Federation University

Federation University ResearchOnline

https://researchonline.federation.edu.au

Copyright Notice

This is the published version of:

Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M. (2020). Investigating Smart Home Security: Is Blockchain the Answer? *IEEE Access, 8*, 117802–117816.

Available online: https://doi.org/10.1109/ACCESS.2020.3004662

Copyright © 2013 IEEE. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/). The use, distribution or reproduction in other forums is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

See this record in Federation ResearchOnline at:
http://researchonline.federation.edu.au/vital/access/HandleResolver/1959.17/185383

CRICOS 00103D RTO 4909

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BLOCKCHAIN-ENABLED TRUSTWORTHY SYSTEMS

Received May 27, 2020, accepted June 17, 2020, date of publication June 24, 2020, date of current version July 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004662

Investigating Smart Home Security: Is Blockchain the Answer?

SAMRAH ARIF[1], (Graduate Student Member, IEEE), M. ARIF KHAN[2], (Member, IEEE), SABIH UR REHMAN[1], (Member, IEEE), MUHAMMAD ASHAD KABIR[3], (Member, IEEE), AND MUHAMMAD IMRAN[4], (Senior Member, IEEE)

[1]School of Computing and Mathematics, Charles Sturt University, Port Macquarie, NSW 2444, Australia
[2]School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[3]School of Computing and Mathematics, Charles Sturt University, Bathurst, NSW 2795, Australia
[4]College of Applied Computer Science, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Muhammad Imran (dr.m.imran@ieee.org)

The work of Muhammad Imran was supported by the Deanship of Scientific Research at King Saud University through the Research Group under Project RG-1435-051.

ABSTRACT Smart Home automation is increasingly gaining popularity among current applications of Internet of Things (IoT) due to the convenience and facilities it provides to the home owners. Sensors are employed within the home appliances via wireless connectivity to be accessible remotely by home owners to operate these devices. With the exponential increase of smart home IoT devices in the marketplace such as door locks, light bulbs, power switches etc, numerous security concerns are arising due to limited storage and processing power of such devices, making these devices vulnerable to several attacks. Due to this reason, security implementations in the deployment of these devices has gained popularity among researchers as a critical research area. Moreover, the adoption of traditional security schemes has failed to address the unique security concerns associated with these devices. Blockchain, a decentralised database based on cryptographic techniques, is gaining enormous attention to assure security of IoT systems. The blockchain framework within an IoT system is a fascinating substitute to the traditional centralised models, which has some significant concerns in fulfilling the demand of smart homes security. In this article, we aim to examine the security of smart homes by instigating the adoption of blockchain and exploring some of the currently proposed smart home architectures using blockchain technology. To present our findings, we describe a simple secure smart home framework based on a refined version of blockchain called Consortium blockchain. We highlight the limitations and opportunities of adopting such an architecture. We further evaluate our model and conclude with the results by designing an experimental testbed using a few household IoT devices commonly available in the marketplace.

INDEX TERMS Internet of Things (IoT), smart homes, security, blockchain, ESP32.

I. INTRODUCTION

In recent years, the expansion in Internet of Things (IoT) technologies has encouraged the transformation of traditional homes to smart connected homes [1]. According to a recent report on global internet growth and trends from Cisco [2], the number of smart home devices is being foreseen to escalate upto 28.5 million by 2022. Moreover, according to Gartner [3] the previously envisioned number of 500 million smart automated home devices is set to increase to around 700 million in the current year. As the number and heterogeneity of smart home devices are accelerating promptly, it is becoming increasingly challenging to maintain security of these devices [4].

IoT networks are susceptible to security threats for a range of reasons. It is straightforward to get access to each device as these devices are usually confined and separated, and there is no manager to regulate or supervise these devices [5]. These individual devices typically interact with one another via a gateway using variant wireless communication protocols, that often paves the way for attackers to perform eavesdropping; and at last, most devices have less processing

The associate editor coordinating the review of this manuscript and approving it for publication was Hong-Ning Dai.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

capabilities and therefore it is troublesome to apply advanced security techniques on each device [6], [7]. Likewise, IoT appliances in smart homes may provide unauthorised access to cyber criminals to monitor the private lives of occupants and exploit them by using sensitive information. Such wrongdoings appear extremely likely in light of the usual practice of demanding ransom from the residents in the present [8]. In 2018, a real case of criminal hacking in which offender tried to steal data from a North American casino via a fish tank was revealed [9], [10]. Although the casino had enforced some security precautions to discover the threats, the tank was still compromised by the hackers in order to send data to a device in Finland. The future of IoT implies that security forces should prepare themselves for advanced, unfamiliar crimes and terrorist attacks [11]. Security issues such as data privacy, authorisation and authentication, vulnerability in access control mechanism, system configuration issues and privacy of information repository are the key security threats in smart home environment [12]–[14]. Furthermore, IoT devices have limited computation power and memory which makes them more susceptible to various security threats. Traditional IoT systems are centralised, linked with cloud servers that can lead to failure of the whole network if the central server is compromised. Hence, to overcome these challenges, various types of solutions have been presented that include the addition of various security layers in existing architectures [15], [16] in addition to implementation of a decentralised network system called blockchain in the smart homes [17], [18]. During the past few years, blockchain has started to be identified as the key to solve security, trust, privacy, scalability, and reliability concerns associated with the IoT paradigm [19], [20]. The adoption of blockchain into the smart homes reduces the massive security concerns such as authentication and authorisation, confidentiality, integrity and single point of attack. Blockchain technology is based on the decentralised digital ledger supported by cryptography. Instead of the traditional centralised networks, it operates with the distributed database that maintains a chain of block. Each block in blockchain is connected to the previous one by maintaining the hash of that previous block which ensures the security of those blocks from tampering [21]. Bitcoin [22], the first cryptocurrency, is one of the most prominant blockchain application [23] and the success of the bitcoin motivates the researchers to adopt this technology into the IoT paradigm. However, adoption of blockchain in smart homes results in complex, time consuming and expensive systems that motivates us to dig deeper in order to optimise the feasibility of the of blockchain adoption in smart homes.

This article investigates the utilisation of blockchain-based smart home architectures in detail and highlights the limitations of applying such solutions without taking into account the actual and unique requirements of individual smart homes by designing a hardware prototype on a refined version of blockchain called consortium blockchain. The designed framework undertakes the consideration to reduce the request processing time, cloud storage usage and user involvement as a node in blockchain verification. The main contributions of this article are summarised as follows:

- Investigated the security issues within the smart home architectures and explored the design of a smart home architecture using Consortium Blockchain.
- Implemented hardware design for a simple secure smart home architecture by utilising commonly available IoT devices to evaluate.
- Designed and presented a working prototype of a Smart Home Mobile App for the proposed architecture.

The remainder of this manuscript is organised as follows: Section III describes the background, preliminaries and the state of the art blockchain-based smart home designs. Section IV presents the smart home architecture considered in this paper. In Section V, the hardware implementation of the suggested framework in this article, along with the exploration of a few IoT devices, has been elaborated. Section VI presents the results and findings of this investigation study along with a prototype model of the suggested architecture in the form of a mobile application. Finally, the paper concludes in Section VII.

II. BLOCKCHAIN OVERVIEW

Blockchain is currently one of the dominant research motivations of recent times [20], [24]. It is an append-only decentralised digital ledger that is supported by cryptography [25]. It provides a platform to process trusted transactions (TXs) without third-party involvement. Each request has a record in the form of a chain of blocks with a digital signature for verification. Since the ledger is generated and maintained by all participants equally within the system [23] and there is no central server to manage the activity, blockchain holds tamper-proof and immutable information in a secure and encrypted manner. Blockchain uses Peer-to-Peer (P2P) network and every node (network user or new user) is allowed to join in a secure manner. Whenever a new node/user joins the blockchain network, it gets the full copy of the blockchain. When a new request is generated, a block is created and is sent to every node in the network, once verified by all the nodes to make sure it is not tampered with, it is then added to the chain of blocks. All the nodes in the network create a consensus to verify validity of the block. Each time a node gets a blockchain for verification, every node in the network matches it with its blockchain; the blocks that are tampered with are rejected by the nodes in the network. Consensus created by the nodes who are participating in block verification is called Proof-of-Work (PoW) [25]. It is an algorithm that is used to confirm TXs and produce new blocks to the chain. The PoW uses random calculations to solve the complex cryptographic puzzle (sufficient number of leading zeros in hash combinations) which requires adequate computing power and fast machines. There is always a chance that the attacker could get a really fast machine to solve cryptographic puzzles, and easily generate new blocks to gain control over the network. To resolve this, a difficulty target

number is used that controls how hard the machine has to work to generate a new block and this is not a fixed number. In bitcoin, the difficulty is automatically adjusted every 2016th block [23]. If more blocks are created within a limited time period, the difficulty escalates and requires adequate time. In small scale applications with limited computational resources and requiring quick response, a standard practice is to keep the difficulty needs between 1 and 2 to acquire the desired results [26].

Currently, blockchain is being implemented in three ways. First is the public blockchain, also called permission-less blockchain, in which the ledger is completely distributed and publicly accessible to users, miners, developer or community members [27]. The second approach is the private blockchain that is a permissioned blockchain where only pre-chosen entities of a known organisation have permission to access the blockchain. These entities are chosen by the respective authorities, i.e. the blockchain developers or ecosystem participants. The third technique to implement blockchain is consortium blockchain technology, and it draws its characteristics from both public and private blockchain. In consortium blockchain, only a pre-chosen set of nodes are pledged for validating the block [28]. It is considered as public blockchain because the chain of blocks are being shared by unlike nodes, and the reason of being private is that the nodes that can access the blockchain are confined; hence, this scheme could be known as partially centralised. According to [29], the consortium blockchain architecture is more suitable for areas that require transaction agility, privacy protection, and internal system superintendence. This blockchain technique provides new grounds for security and privacy assurance of smart homes.

III. RELATED WORK

This section provides a comprehensive synopsis of recently proposed blockchain-based smart homes to overcome the threats and vulnerabilities that are affecting the security of smart homes.

Numerous security infrastructures have been proposed in the research world. Indeed, majority of these state-of-the-art infrastructures are tediously centralised that causes single point of attack, which obstruct scalability and vast adoption of IoT applications as well as raise severe privacy and security concerns [30]. Currently, blockchain represents one of the utmost suited candidates to set up a secure and distributed/decentralised ecosystem for IoT systems [31]. Although blockchain have been extensively investigated in various contexts such as smart cities [32] and cloud [33], however, it is still in infancy in context of smart homes.

A. PUBLIC BLOCKCHAIN SYSTEMS FOR SMART HOMES

In [34], the authors have proposed a security framework using the blockchain technique to protect the IoT system from potential threats. According to the author, the implementation of blockchain technology in IoT paradigm creates a platform that allows all IoT devices to communicate securely with one another in a distributed environment. In [35], the authors came up with a smart district model by combining the IoT with blockchain and developed the power grid access for the users. By this developed prototype model, users are able to collaborate via blockchain with the power grids system. Anyone with a solar panel configuration can engage with the network to primarily buy and/or sell energy straight over the blockchain mechanism. This could be a valuable illustration of blockchain-based IoT applications that are carried out and replicated in the real world. This paper also demonstrates some prerequisite significant factors for a smart home system, that could be considered as a considerable allusion for designing and developing a novel smart home application.

In [36], a secure energy trading scheme called EnergyChain for automated homes using blockchain in the smart grid ecosystem was designed. In the proposed scheme, a thorough security evaluation of the presented framework concerning the communication, costs and computation time that exposes the supermacy of EnergyChain was explained. In [37], a smart home system was used as a representative case study on blockchain. In this study, the core building blocks of the smart home tier were outlined by the author. This paper also examined the transactions and procedures linked with the described components. Furthermore, the author performed the security and privacy analysis of proposed blockchain-based smart homes. In his opinion, his proposed method incurred the low processing overhead and are convenient for IoT devices that are low resource. According to the author, this study was the primary step that aimed to optimise blockchain (BC) for the smart connected homes.

In 2017, a Smart Door Lock system based on blockchain was proposed in [38] that consisted of a plain blockchain method with the three users as a node to perform PoW. This system utilises three sensors to detect the motion and distance of the nodes. However, the scenario of being a single home owner (a single node) has not been discussed in that solution. If there is only a single node, the concern arises that how the blockchain-based door lock will work to verify the transactions created by that single node.

A recent effort on the blockchain-based IoT that upgrades the security and privacy of the smart factory has been observed in [39]. In this research, author proposed an innovative IoT architecture based on blockchain for smart factory consists of five layers: the sensing layer, the management hub layer, storage layer, the firmware layer, and the application layer. The sensing layer incorporates different sorts of sensors, whereas the application layer gives various types of services to users, such as real-time monitoring and failure prediction. The management hub layer consists of a particular node called management hub that has the responsibility to parse, encrypt and packages the uploading data to Create blocks, and stores it in the blockchain database. The storage layer has a data centre that keeps encrypted tamper-resistant data and blockchain records in a distributed manner and synchronises at a predetermined interval. The firmware layer associates each layer by implementing technologies such as

data acquisition, distributed algorithm and data storage technology. Based on the described defence mechanisms of the designed architecture in this research, author mentions that the proposed architecture can boost up the (Confidentiality, Integrity and Availability) CIA prerequisites substantially. The proposed architecture can also be recognised as a suitable framework to increase the security of smart homes. In [40], the authors utilised public blockchain, cloud and smart contract and developed an efficient lightweight integrated blockchain (ELIB) model for IoT systems and implemented it in smart homes for the performance evaluation. Although, the model reduces the processing time and shows adequate performance, but the cloud usage might increase the system cost. In [41], another Ethereum based smart home solution was proposed that minimises the confidentiality, integrity and authentication issues of the IoT devices and centralised gateway issues, however, the proposed design has not addressed the addition computational complexity created by blockchain. The reader is referred to [42] for the description of smart contracts and their role in blockchain.

B. PRIVATE BLOCKCHAIN SYSTEMS FOR SMART HOMES

In [43], authors have proposed a blockchain-based secure and lightweight architecture for a smart home. In this proposed scheme, the local blockchain in the smart home is centrally supervised by its owner. All the communication between the local devices and the overlay nodes uses a shared key issued by the miner to secure the communication. The author applied lightweight hashing to reveal any deviaton in the transactions. The proposed architecture assured data confidentiality, integrity, and availability alongside the protection against Distributed Denial-of-Service (DDoS) attacks. This architecture utilises cloud storage to avoid the low memory issue for the smart home device. However, certain highlighted shortcomings were observed by the author in [44] in the architectures presented in [37] and [43]. Firstly, the recognition of blockchain is its decentralised network, whereas in this model, Home-Miner, CHs (Cluster Heads) and the cloud storage at the respective layer are presented as a centralised point that can result in a single point of compromise. Secondly, Home Minor is mining the block without PoW; however, PoW is the core activity that defends the blockchain against data forgery and double-spending attacks. Next, the Home Minor monitors all the incoming and outgoing TXs instead of consensus-based TX validation as performed in typical blockchain platforms. The author mentions, if the Home miner gets corrupted or attacked, the integrity of the blockchain cannot be assured. Lastly, according to the author, the overlay network in [37] maintains Cluster Heads (CH), that stores Public Keys of the requesters and requestees, and the list of TXs forwarded to other CHs. It is up to the CH, whether to retain a new block or not, whereas Bitcoin blockchain is a consensus-based decision system that makes it a strong mechanism against various attacks.

In [45], the author identified several security aspects in implementing blockchain in the IoT environment that are most extensive and require extreme struggle to deal with, and proposed a 5-layered state-of-the-art efficient and secure framework for blockchain-based IoT systems. This framework comprises of the fundamental IoT layers alongside the extra storage layer that focuses on the adequate data transmission in a permissioned network based on blockchain. The author used cloud for the records provoked by IoT sensors due to the lack of capacity of sensing devices to keep the observed data. The storage layer ensures security features like availability, minimal block creation time, integrity, verified access, scalability, and lastly immutability of the transactions. In the storage layer, a blockchain is set up when each block is verified by running the consensus algorithm and mining activity that is performed by the miners. This proposed design model has enough adaptability to be embraced by businesses, companies, schools, smart cities, and smart homes.

The IoT home device does not have tremendous computation power and storage area; Also, data streaming could require a lot of time and budget. Therefore, the author realises that the combination of blockchain and smart contract can significantly improve the security level of automated homes [46] and presents a novel lightweight blockchain and smart contract-based smart home hierarchy architecture. The smart contracts are the scripts that are built in the private blockchain. The smart home IoT device triggers the smart contract manners when some specific condition is satisfied. In the proposed architecture [47], each IoT device stores the distributed ledger locally, and each smart home deploys a local minor to process the transaction in the private or public blockchain. The local minor also plays a role in storing the device data, adds a new device to the private blockchain and embed new smart contract to IoT devices. By contemplating the low computing capability and storage limitation of IoT device, the author sets the specific time limit for uploading the data from private blockchain to the local minors. The author suggests the private blockchain should upload the data to local miners every ten days and can only keep the last five blocks for future transactions.

In [48], an Ethereum-based decentralised Smart Home System was composed and implemented. Ethereum is a software platform based on blockchain technology that facilitates developers to build and deploy decentralised applications, and it is used by the authors in [48] to build smart contracts. In the proposed design, Smart Contracts are utilised to store the data collected from the sensors, and they can be built using Ethereum. By using Ethereum with smart contracts, a system prototype was successfully designed by the author to simulate the smart home application. This model was set to update the humidity and real-time temperature of smart homes and recur automatically when a certain event is triggered. However, the authors in [48] have mentioned that the proposed system is not cost-effective, and some other design issues which need to be improved has also been discussed in this article. Another implementation of Ethereum on smart home system has been studied in [51] where the authors have proposed a smart

TABLE 1. Summary of recently proposed Blockchain based Smart Home architectures.

Publications	Core Components			Achieved Security				Architectural Features				
	Building Blocks	Blockchain Type	Hardware Implementation	Confidentiality	Integrity	Availability	Prevent from DDOS Attack	Immutability	Scalability	Cloud Storage	Minimise Response Time	Cost Effective
[34]	Distributed Ledger, Wifi / Bluetooth, Physical Layer, Sensors.	Public		✓	✓			✓				✓
[35]	Smart Contracts, Consensus Algorithm (PoW / PoS), Distributed Ledger.	Public		✓		✓		✓	✓			
[36]	A Minor Node (A Central Entity), Normal Nodes, Consensus Algorithm (PoW).	Public & Private		✓		✓			✓	✓	✓	
[37]	Smart Home Minor (A Central Entity), Local Storage (a backup drive).	Public	Simulation	✓		✓	✓		✓	✓		
[38]	Control Module i.e. a CPU, Data Storage, PoW, Indoor & Outdoor Intrusion Detection Algorithm.	Public		✓	✓		✓	✓				
[47]	Smart Contract, Local Miner (Storage), IoT Devices (Nodes).	Private		✓	✓	✓	✓	✓	✓			
[48]	Ethereum (For Smart Contract) Two Local Miners.	Private	Simulation	✓		✓	✓					
[49]	Smart Contract Cloud Network.	Consortium	Simulation	✓		✓	✓		✓	✓	✓	
[40]	Ethereum (For Smart Contract), Consensus Algorithm, Distributed Throughput Management Scheme, Certificateless Cryptography Method.	Public	Simulation	✓	✓	✓		✓		✓	✓	
[41]	Ethereum (For Smart Contract), Smart Home Gateway,	Private		✓		✓	✓			✓		
[50]	Homomorphic Encryption Nodes (smart gateway, leader smart gateway, verification, leader verification).	Consortium		✓	✓							

home architecture consisting of a private Blockchain, a smart home miner (SH miner), local storage linked to Smart Home sensor (SH sensor) and actuator devices. This architecture was the modified version of the design proposed in [37] along with the addition of Ethereum application and smart contract. The system was able to buildup the policies for handling the transactions to specify the authorised individual to access and monitor the data. Additionally, the author mentioned in his research that the Ethereum-based blockchain may undergo a challenge in time-sensitive conditions as it takes around 20 seconds transaction time which can not be sufficient and quick enough for handling a few situations that require urgent responses.

C. CONSORTIUM BLOCKCHAIN SYSTEMS FOR SMART HOMES

In [49], the consortium blockchain was incorporated with cloud computing and the smart home architecture was presented in to achieve confidentiality, integrity, scalability, and availability to keep smart homes safe and secure. The proposed scheme showed the blockchain implementation in a smart home network for manipulating the transactions and uses green cloud computing. The technique implements green service using as a green broker to lessen the factors affecting environmental condition, i.e. managing the selection of energy-efficient service providers, of the proposed model. In [50], the authors have designed a smart home system based on consortium blockchain that is specific to data privacy. The performance of the model was evaluated by simulation; however, the architecture does not explained the energy consumption and activity processing time.

The core components in the recently proposed blockchain-based smart home architectures alongside the achieved security have been summarised in the table 1.

IV. MODEL ARCHITECTURE

This section describes the implemented architecture by highlighting concerns in the previously proposed blockchain-based architectures.

A. PROBLEM STATEMENT

Most of the existing blockchain-based architectures are quite complex to implement, as public blockchain is based on an open network and can suffer from scalability issues. Due to this reason, a reasonable implementation of the 'private and consortium blockchain' has been taken into consideration, however these architectures maximise the use of cloud storage that can easily act as a point of attack; compromising user privacy and resulting in a potential increased cost to implement the solution. Additionally, the use of Ethereum-based models for smart contracts while possible, can not be considered cost effective for smart home systems.

Practical implementation of the currently proposed architectures has hardly been seen in the recent literature. Additionally, in blockchain-based system, there is a requirement to have more than one nodes (user nodes) for the TX verification. Hence, if one wants to connect to the home network, the other nodes must validate the TX created by associated node that creates a problem for a single home owner.

By considering all these issues, we came up with a more appropriate and simplified solution of smart home, based on consortium blockchain. In this scheme, the IoT devices

behave as a node in blockchain process instead of the user nodes and participate in transaction verification. The users are authorised by a separate process via RESTful API. This suggested architecture enhances the privacy and security by implementing the core blockchain process by PoW along with the further security checks that enhances integrity and confidentiality in the system. The solution also provides a design that is simple to implement, cost-effective, secure and less time-consuming. A detailed description of the proposed architecture can be found in the following subsection.

B. BUILDING BLOCKS

Building blocks of the designed architecture are Sensor Nodes (*SeN*), Super Node (*SN*), Blockchain and Users. All SeNs and SN are communicating with each other using mesh network topology locally within the smart home. The solution has been designed using a refined version of blockchain called consortium blockchain [52]. In this type of blockchain, only pre-chosen nodes can participate in consensus and generate blocks; not all nodes participate in consensus. Consortium blockchain methodology was adopted as it dramatically reduces communication overhead and network load which is ideal for smart home environment. In this proposed technique, the concept of a user's performance as a node has been eliminated. Instead, every smart device in the smart home acts as a node and participates in mining. However, in the case of increased devices, the user can choose a minimum of two devices, $N = 2$, for mining. The overall proposed design with four *SeN* along with the *SN* can be seen in Fig 1.

Let us define the total number of miners by M, which is a combination of selected $SeN \in \mathbf{N}$ and $SN \in \mathbf{N}$. Mathematically it can be represented as

$$M = \sum_{i=1}^{N} \left(SeN_i \right) + SN, \tag{1}$$

where $N = 4$, comprising only *SeNs* excluding *SN* in the proposed architecture as per in Fig. 1. The reason to exclude *SN* is that it plays the role of principal player and controls the participation of each *SeN* in various processes and also establishes the communication with the users. We further represent the packet communication between sensor nodes, *SeNs*, by p_{ij}, where p represents the data packet being communicated from node i to node j where $i, j \in \mathbf{N}$. We can represent the network model with *SeNs* and *SN* as a strategic game with a set of N players (network sensor nodes) such that $\mathbf{N} = \{1, 2, \cdots, N\}$. The *SN* sets the rules of participation for $SeNs \in \mathbf{N}$ in the transaction verification. The objective of each *SeN* is to maximise its participation in the verification process. Total time taken by a complete transaction is directly proportional to the number of nodes involved in the transaction completion process. Let us represent the total time taken to complete a transaction by T. This involves the time taken by M miners, given by Eq. 1, and mathematically can

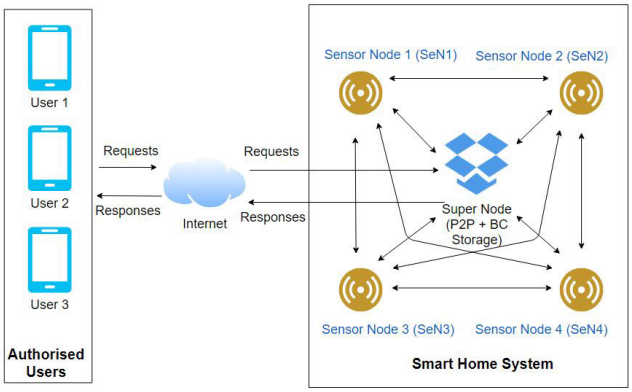


FIGURE 1. Adopted smart home architecture using IoT-Blockchain.

be written as

$$T_M = \sum_{i=1}^{M} \left(t_i \right). \tag{2}$$

In the following, we discuss each of the key building block of the proposed design.

1) SUPER NODE (*SN*)

The *SN* is a Peer-to-Peer (*P2P*) server as well as the storage for the blockchain ledger. This node is responsible for communicating with the sensor nodes for the transaction management and blockchain storage. Furthermore, this node also keeps the complete blockchain ledger and broadcast the last five blocks of the ledger to the connected sensor nodes for transaction verification. The *SN* also communicates with the users through the internet via RESTful API to send and receive the commands and responses to authorise the user to enter the smart home network. It keeps the addresses of the registered users for further communication in the network. The overall user authorisation process can be seen in Section IV-B5.

2) SENSOR/ACTUATOR NODES (*SeN*)

In the proposed architecture, the sensor/actuator nodes are responsible to communicate with *SN* and participating in the transaction verification. When an authorised user wants to join the smart home network to perform any activity and communicate with any of the smart device, *SN* activates by generating a transaction and broadcasts it to *SeNs*. The broadcasted transaction then waits to be picked up by the *SeNs*(miners). Miners on the network select the broadcasted transaction and form it into a 'block'. To add this block of transactions to the blockchain, the block first needs a PoW to be verified by the other miner nodes. The overall transaction flow has been discussed in the following subsection.

3) TRANSACTION VERIFICATION PROCESS

In order for a block, b_i, to be accepted by network participants and added in the blockchain, miners (sensor nodes), M, must

complete PoW as mentioned in previous subsection IV-B2. PoW is a mechanism that slows down the creation of blocks by This makes very hard to tamper with the blocks because if one block is tampered, the offensor needs to calculate the PoW for all the following blocks which is almost impossible. The PoW covers all the data for mining in the block b_i, which is why this process employs adequate time. This PoW is established by resolving a complex mathematical problem that is distinctive to each block of transactions. As each block has a unique mathematical problem, so every miner will strive on a different problem which is unique to the block they constructed and all of these problems are equally difficult to fix. In order to solve this mathematical problem, adequate computational power is required [53]. However, PoW can not be considered ideal for the smart home due to some operations that need to be performed quicker such as light on/off, door lock/unlock. However, PoW is a powerful method that has been proven to achieve the highest level of security in blockchain systems. Therefore, by considering the security measures in a smart home scenario, the difficulty target for PoW is set to 1, which creates an acceptable delay for the smart home operations. When the *SN* receives the command from the authorised user to perform any activity, it finds the blockchain ledger in its database. If the previous ledger is found, *SN* generates block transaction and update the previous ledger; otherwise, *SN* generates new blockchain ledger and create a block transaction. It, then, broadcast a new block to all *SeNs* through P2P server. The SN automatically detects the *SeNs*(miners) based on which *SeN* has strong connectivity and availability.

The *SeNs* validate the new block against the last five blocks in blockchain they previously have. After this process of validation, the *SeNs* will perform mining by finding a hash output for the data in its block for verification with the difficulty target 1. The fulfilment of the block verification process leads all *SeNs* to check the target referenced device in the incoming request. The targeted *SeN* will accept the activity and wait for other *SeNs* for the acknowledgment and will perform the requested action. Fig 2 presents the overall process flow of the transaction verification. Before the transaction goes through the block creation and mining process, the request sent by the user's device is passed through different security checks. This security implementation process on an incoming request has been highlighted with a unique colour in Figure 2. The overall process flow of the proposed architecture has been explained in Section IV-B4.

4) SECURITY IMPLEMENTATION ON INCOMING REQUEST

In order to verify the incoming request from the user's device is the utmost critical phase in the network. Each time the user sends the request to perform any activity, that request will be processed through various security checks to verify that the request has been received from the ultimate source. The first security check is the "firewall deny rule" in the designed system. When the network receives a request, the firewall checks the IP address of incoming request in firewall deny rule. If it is found in the deny list, the firewall will reject the incoming request, and it will not be forwarded for further processing. On the contrary, if the firewall rule check clears and the IP address is not found in the deny list. *SN* then verifies the 'HTTPS header' of the request that makes up of 'X-forward' that contains the IP address of the requester and X-key that contains the unique key of the requester. If any of these properties (X-forward and X-key) in HTTPS header is missing, *SN* will reject the request at this point. Consecutively, *SN* also checks if there are more than two requests within one minute period from the same source, *SN* will identify this request as a suspected request and will immediately block and reject the request by adding the source IP address in firewall deny rule. In contrast, the successful verification of header leads the *SN* to verify the requester's source of truth in its database. SN will check the header property 'X-key' which is the unique key (a combination of user's mobile International Mobile Equipment Identity (IMEI) and system-generated key) in its database. If the request is successful at this stage, it will be forwarded for the decryption process. At this stage, *SN* is expecting the request data in AES256 [54] encrypted form. *SN* checks if an unrecognised encryption method is detected, it will then add the IP address of incoming request in firewall deny rule by executing the iptable command, e.g. iptables -A INPUT -s IP-ADDRESS -j DROP. Upon the successful decryption, the request will be accepted by *SN*, and the block creation process will be started. The overall security check flow of the incoming activity request from the user has been presented in Fig 3.

5) USER AUTHORISATION

The process of user verification as an authorised entity has been described in this subsection. The users are authorised by the *SN* via the RESTful API (Representational State Transfer) [55]. A RESTful API is an application programming interface that promises secure communication over the internet or from one system to another. It utilises REST architectural principles for designing web services. These web services allow the system to access the system's resources by using a predefined set of rules, and these resources can be transferred over HTTPs by various consumers. The RESTful API has been used for the secure communication in our proposed system due the characteristics of its architectural constraints.

There are two kinds of users in the smart home system; Admin user and General user. Admin user is a pre-authorised user who has been initially registered in *SN*. This admin user will have the right to add general users to the smart home network for which, they will have to provide their device's IMEI to the admin user.

Initially, the admin user installs the smart home application as an authorised user and sends the request through the application to add the general users. The application will generate the unique key for that particular user, and that key will be sent to *SN* via the RESTful API. The *SN* will then verify the

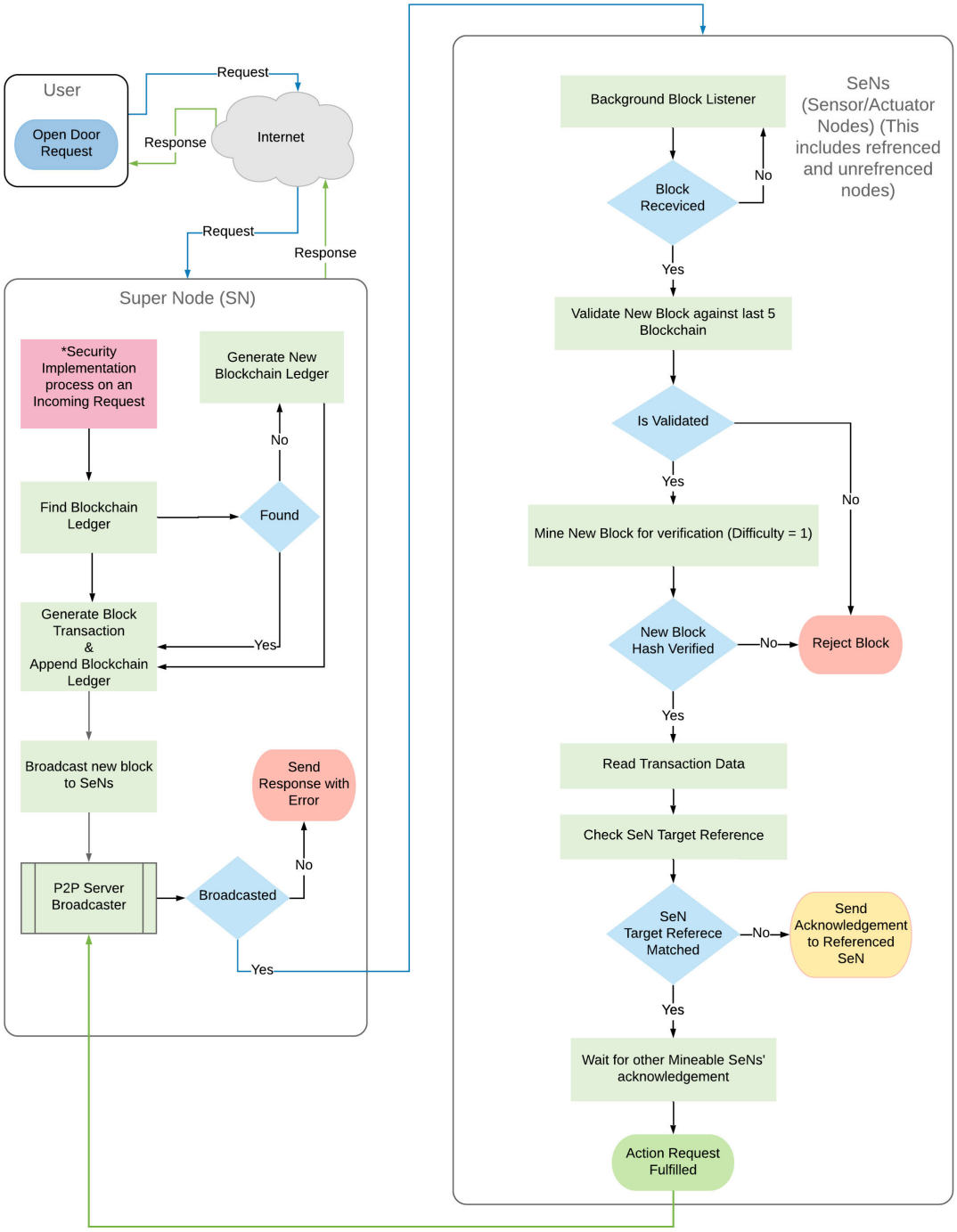


FIGURE 2. **Process flow of the proposed architecture.**

key, and the user will be registered as a new client to the *SN* with its unique identifier. Admin user will provide username and password to the general user for further communication in the smart home network. Each time the *SN* gets any request from the user, that user will be identified with its unique key which is stored in the *SN's* database. Figure 4 represents the process of the user authorisation highlighted in the proposed architecture.

V. HARDWARE IMPLEMENTATION

This section describes the hardware setup for the blockchain implementation by creating a real smart home scenario using four ESP32 devices [56]. As discussed in Section IV, the building blocks of the presented architecture are *SeNs*, *SN*, Blockchain and the Users, however, this experiment implements a fragment of the proposed architecture that only focuses on the blockchain process and block mining time that

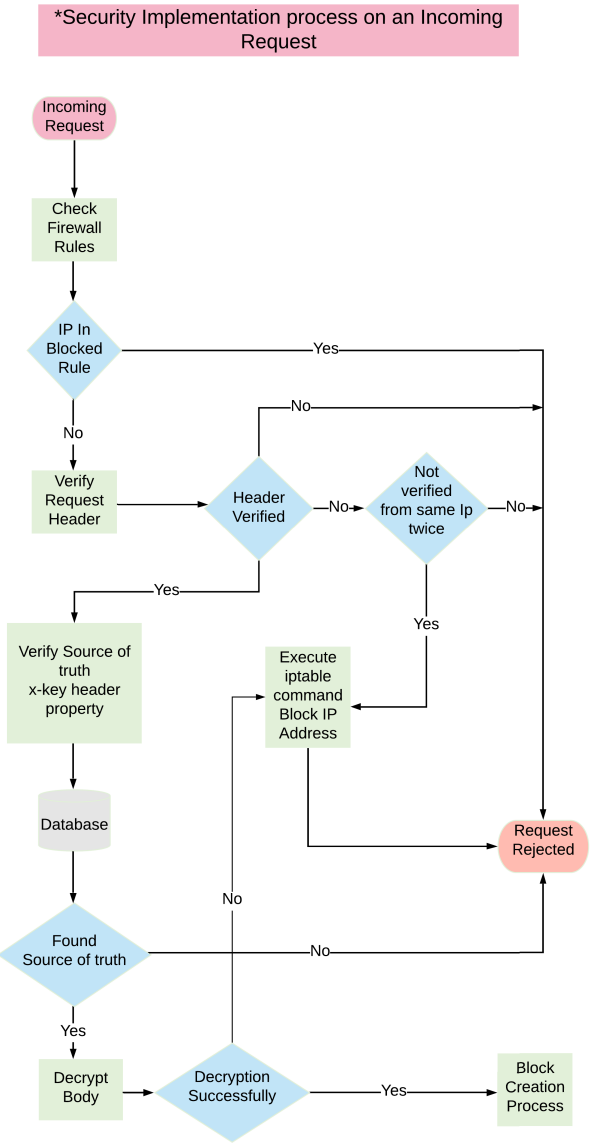


FIGURE 3. Request verification process.

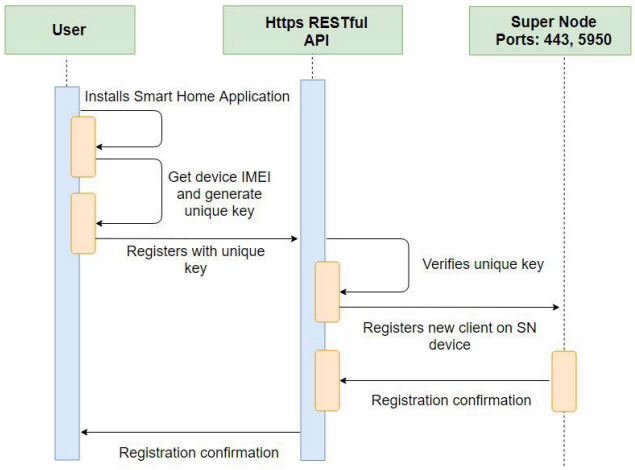


FIGURE 4. User authorisation process.

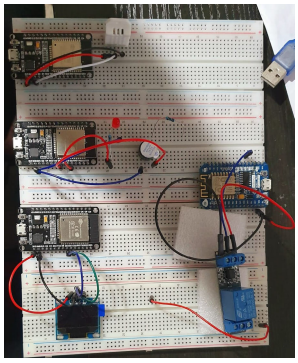


FIGURE 5. Hardware setup for the experiment.

includes *SeNs*, *SN* and Blockchain. This experiment aims to examine the block creation and mining results by observing the block mining time and does not focus on the user authorisation, authentication and the security implementation on the incoming request. For the hardware implementation, a display screen has been used to see the desired responses. A humidity and temperature sensor, buzzer alert, a LED (Light Emitting Diode) and a relay for any electrical on-off device has been used. The combination of these devices is being assumed to be a small smart home. The visual representation of hardware implementation can be seen in Fig 5.

Initially, after the hardware setup, the next step is to write a blockchain code in an appropriate environment for the performance evaluation. For this, Espruino [57] is being used as a Javascript Interpreter. It is a JavaScript Interpreter for Microcontrollers that makes embedded software development quick and easy. It is a very lightweight JavaScript interpreter that runs on the ESP32, and other microcontrollers. In Espruino environment, we created the block and broadcasted it to the *SeNs* through P2P server. The attributes we incorporated in block header for our designed system are as follows:

- **Hash of the previous block -** The block always keeps the hash of the previous block to make the blockchain tamper-proof.
- **Timestamp -** A timestamp has been added in the block to record the event start and finish time in the device/computer and is stored as a log or metadata as temporal information.
- **Nonce -** A nonce is a randomly generated number that is required for the miners as a target value of mathematical calculation to perform PoW.
- **FromDeviceID -** This attribute keeps the address of the source device from where the transaction is coming.
- **ToDeviceID -** This attribute keeps the address of the destination device, i.e. for which SeN, the transaction has been targeted.

As we are making the device as miners, hence, we would have limited computational power, so we tried to make a block in a simplified form and added only the necessary attributes. The body of the block has the action request and the response of the received command. In our blockchain code, the targeted *SeN* is LED and Buzzer as they both are connected to a single ESP32 device. All four *SeNs* are participating in mining. When the block is received by *SN*, it is passed through the verification process performed by SeNs. The targeted *SeN*, i.e. LED and Buzzer, first waits for the acknowledgment of block verification from other *SeNs* and then performs the requested action. The overall blockchain structure that has been created in Espruino using the 'Javascript' language can be found in Fig 6.

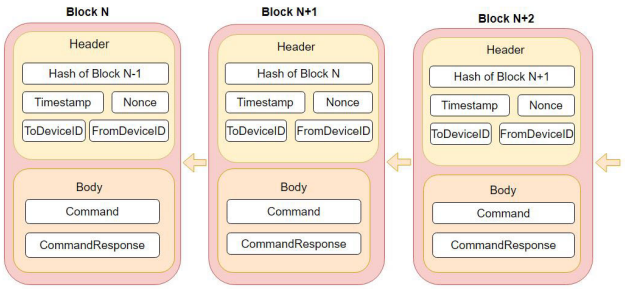


FIGURE 6. Block structure.

VI. RESULTS AND FINDINGS

This section presents the result by performing the experimental tests utilising ESP32 devices for the proposed architecture as explained in Section IV.

We created the block and broadcast to ESP32 device using a local machine, i.e. 3 GHz Intel with 16GB RAM laptop as a P2P server and mined it in ESP32 (*SeN*). According to the architecture, *SN* has the responsibility to create the block and broadcast to *SeNs* for transaction verification. We investigated Raspberry Pi 3 Model B+ [58] to accomplish the duty of *SN* and found as an ideal equilibrium for *SN*. However, the implementation of *SN* will possibly be performed in the next phase of this research. In the experimental testbed, we executed the code that creates a block and provides the time each block takes to mine the SHA256 [59] hash for transaction verification. After completing mining for two blocks per single *SeN*, the result shows that average block mining time taken by each *SeN* is 1 second when difficulty level is set to 1, as shown in Figure 7.

Fig 7 shows that two blocks have been mined. The green highlighted text shows the start time of block one and block two, whereas the text highlighted in yellow displays the completion time of block one and block two. The result we acquired in Espruino after performing the mining of block one and two has been displayed in Unix epoch time. We first converted the Unix time into a human-readable format and subtracted the start time from the completed time to obtain the time taken in mining each block in seconds. Block mining

FIGURE 7. Block mining result (Espruino view).

time in Epoch can also be modified into human-readable time using Epoch and Unix Timestamp Conversion Tool [60]. Similarly, the code has been run by changing the difficulty and the mining time we noted has been recorded in the table 2. This table shows the mining time with different difficulty targets for block 1. The actual difficulty target for the proposed architecture is 1, and fortunately, we acquire the acceptable time delay of approximately 0.9995 seconds per block at difficulty 1, although, increased difficulty leads to the drastic increment in the mining time as presented in Fig 8, thus increases the overall activity response time. According to the graph in Fig 8, the miner consumes 30 seconds at difficulty 2 and 60 seconds at difficulty 3, which are not sufficient for the smart homes.

TABLE 2. The block 1 mining time observed with different difficulty targets.

Difficulty	Mining Time (Seconds)
1	0.9995
2	30
3	60

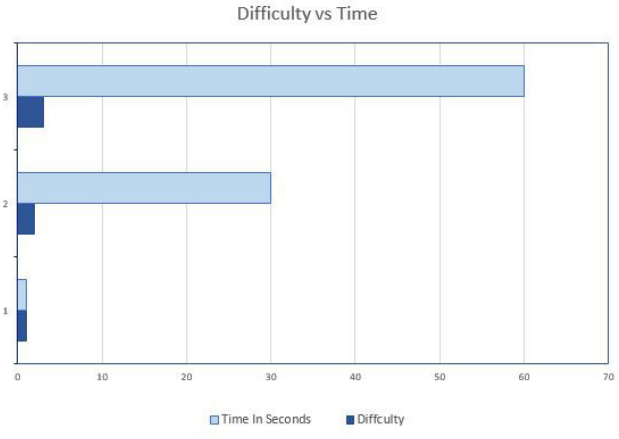


FIGURE 8. Difficulty level vs time taken to complete the transaction.

The results we achieve present the mining time, T_M, for each block by each *SeN*. The equation 3 shows the overall

activity response time, T_R, taken by the connected nodes in the presented smart home system. Due to the participation of SN node in the mining process, an additional delay of 1 seconds are added in the response time, T_R, the time being consumed by SN. The overall activity response time taken by all the nodes in the system can be calculated by using the formula mentioned below in equation 3.

$$T_R = T_M + 0.9995, \tag{3}$$

where T_M is already defined in equation 2.

Using equation 3 and a value of 3 for SeN, the total activity response time can be calculated as:

$$T_R = 0.9995 + (3 * 0.9995\ secs)$$

$\Rightarrow T_R = 4.9975$ secs.

The activity response time T_R we get after the calculation using equation 3 is 4.9975 secs, however, in case of increased devices, the total activity response time may also be increased. Hence, to reduce the activity response time, user can select the number of devices that can participate in mining as discussed in IV-B. The relation between the response time and number of devices can be found in the graph presented in Figure 9.

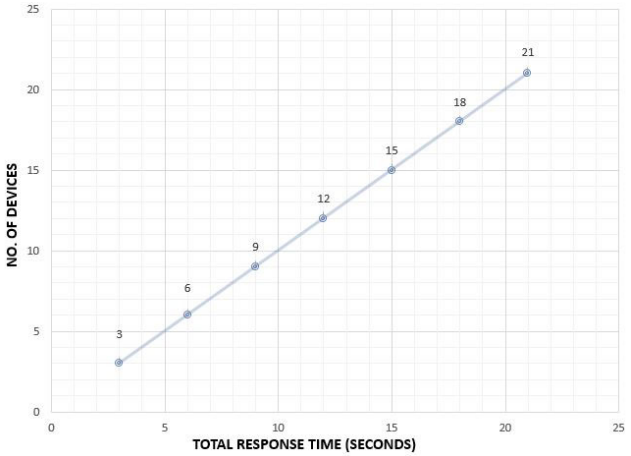


FIGURE 9. Total response time (T_R) vs number of devices.

A. SMART HOME APPLICATION PROTOTYPE

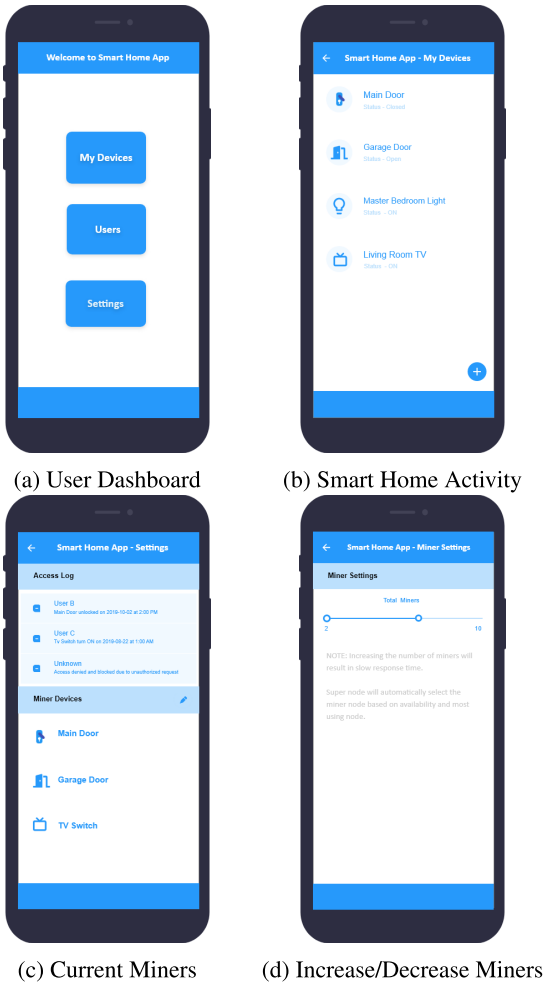
In this technologically advanced and busy era, every homeowner wants to adapt to the automation system. In order to interact with the home appliances through a handheld device, i.e. smartphones or tablets, a user interface is designed that enables the homeowner to efficiently operate and monitor the status of any of the smart product in his living place. For this reason, a user interface is the most significant part of a home automation system. Hence, to realise the necessity of the user interface of the architecture that we described in this paper, we designed a small-scale working prototype for the admin users. In the proposed architecture, the admin user has the following abilities:

- Holds the full rights to access any smart home device and performs an action.
- Changes the miner settings by increasing or decreasing the miner devices according to the security requirements.
- Adds the general users who wants to join the smart home network.
- Holds the right to restrict existing users to perform particular operations in smart homes.

The prototype we designed shows that the admin user has three options: My Devices, Users and Settings, as shown in Figure 10a. When a user selects 'My Devices', the next screen that opens shows the smart devices that are active and the user can perform an action when selects any device, i.e. garage door open/close. The admin user can also add any newly installed smart device in the activity list by tapping on the '+' as seen in Figure 10b. Additionally, the admin user can see the list of other smart home users and their allocated rights to the smart home operations by tapping the button 'Users' and can also cast a new user who wants to join the smart home network and allocates the devices that would be accessible to the new user. The request form of the new user consists of the user's full name, email address, password, device's IMEI and the checklist of devices that would be allocated to the new user. The new user will be able to perform only the permissioned operations. Next, the settings button leads the admin user to change the configuration of the application. This includes accessing and deleting the activity log and increasing or decreasing the number of devices that can participate in mining. As we discussed in Section VI that the increased number of miners can result in increased activity response time; thus, this option has been given to the admin user to update the miner settings according to the user's tolerance of response time. The interface of accessing and updating the number of miner devices can be seen in Figures 10c and 10d.

B. DISCUSSION

Current research clearly shows that employing blockchain itself is a challenge as it is complex to implement and the smart contract based solutions possibly can increase the system cost that motivates us to simplify the blockchain implementation for smart homes. In addition to this, public blockchain architecture is not suitable for use in smart homes, mainly due to its scalability issues as access is open for anyone to join a network;drastically increasing the network overhead. It is due to this extra overhead that the idea of private and consortium blockchain has been considered for the smart home architectures in recent researches as well as in the proposed architecture presented in this paper. Visual outcomes of the implemented architecture represent few issues that highlight the fact that certain aspects must be considered for a reliable implementation of this architecture. One such aspect is to think that the increased number of devices increases the response time that sometimes cannot be tolerable for the



(a) User Dashboard (b) Smart Home Activity

(c) Current Miners (d) Increase/Decrease Miners

FIGURE 10. Smart Home Application Prototype.

smart home user; however, the solution is to limit the device selection. This is directly related to the level of security one wants in the smart home. Secondly, extreme situations where activity requests are sent multiple times at once from a single or multiple users, there would be an obligation to look into the waiting time of the transaction blocks generated by *SeNs*. This situation can occur due to the multiple transactions at a time, and the blocks will be added into the queue [61], waiting for their turn, seemingly increasing the delay in the activity. Let us represent this wait time as T_W, which is a combination of block transmission time (in both forward and backward directions) as well as the processing time, represented by T^f, T^b and T^p respectively. In order to simplify the implementations, we consider $T_W = 0$ in the current work by assuming that the users send a single request at a time. However, in a more realistic implementation of the system, this wait time, T_W should be taken into consideration which is a possible extension of the work presented in this paper. Despite seemingly unpredictable conditions in the proposed architecture, the effectiveness of the proposed scheme cannot be dismissed out of hand as the design has been simplified from the previous architectures, exterminating the use of cloud, reduces the activity response time and lastly providing immutability, integrity, authorisation, authentication, availability and confidentiality due to the implementation of blockchain and consensus algorithm (PoW) and additional security to authorise and authenticate the users and valid incoming request.

VII. CONCLUSION

This article investigated the previous work undertaken on the security of smart homes and undertook the considerations from previous work by presenting a simplistic model to implement a secured architecture that utilises a polished version of the blockchain, i.e. consortium blockchain (a combination of public and private blockchain). The user's performance as a node in blockchain process has been eliminated, instead, the IoT devices perform as miners in the system which makes the system unique with the previously proposed blockchain-based systems. The pre-selected nodes (ESP32 IoT devices) by the home owner in the system have now participated in the block creation and consensus. The *SeNs* communicate with each other through mesh network topology, along with *SN* which performs as a P2P server to broadcast the blocks to other *SeNs* and participates in mining. *SN* also registers and authorises the admin user via the RESTful API and keeps the blockchain storage. A private mechanism has been provided for the user's authorisation and authentication to minimise the user's involvement in blockchain process. Initial security checks have been applied to the incoming request before getting into the blockchain process that ensures the confidentiality and integrity; and the additional security has been implemented through the blockchain process enhancing data privacy and confidentiality alongside providing trusted TXs. The experimental testbed was designed by using ESP32 performing as nodes that are participating in mining; and *SN*'s role was performed via the laptop at this stage, however, during study Raspberry Pi 3b+ was observed better capable of performing as a *SN* due to its superior performance and can further reduce T_R. The time taken by each device to mine a block is approximately 0.9995(1 *second*) at difficulty 1. Due to the limited computational power of the IoT devices, the difficulty has been fixed to 1; however the scheme has been observed with additional two difficulty targets to analyse the difference in the T_R, and this results a drastic and intolerable increment in the T_R. Thus, this scheme seems to be successful implementing in smart homes as it implements a cost-effective secure architecture that is less time consuming and does not require the cloud storage. In the next phase of this study, computational challenges towards the hashing, block queuing and waiting time alongside the relationship between the energy required for solving a problem vs the energy available or required for each node will be investigated. In addition to this, further research will be undertaken by implementing Raspberry Pi 3b+ as a Super Node due to its superior performance capabilities.

ACKNOWLEDGMENTS

The authors would like to acknowledge the support provided by the School of Computing and Mathematics at Charles Sturt University, Australia to conduct this research.

REFERENCES

[1] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, May 26, 2020, doi: 10.1109/COMST.2020.2997475.

[2] *Cisco Visual Networking Index (VNI), Complete Forecast Update, 2017–2022*. Accessed: May 7, 2020. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/1211_BUSINESS_SERVICES_CKN_PDF.pdf

[3] *Competition is Increasing to Be the IoT Gateway to the Connected Home*. Accessed: Jun. 21, 2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2015-08-06-gartner-says-competition-is-increasing-to-be-the-iot-gateway-to-the-connected-home

[4] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of smart home: Privacy and security," *Int. J. Comput. Appl.*, vol. 182, no. 39, pp. 3–8, Feb. 2019.

[5] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[6] T. Alladi, V. Chamola, B. Sikdar, and K.-K.-R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.

[7] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19304194

[8] I. Yaqoob, E. Ahmed, M. H. U. Rehman, A. I. A. Ahmed, M. A. Al-Garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617303468

[9] *Darktrace*. Accessed: Aug. 14, 2019. [Online]. Available: https://www.darktrace.com/en/

[10] I. Ilunin. *IoT Privacy and Security Challenges for Smart Home Environments*. Accessed: Jun. 24, 2019. [Online]. Available: https://hackernoon.com/iot-privacy-and-security-challenges-for-smart-home-environments-c91eb581af13

[11] R. Tzezana, "Scenarios for crime and terrorist attacks using the Internet of Things," *Eur. J. Futures Res.*, vol. 4, no. 1, p. 18, Dec. 2016.

[12] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2017, pp. 1292–1297.

[13] T. A. A. Abdullah, W. Ali, S. Malebary, and A. A. Ahmed, "A review of cyber security challenges, attacks and solutions for Internet of Things based smart home," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 9, p. 139, 2019.

[14] J.-H. Han, Y. Jeon, and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2015, pp. 1116–1118.

[15] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018.

[16] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, 2018.

[17] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S.-U. Rehman, "Blockchain and Internet of Things: A bibliometric study," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106525.

[18] K. Rifat and A. Yurdakul, *IoT Blockchain Integration: A Security Perspective*. Boca Raton, FL, USA: CRC Press, 2020, pp. 29–60.

[19] C. S. Kouzinopoulos, G. Spathoulas, K. M. Giannoutakis, K. Votis, P. Pandey, D. Tzovaras, S. K. Katsikas, A. Collen, and N. A. Nijdam, "Using blockchains to strengthen the security of Internet of Things," in *Security in Computer and Information Sciences*. Cham, Switzerland: Springer, 2018, pp. 90–100.

[20] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[21] P. Rathee, *Introduction to Blockchain and IoT*. Singapore: Springer, 2020, pp. 1–14.

[22] S. Nakamoti. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: May 26, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018.

[24] *Blockchain Technology—Hot Research Topic*. Accessed: Jun. 19, 2019. [Online]. Available: http://linkis.com/Ayjzj

[25] D. J. Yaga, P. M. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8202, 2018.

[26] V. Nehra, A. K. Sharma, and R. K. Tripathi, "Blockchain implementation for Internet of Things applications," in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, ch. 5, pp. 113–132.

[27] DragonChain. *What Different Types of Blockchains are There?* Accessed: Jul. 9, 2019. [Online]. Available: https://dragonchain.com/blog/differences-between-public-private-blockchains

[28] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[29] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019.

[30] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2018.

[31] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications," *Procedia Comput. Sci.*, vol. 98, pp. 461–466, Jan. 2016.

[32] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, Jan. 2020.

[33] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106526. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790618332750

[34] G. Varshney and H. Gupta, "A security framework for IoT devices against wireless threats," in *Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET)*, Aug. 2017, pp. 1–6.

[35] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *Proc. IEEE 6th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Nov. 2017, pp. 454–461.

[36] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. 1st ACM MobiHoc Workshop Netw. Cybersecur. Smart Cities (SmartCitiesSecurity)*, 2018, pp. 1:1–1:6.

[37] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[38] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2017, pp. 1165–1167.

[39] J. Wan, J. Li, M. Imran, D. Li, and Fazal-e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019.

[40] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020.

[41] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–14, Dec. 2020.

[42] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19316280

[43] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, 2019.

[44] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.

[45] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.

[46] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[47] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, and L. Tian, "Improving IoT services in smart-home using blockchain smart contract," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 81–87.

[48] Q. Xu, Z. He, Z. Li, and M. Xiao, "Building an Ethereum-based decentralized smart home system," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1004–1009.

[49] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–18, Apr. 2019.

[50] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving," *IEEE Access*, vol. 7, pp. 62058–62070, 2019.

[51] Y. N. Aung and T. Tantidham, "Review of ethereum: Smart home case study," in *Proc. 2nd Int. Conf. Inf. Technol. (INCIT)*, Nov. 2017, pp. 1–4.

[52] D. Zheng, K. Deng, Y. Zhang, J. Zhao, X. Zheng, and X. Ma, "Smart grid power trading based on consortium blockchain in Internet of Things," in *Algorithms and Architectures for Parallel Processing*. Cham, Switzerland: Springer, 2018, pp. 453–459.

[53] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, pp. 653–659, Sep. 2017.

[54] S. Gueron. *Intel Advanced Encryption Standard (AES) New Instructions Set*. Accessed: Sep. 22, 2019. [Online]. Available: https://www.intel.com.bo/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf

[55] A. Rodriguez. *RESTful Web Services: The Basics*. Accessed: Sep. 22, 2019. [Online]. Available: http://www.gregbulla.com/TechStuff/Docs/ws-restful-pdf.pdf

[56] *ESP32 IoT Development Module*. Accessed: May 4, 2019. [Online]. Available: https://www.espressif.com/en/support/-download/overview

[57] *Espruino on ESP32*. Accessed: Aug. 2, 2019. [Online]. Available: http://www.espruino.com/ESP32

[58] *Raspberry Pi 3 Model B+*. Accessed: Sep. 23, 2019. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

[59] N. T. Courtois, M. Grajek, and R. Naik, "Optimizing SHA256 in bitcoin mining," in *Cryptography and Security Systems*. Berlin, Germany: Springer, 2014, pp. 131–144.

[60] *RESTful Web Services: The Basics*. Accessed: Apr. 30, 2020. [Online]. Available: https://webnet77.net/cgi-bin/helpers/epoch.pl

[61] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in *Computational Data and Social Networks*. Cham, Switzerland: Springer, 2018, pp. 25–40.

SAMRAH ARIF (Graduate Student Member, IEEE) received the Bachelor of Computer Science and Information Technology degree from the NED University of Engineering and Technology, Pakistan, and the bachelor's degree (Hons.) in computing from Charles Sturt University, Australia, where she is currently pursuing the Ph.D. degree. She has previously worked in the industry as a Software Quality Assurance Engineer for a number of years. Her research interests include the Internet of Things, cyber security, and machine learning.

M. ARIF KHAN (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology Lahore, Pakistan, the M.S. degree in electronic engineering from the GIK Institute of Engineering Sciences and Technology, Pakistan, and the Ph.D. degree in electronic engineering from Macquarie University Sydney, Australia. He is currently a Senior Lecturer with the School of Computing and Mathematics, Charles Sturt University, Australia. His broad research interests include future wireless communication technologies, smart cities, massive MIMO systems, and cyber security. He was a recipient of the Prestigious International Macquarie University Research Scholarship (iMURS), and ICT CSIRO scholarships for his Ph.D. degree. He also has the competitive GIK Scholarship for his master's degree.

SABIH UR REHMAN (Member, IEEE) received the bachelor's degree (Hons.) in electronics and telecommunication engineering from the University of South Australia, Adelaide, and the Ph.D. degree in the area of wireless sensors networks from Charles Sturt University, Australia. He is currently a Senior Lecturer and the Course Director with the School of Computing and Mathematics, Charles Sturt University. He has extensive experience in delivering large scale networking solutions along with providing system administration, security and data integration services. His research interests include wireless communication, network planning, routing and switching, and information security. His current research interests include the Internet of Things (IoT), robotics and big data analytics, especially in the domains of intelligent transport systems, environmental sustainability, e-health and precision agriculture, with the aim to positively influence social, economic, and environmental sustainability of communities in rural Australia via digitally enabled solutions. He regularly publishes his research and serves as a Reviewer for a number of respected journals and conferences. He is a member of Australian Computer Society (ACS). He was a recipient of the Competitive Scholarship from Charles Sturt University during his Ph.D. degree.

MUHAMMAD ASHAD KABIR (Member, IEEE) received the Ph.D. degree in computer science from the Swinburne University of Technology, Melbourne, Australia. He is currently a Senior Lecturer in computer science and the Deputy Leader of Data Mining Research Group, Charles Sturt University, Australia. He has published more than 50 peer-reviewed articles. His research interests include data mining, blockchain and security, smart mobile applications, health informatics, human computer interactions, adaptive and context-aware software systems. He is a member of ACM.

MUHAMMAD IMRAN (Senior Member, IEEE) received the Ph.D. degree in information technology from University Teknologi PETRONAS, Malaysia, in 2011. He is currently an Associate Professor with the College of Applied Computer Science, King Saud University, Saudi Arabia. His research interests include the Internet of Things, mobile and wireless networks, big data analytics, cloud computing, and information security. His research is financially supported by several grants. He has completed a number of international collaborative research projects with reputable universities. He has published more than 250 research articles in peer-reviewed, well-recognized international conferences and journals. Many of his research articles are among the highly cited and most downloaded. He has been involved in about 100 peer-reviewed international conferences and workshops in various capacities, such as the Chair, the Co-Chair, and a Technical Program Committee Member. He has served as the Editor-in-Chief for the *European Alliance for Innovation (EAI) Transactions on Pervasive Health and Technology*. He has been serving as an Associate Editor for top ranked international journals, such as the *IEEE Communications Magazine*, the IEEE Network, *Future Generation Computer Systems*, and IEEE Access. He has served/serving as a Guest Editor for about two dozen special issues in journals, such as the *IEEE Communications Magazine*, the *IEEE Wireless Communications Magazine*, *Future Generation Computer Systems*, IEEE Access, and *Computer Networks*. He has been consecutively awarded with the Outstanding Associate Editor of IEEE Access, in 2018 and 2019, besides many others.