT, Blockchain, and other social network domains are fed to the AI engine for emotion extraction, digital forensics, and finding patterns of interest for various sharing economy services.

A. SEMANTIC WEB DATA EXTRACTOR

Figure 3 shows the modules that are responsible for collecting raw contents from heterogeneous Internet-based sources, Blockchain, off-chain, and IoT devices. The framework uses a restful architecture to connect third party APIs securely and extracts sharing economy related profiles and sources for preprocessing, caching, and indexing. This information serves as the AI dataset of a particular sharing economy scenario.

B. INTELLIGENT SHARING ECONOMY EMOTION EXTRACTOR

This component preprocesses, analyzes multimedia big data or Blockchain and off-chain data, extracts semantic values, indexes the semantic primitives, presents the results to the

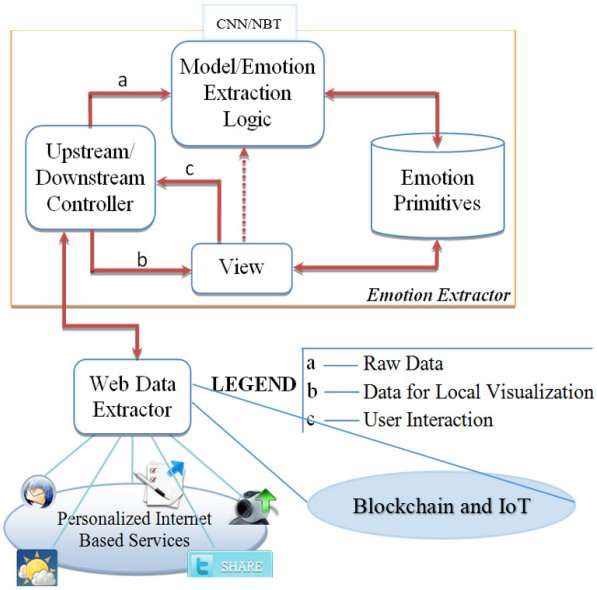


FIGURE 3. Blockchain-based AI assistance framework.

user, and adapts the emotion value to train the system using a Deep Neural Networks model called Convolutional Neural Networks (CNN) or Naïve Bayes Theorem (NBT), depending on the need. Semantic knowledge representation is done by the machine-learning algorithm through clustering, classification, and regression analysis of the extracted features after raw data cleaning, transformation, and reduction [16].

Primitives regarding sharing economy such as indexed smart contract term details (for example, smart hotel, driver less car renting, on demand doctor, on demand hospital etc.) are handled by emotion extraction logic. Dedicated APIs are developed for different primitives' logic, each of which uses the model primitives as a training dataset and uses it as input to the smart contract logic. Over time, the more the dataset gets enriched, the better the outcome results. It implements the intelligent data processing through the following three steps.

1) TRAINING

In this mode, the system tries to classify the newly arrived content into positive, negative or neutral logic by applying a supervised learning method. The posterior probability of sentiment membership is leveraged for labelling and the new input sample is mapped in accordance with sharing economy features.

2) EXECUTION

As shown in Figures 1 and 5, when the AI engine receives new spatiotemporal multimedia content, such as IoT, social network, crowdsourced or Blockchain data, it first analyzes the data before classification. The proposed algorithm can classify sharing economy data against the training data set even with the possibility of noises in the trained data.

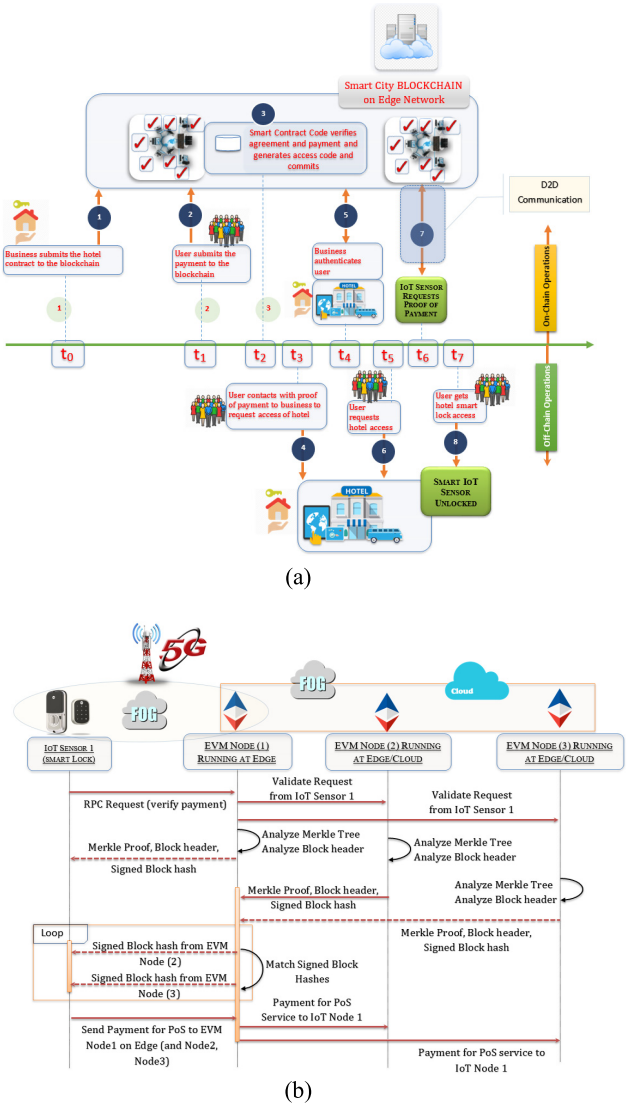


FIGURE 4. (a) A scenario where a user books a hotel with the help of Blockchain and IoT devices (b) the detailed machine to machine communication among different Blockchain nodes to commit the transactions.

3) FEEDBACK PHASE

Although the system has the provision of leveraging and auto-reasoning sharing economy dataset using DNN and CNN, it supports NBT to leverage the human intelligence and keep users' feedback within the loop.

As shown in Figures 1 and 5, the sharing economy requires an intelligent bot that can understand the logic of different business model, accordingly prepare the data, and provide the necessary machine intelligence to the parties for enhanced visualization. The system uses different augmented, virtual and mixed reality visualization metaphors to search the Blockchain and off-chain data of interest.

Design of a Sharing Economy Service (Cyber Physical Blockchain and IoT-Based Smart Hotel Booking in a Smart City): Figure 4(a) shows a scenario in which a user rents a

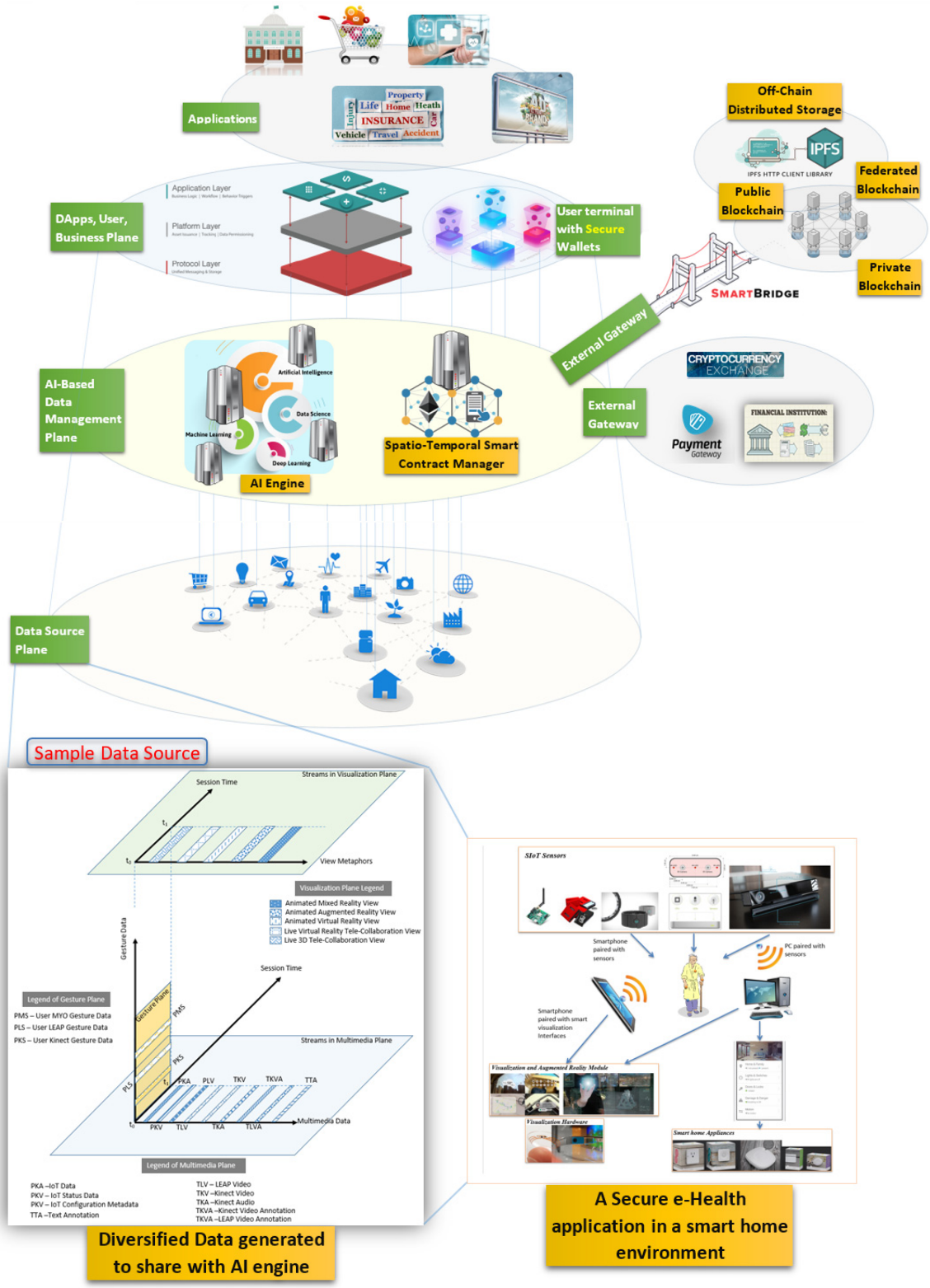


FIGURE 5. A complete smart home scenario where different types of data that needs to be recorded in the Blockchain and used in a sharing economy service.

hotel using cyber-physical interaction between Blockchain and IoT devices. Figure 4(b) represents the interaction between the smart lock and the rest of the Blockchain clients to handle the complete D2D contractual agreements successfully and securely. The IoT smart lock cannot store the complete Blockchain record and cannot run the complete

Ethereum Virtual Machine (EVM) due to its storage and processing limitations. Hence, the smart lock has to rely on a set of miners for proof of payment and smart contract logic execution operating within edge or in a decentralized cloud. The smart lock will use the proof of payment from which it has also to pay to the miner nodes that calculated the hash as proof of payment from the complete Blockchain.

As shown in Figure 4(a), at time t_0, a property owner publishes the smart contract to the Blockchain with the spatiotemporal terms and condition of the rent. A user searches the Blockchain and agrees to the smart contract and provides the payment from his/her digital wallet at t_1. The smart contract verifies the payment and commits to the Blockchain at time t_2; however, the payment will be on hold until the IoT-based smart lock of the property of interest is activated.

Upon payment written in the block, the potential renter contacts the property owner at time t_4, which is verified by the business through a query to the Blockchain at time t_5. When verified at time t_6, the owner issues an IoT-based smart lock access card to the renter at time t7. Upon receiving the access card, the renter can now punch it to open the IoT-based smart lock at time t_8. As the smart lock has limited capability, it communicates through an incentive-based consensus protocol running within the MEC node in a decentralized manner, as explained in Figure 4(b). Similarly, other types of sharing economy scenarios are designed for automatic execution and maintaining cyber physical interactions for a mass crowd.

V. SYSTEM DEPLOYMENT AND IMPLEMENTATION

To best represent the sharing economy by leveraging the developments in the abovementioned areas, we assume Hajj, which attracts an ad-hoc massive crowd, wherein each individual has to perform diversified sharing economy activities at a certain day and time [3]. Since there is no single central authority to govern any particular pilgrim, each pilgrim has to create numerous contracts in advance with a subset of agencies prior to the pilgrimage, which includes payment for residence, insurance, airlines, internal transportation, food, and health. The most challenging issue is that pilgrims worldwide have to sign the contract on numerous sharing economy services while they are in their respective countries.

The sharing economy has to deal with both inter- and intra-user sharing economy contracts spatiotemporally while the pilgrims arrive in the event location. Hence, the infrastructure has to deal with smart contracts among numerous parties within the mass crowd, by respecting a large number of on- and off-chain sharing economy smart contracts and transactions [15]. Remembering such a large volume of contract states for a massive crowd is a daunting task. With the AI and deep learning advancements, AI can work on a large number of sharing economy scenarios and help in digital analytics for different stakeholders. In this manuscript, we present the design and implementation of different sharing economy scenarios that leverage Blockchain/off-chain solutions, MEC, and AI.

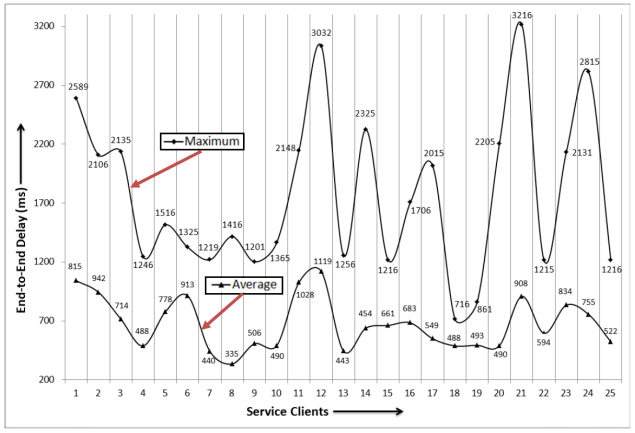
We develop a proof of concept system comprising of smartphone applications to collect data about sharing economy services, and private Blockchain. Figure 5 shows a scenario in which data collected from the smart home IoT sensors are shared with both Blockchain and decentralized repository for assisting the AI engine in the claim or other types of sharing economy related evidence. The multidimensional data types originated from the smart home can be those sensing ambiance, user activity, energy usage, different security aspects, and human physiological data, to name a few. These data are fed to the AI engine for event analysis, event indexing in the Blockchain, and saving the payload in the off-chain solutions or inquiring other Blockchain bridges, if deemed necessary, and alert generation for different high-level threshold values of particular sensory data. The smart contract can also interface with the external cryptocurrency gateway and exchange in case of payment for any third party services. Finally, the house owner can share the results of smart home data with a subset of his online service providers. The services use distributed apps to connect to the decentralized databases.

We deploy several permissioned private Blockchain nodes at the mobile edge, which will commit the sharing economy services. To achieve scalability and a large number of sharing economy transactions per minute, the framework relies on the consensus in a set of trusted nodes. The sharing economy logic and conditions and the IoT node access policies and subsequent data flow are executed by smart contract logic. The IoT raw data related to sharing economy services are captured and subsequently processed by the MEC node, and the key and salient transaction data, which must be digested for permanent storage, are stored in the Blockchain. A sample sharing economy transaction uses the following parameters:

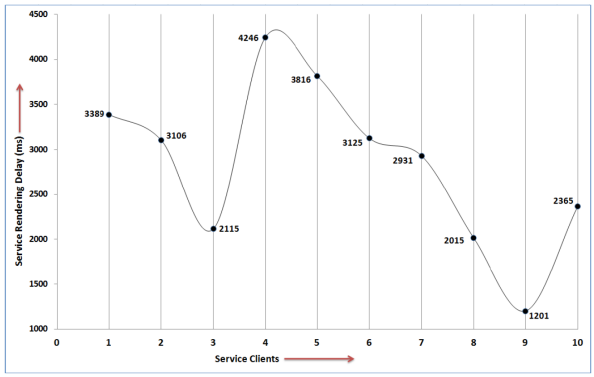
{ChainID, TxNonce, From-To-Value-Data, TxDependsOn, BlockRef, BlockExpiration, gasPriceFactor, senderMaxGasValue, SignatureTxBody}

We have used Amazon AWS platform to instantiate 100 nodes of different types, including SPV and full nodes. Each P2P node is configured to run within a Linux Virtual Machine. The testing environment was set up to test the IoT security, other functionality, terminals using Mobile Distributed Apps, distributed IPFS-based cloud repositories, Blockchain nodes, effectiveness of smart contracts, and different designed APIs. 4 bands of writing test was performed: 10,000 transactions, 50,000 transactions, 100,000 transactions and 1,000,000 transactions. During each transaction, the RAM used, time taken to complete the transaction, maximum transaction per block, average transaction count per block, disk usage, number of crashes, and average block creation time were noted down.

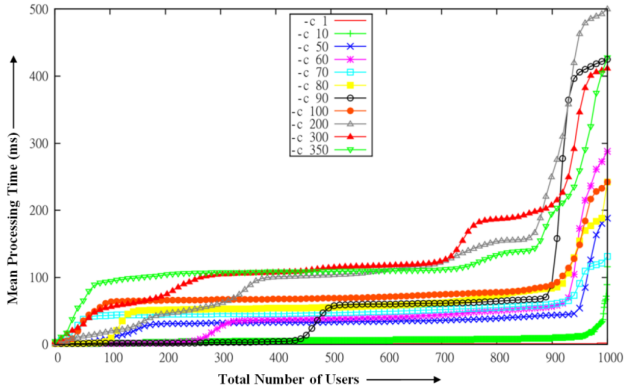
Each IoT device, which needs to be added to the framework is represented by a 24 bytes ID, which is hashed using SHA-256 algorithm. Each IoT device is assigned a public key to share data with outside world and a private key for secure signature. The hash value can then be written into a tag in the form of QR code or an NFC or an RFID. Each sharing economy service can associate each IoT device with



(a)



(b)



(c)

FIGURE 6. Measurement in accessing sharing economy services via the edge network.

the transaction parties' private and public keys. A unique hash generated and then stored in the Blockchain can be inquired by a RESTful service.

We leverage permissioned, private Ethereum and Hyperledger Blockchain along with IPFS as off-chain distributed big data storage. Figure 6 shows the round trip delay in realizing the sharing economy data, which is added to the Blockchain, then saved to the distributed repository at the edge network, and finally processed by the cognitive engine. Measuring the delay in accessing a particular sharing economy service is performed as follows:

TABLE 1. Average end-to-end delay between a client IoT node and decentralized cloud.

IoT Sensor	#Requests	#Successful Query Response	Success Ratio	Average Delay (ms)
Luxometer	1000	989	98.9	1350
Humidity	1109	1109	100	1559
Invasive Temperature	1097	1093	99.6	1551
IR-based non-invasive Temperature	1020	1017	99.7	1449
Barometer	936	933	99.7	2167
Motion	1381	1379	99.9	2671
Gas	1002	1000	99.8	1995
Dust	1343	1343	100	3032
Pressure	1049	1047	99.8	2815
UV	1419	1410	99.4	1706
Flame	409	408	99.8	1665
Air Quality	2006	2005	99.9	2873
Noise	2145	2138	99.7	1943

Round Trip Delay of Extracting Content from a Sharing Economy Service = (*The delay in initializing the appropriate service client + instantiating appropriate protocol + handshaking with the 3rd party service provider + accessing and parsing the appropriate content extraction API + storing the results in the indexer*)

Figure 6(a) shows the maximum end-to-end delay of accessing 25 sharing economy services, with a sample size of 2000. Figure 6(b) presents an instance of delay of rendering 10 different sharing economy services. A typical instance shown in the figure portrays that all the services were dynamically derived within approximately 5 seconds. Run time test results presented above only considers that an individual user is interacting with the framework at any given moment. Figure 6(c) displays the mean processing time for different numbers of concurrent users when each group one particular type of sharing economy service. This does not include the delay in accessing other contents.

We have used RESTful architecture to read/write IoT data to the framework. For example, writing Gas sensor's instantaneous and the raw data to the block and IPFS can be initiated by the following HTTPS POST and PUT methods, respectively. Similar RESTful access API is designed for other types of primitive IoT devices. Table 1 shows different primitive IoT sensory data that have been tested within this framework, depending on the type of sensing requirements. The sensory data are first processed within the nearby MEC node, processed within MEC node API in decentralized fashion, and then sent to decentralized cloud API for raw data storage. As shown in the Table 1 and Figure 7, in one the testing period, various RESTful requests have been made to the MEC node and the response received. Total successful response is recorded during these testing phase along with

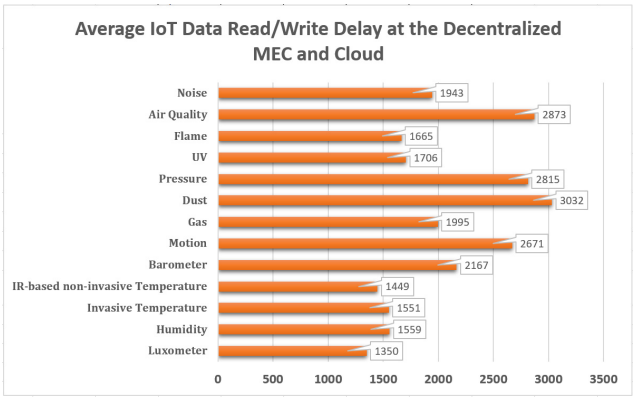


FIGURE 7. IoT data read/write delay for a sharing economy service via the edge network.

average delay time. The average delay is found to be within the tolerable range, considering that the Blockchain and IPFS read/write processing is relatively variable due to consensus mechanism. Hence, the framework shows promising results to be used for sharing economy services of IoT devices.

https://abc.com/madinah/MEC1/sensors/gas/blockchain/write

https://abc.com/madinah/MEC1/sensors/gas/IPFS/write

VI. CONCLUSION

In this paper, we have proposed an MEC-based sharing economy system, which leverages the Blockchain and off-chain framework to store immutable ledgers. With the support of our proposed AI infrastructure, a future generation smart city can offer cyber-physical sharing economy services through IoT data. By using smart contracts, the framework can offer complex spatio-temporal services to a global level without requiring a central verification authority. We envision to test different sharing economy scenarios at a large scale during Hajj 2019 and Hajj 2020.

REFERENCES

[1] M. Möhlmann, "Collaborative consumption: Determinants of satisfaction and the likelihood of using a sharing economy option again," *J. Consum. Behav.*, vol. 14, no. 3, pp. 193–207, May/Jun. 2015.

[2] M. A. Rahman, M. S. Hossain, E. Hassanain, and G. Muhammad, "Semantic multimedia fog computing and IoT environment: Sustainability perspective," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 80–87, May 2018.

[3] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards a secure mobile edge computing framework for Hajj," *IEEE Access*, vol. 5, pp. 11768–11781, 2017.

[4] N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.

[5] M. S. Hossain, *et al.*, "Cloud-assisted secure video transmission and sharing framework for smart cities," *Future Gener. Comput. Syst.*, vol. 83, no. 2018, pp. 596–606, 2018.

[6] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Netw.*, vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.

[7] Q.-V. Pham, T. Leanh, N. H. Tran, B. J. Park, and C. S. Hong, "Decentralized computation offloading and resource allocation for mobile-edge computing: A matching game approach," *IEEE Access*, vol. 6, pp. 75868–75885, 2018.

[8] 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 Things J.*, vol. 5, no. 4, pp. 2548–2556, Aug. 2018.

[9] T. Zhang, "Data offloading in mobile edge computing: A coalition and pricing based approach," *IEEE Access*, vol. 6, pp. 2760–2767, 2017.

[10] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Nov. 2017.

[11] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[12] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[13] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, Jul. 2017.

[14] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017.

[15] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8386853, doi: 10.1109/JIOT.2018.2847705.

[16] S. Pouyanfar, Y. Yang, S.-C. Chen, M.-L. Shyu, and S. S. Iyengar, "Multimedia big data analytics: A survey," *ACM Comput. Surv.*, vol. 51, no. 1, p. 10, Jan. 2018. doi: 10.1145/3150226.

[17] M. A. Rahman and M. S. Hossain, "'A location-based mobile crowdsensing framework supporting a massive ad hoc social network environment," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 76–85, Mar. 2017. doi: 10.1109/MCOM.2017.1600725CM.

[18] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *Proc. IEEE 13th Int. Symp. Auton. Decentralized Syst. (ISADS)*, Bangkok, Thailand, Mar. 2017, pp. 229–234.

[19] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for eHealth data access management," in *Proc. 4th Int. Conf. Adv. Biomed. Eng. (ICABME)*, Beirut, Lebanon, Oct. 2017, pp. 1–4.

[20] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[21] 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. 14757–14767, 2017.

[22] M. Chen, Y. Hao, L. Hu, M. S. Hossain, and A. Ghoneim, "Edge-CoCaCo: Toward joint optimization of computation, caching, and communication on edge cloud," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 21–27, Jun. 2018.

[23] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. Int. Smart Cities Conf. (ISC2)*, Wuxi, China, Sep. 2017, pp. 1–4.

[24] 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," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[25] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in *Proc. IEEE 19th Int. Conf. E-Health Netw., Appl. Services (Healthcom)*, Dalian, China, Oct. 2017, pp. 1–4.

[26] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[27] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 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," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 145–155, Jan. 2018.

[29] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Gener. Comput. Syst.*, vol. 91, pp. 563–573, Feb. 2019.

[30] L. Liu, Z. Chang, X. Guo, S. Mao, and T. Ristaniemi, "Multiobjective optimization for computation offloading in fog computing," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 283–294, Feb. 2018.

[31] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Gener. Comput. Syst.*, vol. 85, pp. 76–87, Aug. 2018.
[32] K. Lin, J. Song, J. Luo, W. Ji, M. S. Hossain, and A. Ghoneim, "Green video transmission in the mobile cloud networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 1, pp. 159–169, Jan. 2017.
[33] 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 Gener. Comput. Syst.*, vol. 88, pp. 333–341, Nov. 2018.
[34] Q. Fang, J. Sang, C. Xu, and M. S. Hossain, "Relational user attribute inference in social media," *IEEE Trans. Multimedia*, vol. 17, no. 7, pp. 1031–1044, Jul. 2015.
[35] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61876–61885, 2018. doi: 10.1109/ACCESS.2018.2875242.
[36] M. A. Rahman *et al.*, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018. doi: 10.1109/ACCESS.2018.2881246.
[37] M. F. Alhamid, M. Rawashdeh, H. Al Osman, M. S. Hossain, and A. El Saddik, "Towards context-sensitive collaborative media recommender system," *Multimedia Tools Appl.*, vol. 74, no. 24, pp. 11399–11428, Dec. 2015.
[38] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

MD. ABDUR RAHMAN (M'–SM'17) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada, in 2011. He is currently an Assistant Professor with the Department of Forensic Computing and Cyber Security, University of Prince Muqrin (UPM), Medina, Saudi Arabia, and also the Chairman of Computer Science and Forensic Computing and Cyber Security Department. He has authored and co-authored around 100 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He has seven U.S. patents and several are pending. He has received more than 12 million SAR as research grant. His research interests include serious games, cloud and multimedia for healthcare, the IoT, smart city, secure systems, multimedia big data, and next generation media. He is a member of IEEE and ACM. He was a recipient of the Best Researcher Award by the UPM, in 2018. He was also a recipient of three best paper awards from ACM and IEEE Conferences.

MD. MAMUNUR RASHID received the Ph.D. degree from the University of Cranfield. He received the Ph.D. Scholarship to work at the European Organisation for Nuclear Research (CERN), Switzerland. He was with the Physics Department, Imperial College London. He was a Scientific Research Computing Specialist with the Department of Engineering Science, University of Oxford. He is currently a Senior Research Fellow with the King's Business School, King's College London. He is also working in a leading Digital Analytics Centre called Consumer and Organizational Digital Analytics Research Centre. He also works on solving the diverse set of problems for finding impacts of state-of-the-technology in the IoT, big data, blockchain, pattern recognition, smart infrastructure, future cities, and distributed HPC. Alongside his current position, he is also involved in a number of international multidisciplinary collaborative research activities. In his research career, he has successfully secured a number of scientific research and travel grants from the Natural Environment Research Council and Newton Fund (British Council) with Brazil, Thailand, Turkey, Peru, China, Bangladesh, Kazakhstan, Azerbaijan, Dubai, Vietnam, and Azerbaijan. His research interests include multi-disciplinary research spectrums focusing on a force for innovation, scientific discovery, and potentially those can make a worldwide impact.

M. SHAMIM HOSSAIN (SM'09) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada. He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. He has authored and co-authored approximately 200 publications including refereed journals, conference papers, books, and book chapters. Recently, his publication is recognized as the ESI Highly Cited Paper. His research interests include cloud networking, smart environment (smart city, smart health), social media, the IoT, edge computing and multimedia for health care, deep learning approach to multimedia processing, and multimedia big data. He has served as a member of the organizing and technical committees of several international conferences and workshops. He is a Senior Member of the IEEE and ACM. He was 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, King Saud University, (3 times in a row). He has served as a co-chair, a general chair, a workshop chair, a publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. He is currently the Co-Chair of the 2nd IEEE ICME Workshop on Multimedia Services and Tools for Smart-Health, in 2019. He is on the Editorial Board of the IEEE TRANSACTIONS ON MULTIMEDIA, the IEEE NETWORK, the IEEE MULTIMEDIA, the IEEE WIRELESS COMMUNICATIONS, the IEEE ACCESS, the *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *Human-Centric Computing and Information Sciences* (Springer), *Games for Health Journal*, and the *International Journal of Multimedia Tools and Applications* (Springer). He served as a Guest Editor of the *IEEE Communications Magazine*, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), the IEEE TRANSACTIONS ON CLOUD COMPUTING, the *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *Sensors* (MDPI), and the *International Journal of Distributed Sensor Networks*. He also presently serves as a Lead Guest Editor of the IEEE NETWORK, *Future Generation Computer Systems* (Elsevier), and the IEEE ACCESS.

ELHAM HASSANAIN served as the Vice Dean of the College of Computer and Information Systems, Umm Al-Qura University. She is currently an Assistant Professor with the Department of Forensic Computing and Cyber Security, University of Prince Muqrin (UPM), Medina, Saudi Arabia. She is also the Deputy Rector for Academic Affairs of UPM. She also served as a member of Saudi Parliament for the duration of 4 years. She has publications in refereed IEEE/ACM journals and conferences. Recently, she received 1 U.S. patent on vision therapy. Her research interests include e-health, cloud and multimedia for healthcare, the IoT, and smart city. She has served as a member of the organizing and technical committees of several workshops.

MOHAMMED F. ALHAMID (M'10) received the Ph.D. degree in computer science from the University of Ottawa, Canada. He is currently an Assistant Professor with the Software Engineering Department, King Saud University, Riyadh, Saudi Arabia. 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 with the University of Idaho. He has authored nine books and more than 400 publications in refereed journals and conferences. He also served as a member, a chair, and the general chair of a number of international conferences. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He guest edited a number of special issues in IEEE journals and magazines. He currently serves on the Editorial Boards of several international technical journals, including the *IEEE Wireless Magazine*, Editor-in-Chief of the *IEEE Network Magazine*, and the Founder and the Editor-in-Chief of *Wireless Communications and Mobile Computing* journal (Wiley). He is on the Advisory board of the IEEE INTERNET OF THINGS JOURNAL. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005.