Blockchain and IoT-based Secure Multimedia Retrieval System for a Massive Crowd: Sharing Economy Perspective

Md. Abdur Rahman
Cyber Security and Forensic Computing Department,
University of Prince Mugrin,
Madinah, KSA
m.arahman@upm.edu.sa

George Loukas
Computing and Mathematical Sciences, University of Greenwich, London, UK
G.Loukas@greenwich.ac.uk

Syed Maruf Abdullah
Smart City Research Laboratory, University of Prince Mugrin, Madinah, KSA
s.maruf@mysmartciti.com

Areej Abdu
Smart City Research Laboratory, University of Prince Mugrin, Madinah, KSA
a.abdu@ mysmartciti.com

Syed Sadiqur Rahman
Cyber Security and Forensic Computing Department,
University of Prince Mugrin,
Madinah, KSA
s.sadiq@upm.edu.sa

Elham Hassanain
Cyber Security and Forensic Computing Department,
University of Prince Mugrin,
Madinah, KSA
e.hassanain@upm.edu.sa

Yasmine Arafa
Computing and Mathematical Sciences, University of Greenwich, London, UK
Y.Arafa@greenwich.ac.uk

ABSTRACT

Blockchain's properties in addressing trust in highly decentralized environments can make it an enabler for novel sharing economy services. In this paper, we demonstrate the practicality of blockchain-based Secure IoT as a Service (SIoTaaS), where an IoT device can be rented from a service provider, securely and in a privacy-preserving fashion. Our framework allows the simultaneous operations of distinct providers of IoT-based sharing economy services at a large scale. Multiple parties can securely share text and multimedia in the context of location and point-of-interest sharing, perform financial transactions by hiding true identity of parties involved in various online transactions, perform user and IoT registration, transfer value transactions via Ethereum tokens between providers and consumers, as well as raw IoT data payload. This can turn smart room IoT devices, such as smart locks, light bulbs, air conditioning and fans into rentable business entities within a secure sharing economy platform. We will demonstrate such a proof of concept IoT sharing economy framework, which is specifically designed to support the temporary IoT needs of very large numbers of users, such as Hajj pilgrims concentrating for a short period of time at a single area in Saudi Arabia.

Categories and Subject Descriptors

• Computer systems organization → Embedded and cyber-physical systems; • Security and Privacy → Cryptography;

General Terms

Design; Security; Experimentation

Keywords

Sharing economy; blockchain; off-chain; IoT as a service.

ICMR'19, June 10-13 2019, Ottawa, Canada.
ACM 978-1-4503-2033-7/13/04.
http://dx.doi.org/10.1145/2578726.2582619

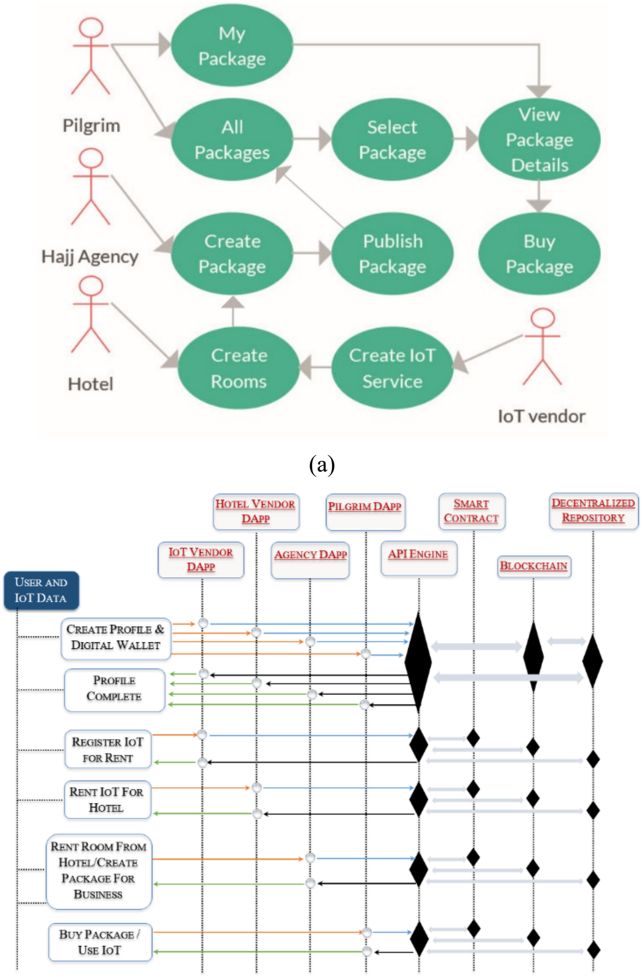
1. INTRODUCTION

Due to the industry 4.0 revolution, sharing economy services can take benefit from IoT and edge computing paradigm, not only for processing large amounts of data, but also for incorporating decentralized security mechanisms. For example, blockchain and off-chain can provide data security and privacy of the IoT data and the identity of the stakeholders [1] [2]. Two parties, without knowing each other, can perform a sharing economy business contract in which financial transaction or multimedia IoT data sharing needs to be performed without a middleman [3] [4] [5]. This has given rise to the popularity of Web3.0, which is also termed as Distributed Applications (DApps), in which the users can do business transactions with the backend decentralized Blockchain and off-chain repositories via the popular web interfaces. Since location of data source, captured event and type of data, and identity of the transaction-parties are secured, sharing economy applications can be performed ubiquitously [8].

In this demonstration, we address the challenge of bringing the intelligent IoT processing required for novel sharing economy services to the edge. Since IoT devices produce a massive amount of IoT data at the edge, we have developed analytics to process the IoT data at the edge, extract business semantics from the IoT data, secure and analyze the transactions, and save the transaction to the blockchain. We have developed digital wallets for different actors such as IoT vendor and IoT data consumes. The multimedia payload available from the IoT devices or from the sharing economy ecosystem are stored at decentralized repositories. By using our proposed framework, smart contract-based business intelligence can be enforced at the edge to coordinate seamlessly with the IoT data processing framework. This allows the needed types of security to be maintained such as confidentiality, integrity, availability, and authentication of the data, whether at the edge network, during the data communication between the edge and the decentralized cloud or at the remote cloud.

The remainder of the paper is organized as follows: section 2 describes the design and function of the different subsystems of the framework developed. Section 3 illustrates the implementation details. Section 4 outlines concluding remarks and our future directions.

2. DESCRIPTION OF THE SYSTEM



(a)

(b)

Figure 1. To be shown during demo (a) Salient use cases (b) Interactions among key actors.

Fig. 1 shows the major use cases and interactions among different key actors of the demo environment. Our system has four types of human actors: IoT vendor, hotel that wants to securely incorporate a number of IoT devices as a service, business agency that incorporates the hotel within its packages, and end user who purchases the packages from the business agency. Figure 1(a) shows the use cases that will be demonstrated during the presentation, where the end-user is a Hajj pilgrim who is provided with different packages by his/her corresponding Hajj agency and hotel. Figure 1(b) shows the sequence of interactions for a subset of salient use cases. Before using the system, each actor has to register their blockchain profile. During registration, the big data such as images, audio, and video, which cannot be saved into blockchain due to its limitation in block size, is saved to a decentralized repository, while a hash or a set of hashes are linked within the blockchain, and a digital wallet containing the secure keys and virtual currencies are created.

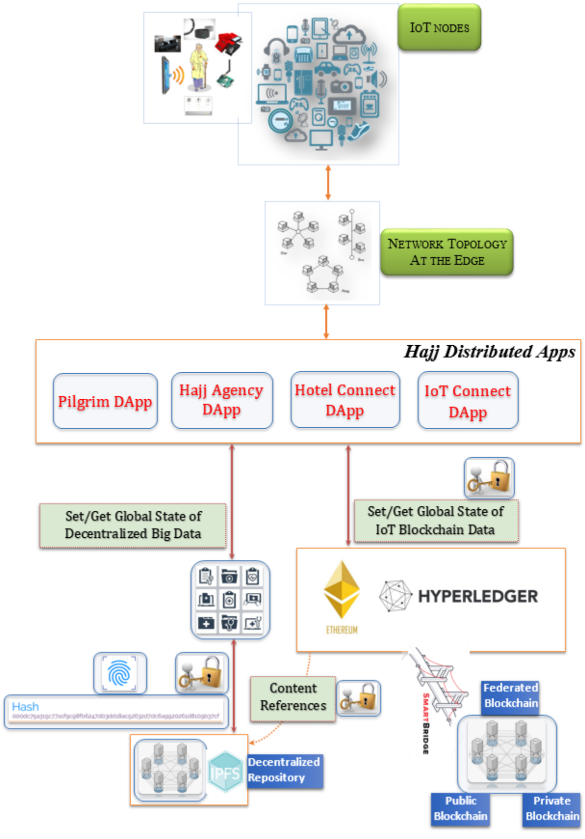


Figure 2. Block diagram of the framework.

The virtual currencies are mapped with physical assets that are available to each actor to support business transactions. We have developed a distinct Distributed App (DApp) for each type of actor. As shown in Figure 1(b), each IoT vendor adds each rent-able IoT device to the blockchain and off-chain. Any hotel can search and rent any number of IoT devices from any IoT vendor. Any business entity such as a Hajj/Travel agent can search, explore the IoT features, and create packages for pilgrims including hotel rooms with various numbers of IoT devices and pay from their wallet. After each business transaction, the account balance (amount of virtual currencies in the wallet) of each participating party is updated, notifications are generated, and ownership of the IoT devices are also updated in the blockchain. An actor can always check the live status of the IoT devices in use or in possession through our live blockchain and off-chain visual data analytics.

Figure 2 shows a high-level flow of different components. IoT nodes communicate with the distributed applications via available edge networks. During each type of transaction, a block is created in which the encrypted IoT or business transactional data is stored. If there is any raw data associated with the transaction such as captured IoT sensory data payload, it is sent to the decentralized repository, which returns a set of hashes. These hashes are stored within the block to keep an immutable link between the transaction and the associated multimedia big data in the off-chain. Figure 3 shows an instance of the timeline of a business transaction taking place between different actors.

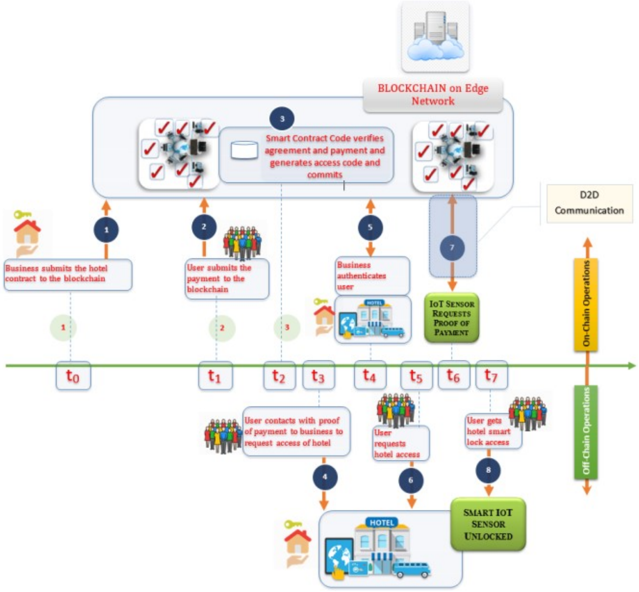
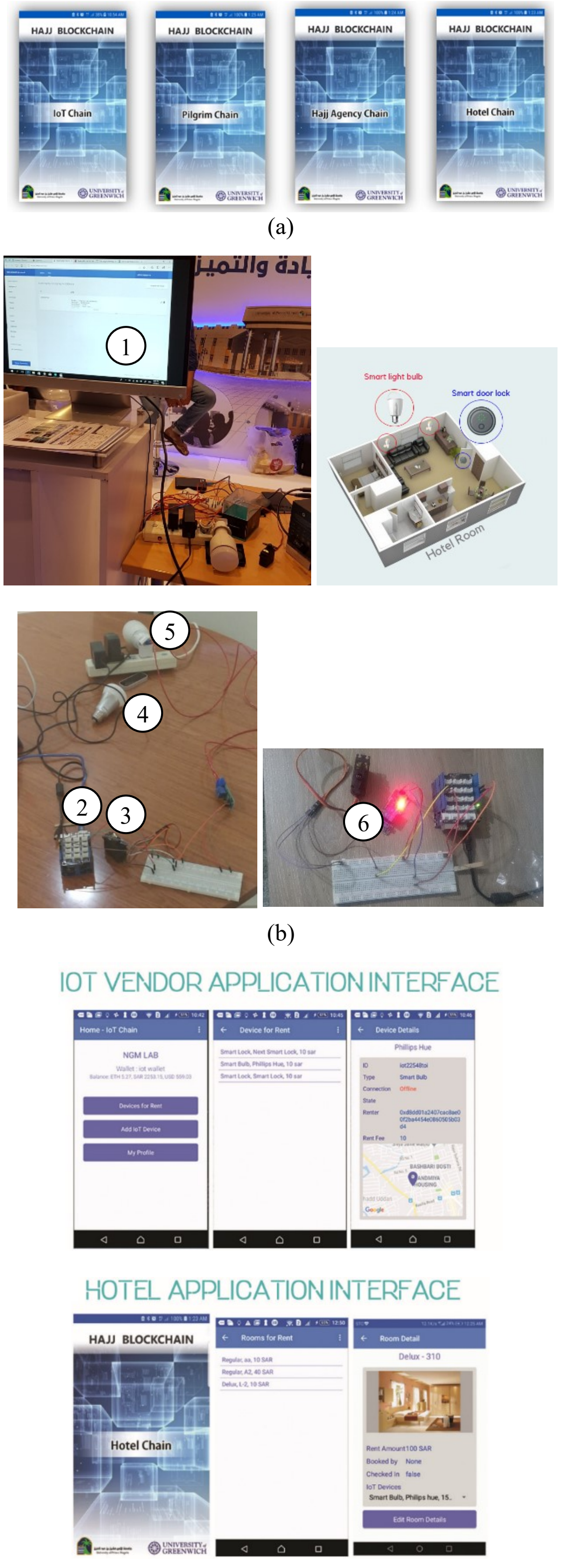

BLOCKCHAIN on Edge Network
3
Smart Contract Code verifies agreement and payment and generates access code and commits
D2D Communication
1
Business submits the hotel contract to the blockchain
2
User submits the payment to the blockchain
5
Business authenticates user
HOTEL
7
IoT Sensor Requests Proof of Payment
On-Chain Operations
1
2
3
t0
t1
t2
t3
t4
t5
t6
t7
Off-Chain Operations
User contacts with proof of payment to business to request access of hotel
User requests hotel access
User gets hotel smart lock access
4
6
8
HOTEL
Smart IoT Sensor Unlocked

Figure 3. Detailed timeline of a sample sharing economy transaction that will be demonstrated.

3. IMPLEMENTATION

The hardware used for our work consists of a number of cloud machines running Ubuntu 64-bit as virtual machine with 8GB of RAM. We have used Docker Containers for full node, simplified payment verification (SPV) nodes, and certificate authority nodes. For secure, reliable, and scalable access to Ethereum transactional APIs and IPFS gateways, we have used Infura, a scalable blockchain infrastructure. We have used Ethereum for business transactions and Hyperledger Fabric for blockchain nodes, smart contract management and API, and Node.js V10.15.1 for communication with the IoT gateway. The off-chain has been implemented using InterPlanetary File System (IPFS). Figure 4(a) shows the user interfaces of the four distributed smartphone applications which will be demonstrated, while Figure 4(b) shows the integration of the IoT devices that can be registered into the system and added to different business scenarios. In the demo scenario, we will show a smart lock and a smart bulb that can be added to a hotel.

An end user can buy any package of their choice from a business agent that will include one or more IoT devices. Once purchased, the IoT device's status is associated with the public blockchain address of the end user. The status of these devices can be controlled via the DApps. The DApps use smart contracts that implements the business logic. Figures 4 (b) and (c) show sample use case interfaces. In each of the business cases, location of the transaction parties and the IoT nodes are stored in the blockchain and can be shared with anyone. Since blockchain cannot be used as a real-time database, we have used a no-SQL key-value pair database for storing the live location and any other data available from any of the peer nodes. The live data is supported by a queue service which can store a very large number of key-value pairs to share with the API server. The API server interacts with the smart contract, blockchain and off-chain to store the live location and other data into the permanent decentralized and immutable repositories.



(a)

(b)

Home - IoT Chain

NGM LAB

Wallet : iot wallet

Balance: ETH 5.27, SAR 2253.15, USD 559.03

Device for Rent

Smart Lock, Next Smart Lock, 10 sar

Smart Bulb, Phillips Hue, 10 sar

Smart Lock, Smart Lock, 10 sar

Device Details

Phillips Hue

ID	iot22548toi
Type	Smart Bulb
Connection	Offline
State	
Renter	0xd8dd01a2407cac8ae00f2ba4454e0860505b03d4
Rent Fee	10

Rooms for Rent

Regular, aa, 10 SAR

Regular, A2, 40 SAR

Delux, L-2, 10 SAR

Room Detail

Delux - 310

Rent Amount100 SAR

Booked by None

Checked In false

IoT Devices

Smart Bulb, Philips hue, 15..

(c)

Figure 4. Developed user and IoT cyber physical interfaces (a) four distributed Apps connected with the Blockchain and distributed big data repository via IPFS (b) smart lock and smart bulb connected to the Blockchain, DApps, and IPFS via edge networks, and (c) user interfaces of sample sharing economy services.

Figure 4 (b) shows some sample cyber physical interactions. For example, Figure 4 (b)-(1) in top left figure shows the live blockchain analytics and transaction explorer. Figure 4 (b) top right figure shows a schematic of smart lock and smart bulb placement in a real hotel room. Figure 4 (b)-(2) shows an Arduino board running on-board sensors and communication modules to connect with IoT devices and the smartphone DApps running within the edge network. Figure 4 (b) – (3) (4) (5) in the bottom left figure show the servo motor running as smart door lock, ZigBee based smart bulb, and Wi-Fi-based smart bulb respectively that are interfaced with the Arduino board. Finally, Figure 4 (b)-(6) shows a connection between a smart bulb with the relay device and blockchain based control of the IoT device, which is at the edge network.

4. CONCLUSION AND FUTURE WORK

The secure integration of IoT devices within business transactions can become an enabler for novel sharing economy scenarios, in which two parties unknown to each other can perform cyber-physical business transactions in a trustworthy and decentralized manner. We have designed[1] such an IoT ecosystem in which IoT devices can be rented as a service within a variety of sharing economy scenarios. To emphasize on the practicality of this work, we have developed blockchain and off-chain data analytics and digital wallet visualization metaphors, which will show live visuals during different IoT-based business transactions. In the future, we will be adding more functionalities to support a complete sharing economy business case.

5. ACKNOWLEDGMENTS

This work has been supported by the British Council's Gulf Science, Innovation and Knowledge Economy (GSIKE) project "Secure Hajj and Umrah" with Application ID 372628808, and the University of Greenwich, London UK and University of Prince Mugrin, Madinah, KSA.

6. REFERENCES

[1] Rahman, M. A., Hossain, M. S., Hassanain, E., and Muhammad, G., 2018. “Semantic Multimedia Fog Computing and IoT Environment: Sustainability Perspective,” *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 80–87, 2018.

[2] Rahman, M. A., Hassanain, E. , and Hossain, M. S. , 2017. “Towards a Secure Mobile Edge Computing Framework for Hajj,” *IEEE Access*, vol. 5, pp. 11768–11781.

[3] Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q., 2017. “A survey on the security of blockchain systems,” *Futur. Gener. Comput. Syst.*, 2017.

[4] Yin, H., Guo, D., Wang, K., Jiang, Z., Lyu, Y., and Xing, J., 2018. “Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm,” *IEEE Netw.*, vol. 32, no. 1, pp. 112–117.

[5] Pham, Q.-V., LeAnh, T., Tran, N. H., and Hong, C. S., 2018. “Decentralized Computation Offloading and Resource Allocation in Heterogeneous Networks with Mobile Edge Computing,” *IEEE Access*, vol. 6.

[6] Rahman, M. A., and Hossain, M. S., 2017. “m-Therapy: A Multi-sensor Framework for in-home Therapy Management: A Social Therapy of Things Perspective,” *IEEE Internet Things J.*, vol. 4662, no. c.

[1] https://www.dropbox.com/s/0av9oou1356mtgu/Blockchain-sharingEconomy-IoT.MOV?dl=0