Computers, Materials & Continua
DOI:10.32604/cmc.2021.014151
Article

Tech Science Press

OTS Scheme Based Secure Architecture for Energy-Efficient IoT in Edge Infrastructure

Sushil Kumar Singh[1], Yi Pan[2] and Jong Hyuk Park[1,*]

[1]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 01811, South Korea
[2]Department of Computer Science, Georgia State University, Atlanta, GA, 30302-5060, USA
*Corresponding Author: Jong Hyuk Park. Email: jhpark1@seoultech.ac.kr
Received: 02 September 2020; Accepted: 17 October 2020

Abstract: For the past few decades, the Internet of Things (IoT) has been one of the main pillars wielding significant impact on various advanced industrial applications, including smart energy, smart manufacturing, and others. These applications are related to industrial plants, automation, and e-healthcare fields. IoT applications have several issues related to developing, planning, and managing the system. Therefore, IoT is transforming into G-IoT (Green Internet of Things), which realizes energy efficiency. It provides high power efficiency, enhances communication and networking. Nonetheless, this paradigm did not resolve all smart applications' challenges in edge infrastructure, such as communication bandwidth, centralization, security, and privacy. In this paper, we propose the OTS Scheme based Secure Architecture for Energy-Efficient IoT in Edge Infrastructure to resolve these challenges. An OTS-based Blockchain-enabled distributed network is used at the fog layer for security and privacy. We evaluated our proposed architecture's performance quantitatively as well as security and privacy. We conducted a comparative analysis with existing studies with different measures, including computing cost time and communication cost. As a result of the evaluation, our proposed architecture showed better performance.

Keywords: Blockchain; energy-efficient IoT; ots scheme; edge infrastructure; security and privacy

1 Introduction

In today's era, the rapid advancement of the Internet of Things (IoT) and Information Communication Technologies (ICT) is translating into intelligent services for daily human life in sustainable computing with smart applications, including advanced manufacturing, smart vehicles, and others [1]. Billions of physical devices worldwide connected in different topological ways to the Internet are known as IoT. Technologies include Radio Frequency Identification (RFID), Network Information Card (NIC), Wireless Fidelity (Wi-Fi), and Access Points (APs). It provides a large number of intellectual services for edge infrastructure in smart city applications. These cities are entirely dependent on multiple communication perspective computing (Cloud, Fog, and Edge) wherein data are exchanged in heterogeneous mode, offering a

distributing environment [2]. It has the various advantages of technological advancements, such as manufacturing and distribution of IoT data according to different smart cities' criteria. Still, it has multiple challenges, including big data, greenhouse gas emissions, consumption of non-renewable data, and others. The number of IoT devices is forecast to reach 41.6 billion, with 79.4ZB data expected to be generated by 2025, according to International Data Corporation's (IDC) forecast report [3].

To address these challenges, energy-efficient IoT is utilized because IoT is transforming into G-IoT (Green Internet of Things) nowadays. It is the combination of IoT, G-Tech (Green Technology), G-Eco (Green Economy), and G-Net (Green Networking). With the adoption of G-Tech, sustainable designing, and manufacturing, smart factories increase productivity day by day [4]. A user-friendly environment is developed in smart industries, based on R^5 factors such as Reduce (fuels, energy), Renew (electricity, wind and water power), Recycle (paper, plastic, battery cells), Responsibility, and Refuse (do not use unwanted things). Green economy means reducing the smart city's risk through the green development of ecological economies. G-Net has a vital role in deploying IoT applications, minimizing operational costs and power consumption with decreased pollution and maximizing environmental conservation [5].

G-IoT also uses communication technologies such as Green Radio Frequency Identification (G-RFID), Green Wireless Sensor Network (GWSNs), Green Data Center (GDC), Green Base Stations (GBS), Green Machine-to-Machine (GM2M), and others [6]. Routray et al. [7] discussed the five-layer G-IoT architecture: Physical layer, MAC layer, Radio link control layer, Packet data convergence layer, and No-access stratum layer. There are various advantages of G-IoT with regard to edge infrastructure in a smart city such as enhancing energy efficiency, reducing carbon emissions, decreasing resources and pollution, minimizing environmental degradation, and improving productivity. Still, there are many challenges in G-IoT, such as centralization, latency, networking, security, and privacy. IoT sensor devices are increasing continuously; various cyber-attacks such as optimal Green Hybrid attack, DDoS and Hacking attacks are also growing, harming Green IoT applications. Various next-generation industries (financial companies) have to invest 10% of their total ICT budget in addressing and preventing network and security threats for G-IoT [8]. The comparison of the proposed layered architecture and the existing research is shown in Fig. 1.

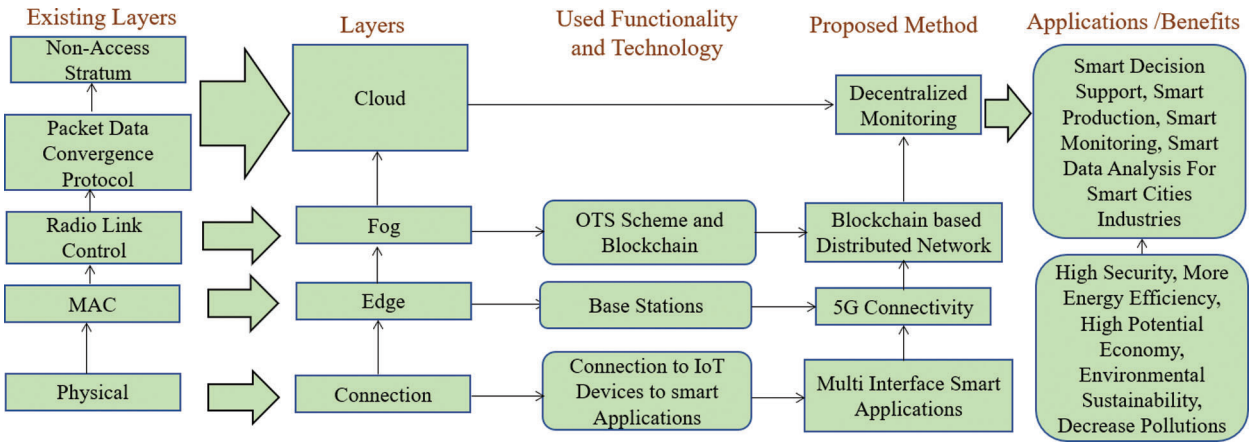

Figure 1: Comparison of proposed layered architecture to existing research

To resolve G-IoT's issues, we can deploy the new advanced, high-demand technology, called Blockchain. As a widely used technology for security purposes in the advanced applications of smart cities nowadays [9], it supports essential properties like digital integrity, distributed ledger, and decentralization for secure advanced city infrastructures [10,11]. Thus, it offers the opportunity for radically changing and improving data security in many use cases by enabling trusted architecture.

Blockchain is the collection of blocks, each of which is linked to the previous block with a hash pointer. Each block has transaction data, timestamp, last hash value, and own hash value. To verify and validate transactions, miner nodes provide security and privacy for data in a smart city edge environment [12]. To provide more secure infrastructure in IoT applications, Shu et al. [13] proposed a digital signature scheme-based hash function. They prevent key exchange with the elliptic curve discrete logarithmic algorithm (ECDLA) and subsequently create a hash function, proving reliability in IoT applications. Based on this scheme, it supports authentication, non-repudiation, and integrity. Still, this scheme has a drawback: the key and signature sizes are too large here, so they cannot be used in space-critical applications in a smart city [14–17].

The OTS scheme has a substantial role in determining the size of keys and signature. Second, the hash-based signature scheme cannot be utilized in blockchain technology. Thus, we introduced four layer-based secure architecture, which uses the OTS scheme-based Blockchain at the fog layer and provides more security in a smart city. OTS means one-time signature, and it is part of cryptography. The main purpose of the OTS is to provide more security and privacy. Nowadays, the latest methodology uses a green environment such as energy-efficient infrastructure in smart city applications [18–21]. Thus, energy-efficient, secure architecture in edge infrastructure is proposed with the fusion of the OTS scheme and Blockchain technology.

This paper addresses the issues of security and privacy, centralization, and communication bandwidth by using the proposed OTS scheme-based secure architecture for Energy-Efficient IoT in Edge Infrastructure.

Research contribution: The following are the main contributions of this paper:

- Propose OTS Scheme-based Secure Architecture for Energy-Efficient IoT in Edge Infrastructure.
- OTS-based Blockchain provides more security in a distributed manner with key generation, signature generation, and signature verification for Edge Infrastructure in smart city applications.
- Evaluate the performance of the proposed architecture in terms of computing and communication costs for advanced applications.
- We compare our proposed work with the existing research studies quantitatively and in terms of security and privacy by performing comparative analysis.

The rest of this paper is organized as follows: Section 2 discusses the seminal contributions for Green IoT in advanced smart city applications; in Section 3, we propose the OTS Scheme-based Secure Architecture for Energy-Efficient IoT in Edge Infrastructure; we assess the computing and communication cost through quantitative analysis in Section 4 to evaluate the performance of the proposed architecture in terms of security and privacy and perform comparative analysis; finally, Section 5 presents the conclusions of our paper.

2 Related Work

In this section, we discuss the seminal contribution of the existing research studies with regard to Energy-Efficient, IoT-related sustainable smart cities applications and address centralization, communication bandwidth, security, privacy, and other challenges. The basic and essential purpose of Edge Infrastructure in smart city applications is to provide a reliable, trustworthy environment for the smart city with the help of advanced technologies, services, rules, and regulations.

2.1 Seminal Contribution

For the deployment of greenery in IoT infrastructure, Kim et al. [22] proposed an empirical model of the Blockchain of Things (BoT) to overcome the security vulnerability of existing IoT devices such as airplanes, automobiles, and CCTV in the sensor multiplatform by the radix of the blockchain core algorithm and

multiple-agreement algorithm. Nonetheless, it has some issues with regard to IoT networks such as authentication of IoT devices collected by the IoT gateway through LAN. Kaur et al. [23] designed Green IoT architecture for reducing the energy utilization of IoT smart city applications. It is based on a cloud system that is used for decreasing hardware consumption, but the security vulnerability issue is not resolved. Yang et al. [24] introduced an AI-enabled cloud data center for a green cloud and studied about timing control and refrigeration engine intelligently. It realized low consumption of energy and high efficiency intelligently for IoT applications, but it has some limitations such as AI-enabled networking like edge computing, caching, and offloading for a greener environment.

Sukjaimuk et al. [25] proposed a congestion control mechanism to mitigate the congestion rates of the network for Green IoT Sensing devices. It reduced sensor efficiency consumption and increased network performance for Green, Efficient, Information-Centric, Networking-based Green IoT Sensor. Overall network efficiency for various topological structures is a major issue, which is not covered by this research. For the improvement of quality of experience (QoE) in the content-centric computing system for IoT users, He et al. [26] proposed QoE models as well as a sub-optimal dynamic approach to evaluate the qualities of IoT users and networks based on green resource allocation with deep reinforcement learning. They did not address the continuous increase of IoT devices and network, security, and privacy issues, aiming only aims at the enhancement of the quality of experience.

Patil et al. [27] provided a lightweight blockchain-based secure framework for smart greenhouse farming to provide security and privacy. The private immutable ledger in blockchain optimized energy consumption and secured communication with each other. Singh et al. [28] presented Blockchain and Fog-based secure architecture for the Internet of Everything (IoE) in smart cities. This architecture maintained properties such as sensitive data encryption, authentication, and reduced latency and energy. Shaikh et al. [29] provided various G-IoT approaches with communications services and others. They also addressed various challenges for G-IoT, such as large data, energy efficiency, latency, scalability, security, and privacy. Linde et al. [30] constructed a secure signature scheme to integrate hash-based one-time signature scheme and blockchain technology and compared it with the traditional system. Nonetheless, it has stateful properties and requires storage, and backup for advanced application requirements leaves a lot to be desired.

2.2 Needs Addressed by the Proposed Architecture

For effective and secure environments in smart applications, the proposed architecture considered five security threats for Energy-Efficient IoT in a smart city for Edge Infrastructure:

- Mismatched security policy: An attacker can access the IoT and control entities easily via a less secure environment because of the various security protocols used in different layers in the system.
- DoS attack: An attacker launches a DoS attack on physical services to exhaust the available network resources for other devices in the G-IoT infrastructure. With the DoS attack, an attacker can launch an attack easily on a virtualized platform system.
- Impersonation attacks: An attacker can pose as a physical platform to allocate unavailable IoT resources. Moreover, an attacker can masquerade as a G-IoT controller to steal network resources.
- Hypervisor attacks: An attacker can achieve attacks with respect to the hypervisor to jeopardize the virtualization of IoT device resources in the Green IoT infrastructure. These attacks cause software-based errors in the hypervisor.
- Side-channel attacks: An attacker can easily access one IoT device and attack the set of IoT devices sharing the same primary hardware resources.

Based on the analysis of research studies, this study focused on the five-layer architecture for Green IoT in smart city applications with energy efficiency, latency, and other issues. Note, however, that such existing methodologies have various limitations, such as networking, centralization, communication bandwidth,

security, and privacy. Thus, we provided four layers based on secure architecture with OTS-based Blockchain used at the fog layer.

3 Proposed OTS Scheme Based Secure Architecture for Energy-Efficient IoT

The previous research proposed a Green environment for the smart city with IoT-oriented infrastructure. Nonetheless, it has various considerations such as communication bandwidth, security, and privacy for advanced applications of a smart city. Therefore, we present the OTS scheme-based secure architecture for energy-efficient IoT in the smart city for edge infrastructure to address issues, including security, privacy, and communication and computing cost. The OTS scheme has three functions: Generate Keys, Generate Signature, and Signature Verification. This scheme is utilized in the Blockchain for creating the Blocks' hash values. With the integration of the OTS scheme and Blockchain, the proposed architecture offers more security and privacy for Energy-Efficient IoT applications in Edge Infrastructure.

3.1 Design Overview of the Proposed Architecture

The design overview of the proposed architecture for Energy-Efficient IoT in Edge Infrastructure is shown in Fig. 2. It has four layers: (1) Connection layer; (2) Edge layer; (3) Fog layer; and (4) Cloud layer. The connection layer is used as a physical layer as well as for monitoring of IoT device for smart applications, including smart manufacturing, and many more. It also provides filtered data and connection between IoT. This data is forwarded to the edge layer with 5G connectivity. Access and Core Network provide such connectivity with the help of user plane and control plane functions (UPF, CPF). Many responsibilities, including network functionality, Quality of Services (QoS), controllability, and stability of the applications, are provided by the user plane and control plane. Various base stations and switches are available at the edge layer, which is utilized for providing a multi-interface network with smart applications. It is also used for providing the best route and communicating with the fog layer. We deployed multi-interface smart applications (SA1, SA2, SA3….) and established a communication relationship between IoT devices and advanced applications.

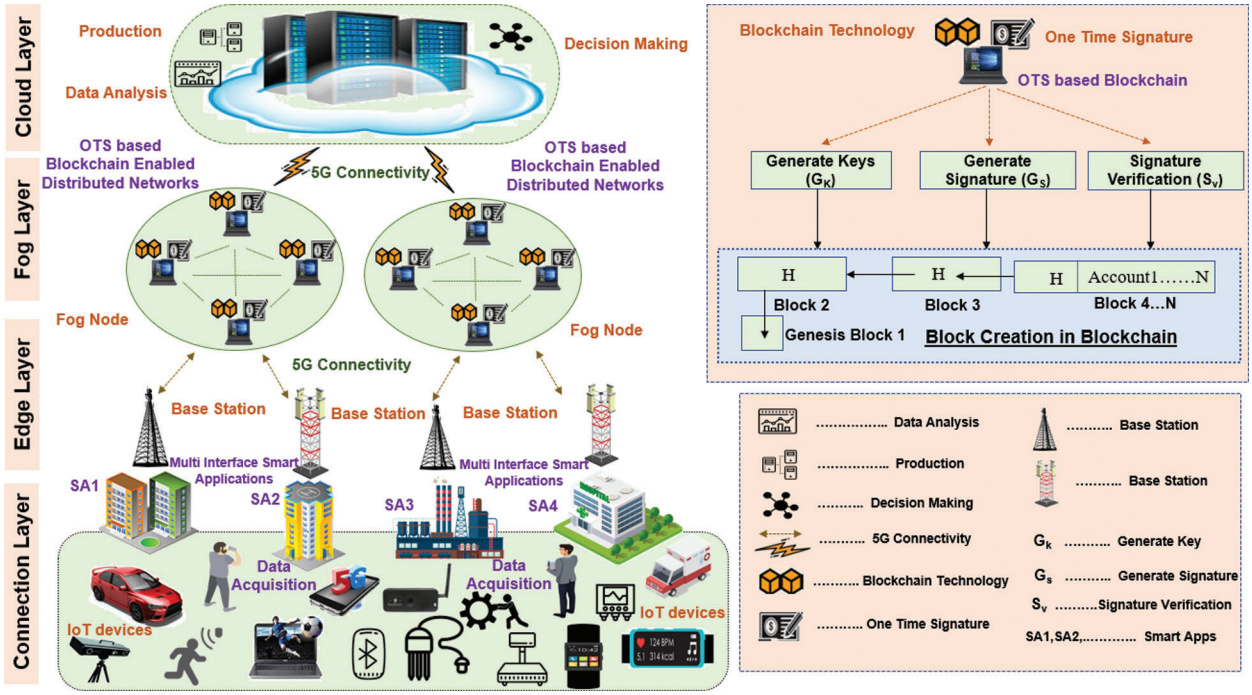

Figure 2: Design overview of the proposed architecture for energy-efficient IoT in edge infrastructure

In the Fog layer, we used the OTS scheme-based Blockchain for security and privacy purposes. Blockchain technology is known to be used for secure IoT-oriented infrastructure. By employing the blockchain, an untrusted individual manufacturer can link together with an associate in a peer-to-peer network and transfer data in a verifiable manner without the aid of a trusted intermediary. For enhanced security, however, we are using the OTS scheme-based blockchain at the fog layer, and we have developed distributed networks between various fog nodes. By leveraging the OTS scheme and Blockchain technology, we provide more security and privacy and incur low computing and communication cost for Energy Efficient-IoT in Edge Infrastructure for a smart city. On the cloud layer, data analysis, production analysis, and decision-making functions are provided in a decentralized manner with the help of the data center. Blockchain is responsible for the scalability and analysis of data. The cloud layer consists of large-capacity storage space, and high-performance servers equipped with processing capabilities. It also automatically provides various application services for smart cities, including smart industries such as management, configuration, distribution, and decision support.

3.2 Methodological Flow of Proposed Architecture with OTS Scheme-Based Distributed Blockchain

This subsection provides the methodological flow of the proposed architecture with the OTS scheme-enabled distributed blockchain network. It is categorized into three parts: data acquisition, data conversion, and OTS scheme-based blockchain-enabled distributed network. The first part, data acquisition is conveyed at the connection layer, and data conversion is realized at the edge layer, with the OTS scheme and blockchain concept employed at the fog layer of the proposed architecture. It has various advantages, including distributed and decentralized secure transactions between manufacturer, transparency, decentralization, trustworthy environment, and others. The OTS scheme offers more security and privacy with blockchain networks. The methodological flow of the proposed architecture with the OTS scheme-based distributed blockchain is shown in Fig. 3.

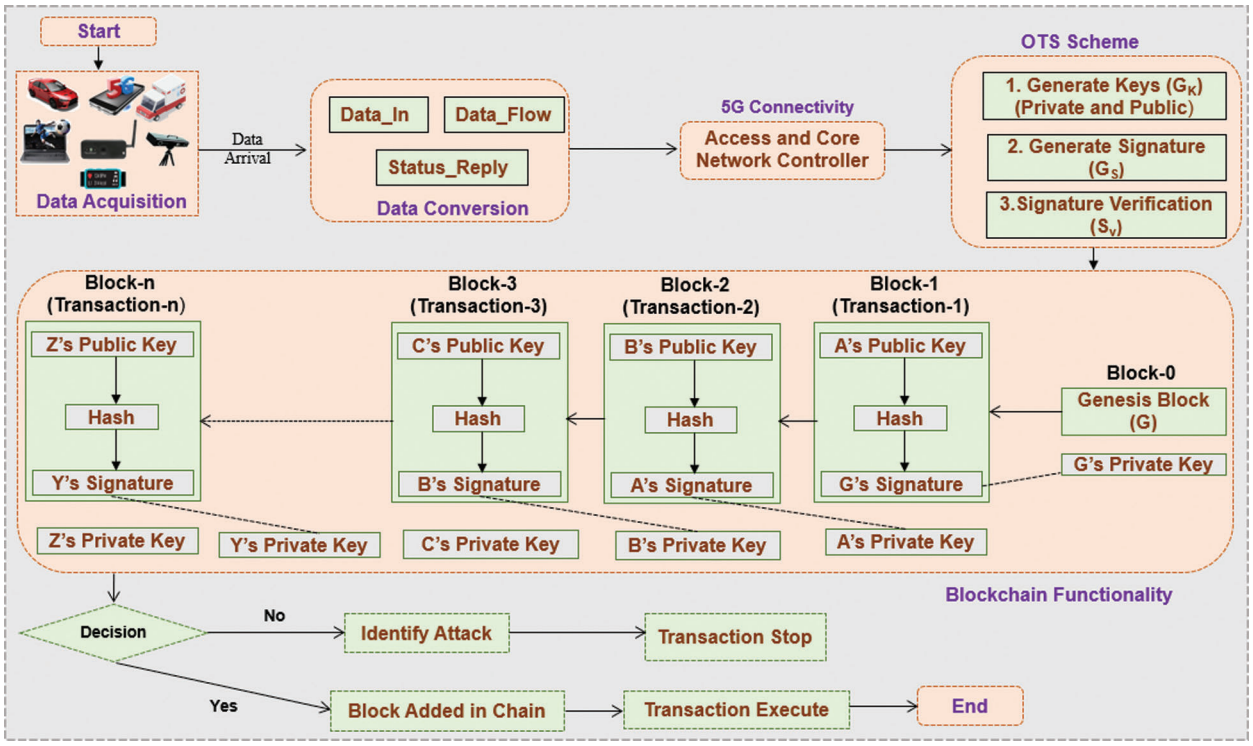

Figure 3: Methodological flow of proposed architecture with OTS scheme-based distributed blockchain

Data Acquisition: Data acquisition is the essential and primary task of the proposed architecture. Used at the first layer, called the connection layer of Energy-Efficient IoT, it gathers the raw industrial data from various IoT devices, including flow meter, smartwatch, smart vehicles, and healthcare assets according to advanced applications such as smart manufacturing, smart vehicles, and smart grid. Improved sustainability, economic development, enterprise resource planning, and manufacturing execution are the functions of the smart city realized by IoT devices. In the proposed architecture, a different type of IoT device connects to multiple smart applications (SA_1, SA_2, SA_3,…). These applications collect IoT data such as the speed of vehicles, temperature, disease parameters, manufacturing details, pressure, network data rate, and others. The automatic collection of data from IoT devices is a function provided by IoT technology. These data then communicate with the edge layer where various base station switches and gateways are available, offering receiver/transmitter services for the communication.

The data conversion function is also used in this layer. It provides useful information from raw data with the help of Data_In, Data_Flow, and Status_Reply functions, which offer the needed information for smart applications. The data conversion is also part of Green-IoT. For 5G connectivity, we are using access and core network controller between layers of the proposed architecture. It is categorized into two parts: (1) UPF (user plane function) and (2) CPF (control plane function). UPF performs various tasks such as traffic reporting and data forwarding in the network in a 5G environment. CPF also has some services like session management, policy control, mobility management, network selection, and authentication server. At present, information is communicated to the upper layer, called the fog layer. In this layer, we utilize an OTS scheme based blockchain-enabled distributed network. A list of abbreviations with all descriptions is provided in Tab. 1.

Table 1: List of abbreviations

Abbreviation	Description	Abbreviation	Description
$\{SA_1, SA_2, SA_3\}$	Smart applications notation.	$h = h_{hd}$	Hexadecimal Symbols.
G_k	Generate keys.	T	Summation of digits, $Summation\_String\_index_i$
G_{pr}	Private key.	V	Final Hash Output.
G_{pub}	Public key.	S_V	Signature Verification.
G_s	Generate signature.	$F\partial$	Forward Signature.
M	Parameters of keys.	$B\partial$	Backward Private Signature.
m	Smart application information.	FG_{pr}	Forward Private Sign.
α_{OTS}	Size of keys.	BG_{pr}	Backward Private Sign.
∂	Signature	V_k	Verification Key.
$\{Z, Zf, Zt, Zu, Zy\}$	Four parts division of private key.	L	Summation of 16 different String List

OTS Scheme Based Blockchain-Enabled Distribution Network: In this subsection, we show the OTS scheme-based blockchain-enabled distribution network. As a distributed ledger system that promotes decentralization, transparency, and digital integrity, blockchain technology follows the rules and regulations of the OTS scheme such as key generation, signature generation, and signature verification and provides a distributed network. Thus, it is called the OTS scheme based Blockchain. It is mainly

used for security purposes in smart city applications for Edge Infrastructure. In the blockchain, digital assets are distributed rather than copied or transferred. These assets are decentralized, maintaining the property of distributed networks in the Blockchain. Fig. 3 shows the blockchain functionality with the OTS scheme, where various blocks, named A to Z are connected to each other as a series of information transactions. If A wants to send the information to B, then A must follow the condition that A will use its own private key to sign the hash of transaction 1 and B's public key. Similarly, B, C, D, …, Z maintain this property. If it is OK, then add a block in the blockchain network, and the transaction is executed easily; otherwise, identify the malicious data and stop the transaction in the network.

The OTS scheme has three parts: (1) Generate keys G_k (Private G_{pr} and Public G_{pub}); (2) Generate Signature Gs; and (3) Signature Verification S_v. Hash-based signature has the drawback of generating large keys and signature, so this cannot be used in the blockchain technology. Therefore, we are proposing an OTS scheme-based blockchain. In this scheme, we utilized a bunch of information instead of large-size information. The proposed scheme uses 4-bit long bunches of information for the Blockchain network. Eqs. (1) and (2) are used for calculating the size of keys and signature, respectively.

$$\alpha_{OTS} = 2^n \tag{1}$$

$$\alpha_{OTS} = p \tag{2}$$

$$\text{Size of Keys and Signature have the relation, Signature Size} = 2 * \text{Key Size} \tag{3}$$

If key Size = 256 bits, then Signature Size = 512 bits, which is smaller than the Hash-based signature scheme. The signature size is 512 bits long so security parameter M = 512.

A scheme is defined as a triple algorithm (G_k, Gs, S_v) for Information m (which is often defined as the output range of the hash function), which is offered in the Blockchain network in a smart city.

G_k = generates a key pair (G_{pr}, G_{pub}) given security parameter M;

M = Parameters: size of private key, public key, signature elements, and others.

Gs ($G_{pr,}$ m) = creates signature ∂ on m using secret key G_{pr}.

S_v($G_{pub,}$ ∂, m) = returns 1 if ∂ is a valid signature on message m for public key G_{pub}.

For all (G_{pr}, G_{pub}) ← G_k and all information m, every signature ∂ ← Gs ($G_{pr,}$ m) can be verified with S_v(G_{pub}, ∂, m) = 1. The generation of keys, generate signature, and signature verification are discussed below.

Algorithm 1: Generate Keys G_k *(Private* G_{pr} *and Public* G_{pub}*)*

Input: Provide security parameters (M = 512) in the Blockchain network.

Output: Create keys G_k, it is the combination of G_{pr}, G_{pub}.

$G_{pr}[\,]$, $G_{pub}[\,]$

Process:

1: part ← *Random_Value* (512*bits*); /* Divide Random Values

2: A ← $SHA_{512}(part)$ *and* $G_{pr} = [\,]$; /* Private Key Initialization

3: **for** $\mathbf{x_{0\rightarrow 15}}$

4: **do**

5: $G_{pr}.merge(A)$, $A \leftarrow SHA_{512}(A)$;

(continued).

6: ***end for***

7: $G_{pub} = [\,]$; /* Public Key Initialization

8: ***for*** $\boldsymbol{x}_{0\rightarrow 15}$

9: ***do***

10: $Z \leftarrow G_{pr}[x], Zf \leftarrow Z[0:127], Zt \leftarrow Z[128:255]$; /* Divide private keys into four parts.

11: $Zu \leftarrow Z[256:383], Zy \leftarrow Z[384:511]$

12: ***for*** $\boldsymbol{y}_{0\rightarrow 128}$

13: ***do***

14: $Zf \leftarrow SHA_{256}(Zf), Zt \leftarrow SHA_{256}(Zt), Zu \leftarrow SHA_{256}(Zu), Zy \leftarrow SHA_{256}(Zy)$

15: ***end for*** $G_{pub}.merge(Zf, Zt, Zu\ and\ Zb)$

16: ***end for***

Generate Keys G_k (Private G_{pr} and Public G_{pub}): Every block has four types of information in the blockchain networks: previous has value, own hash value, timestamp, and data. The hash value is dependent on private and public keys. Private keys are the collection of 16 values (2^4), each of which is 512 bits long [18].

$$G_{pr} = \sum_{i=0}^{15}\left\{ g_{pr_{k_i}}.bitlength\left(g_{pr_{k_i}}\right) == 512\right\} \tag{4}$$

We can apply a hash chain to generate a private key value (g_{pr_k}). During signature verification in Blockchain, private key values are not disclosed, so it is secure. The calculation of public keys (G_{pub}) is dependent on the value of private key G_{pr}. For the computation of public keys, we divide private key values g_{pr_k} into four parts for Blockchain [18].

$$Values\ of\ g_{pub} = Values\frac{g_{pr_k}}{4} = \frac{512}{4} = 128bits \tag{5}$$

$$G_{pub} = \sum_{i=0}^{15}\left\{ g_{pub_{k_i}} = SHA256^{128}\left(g_{pr_{k_i}}\left(0, \frac{g_{pr_{k_i}}}{4}\right)\right)\right\} \tag{6}$$

$$G_k = G_{pr} + G_{pub} \tag{7}$$

Algorithm 2: Generate signature G_s

Input: Provide private key Gpr and Smart application Information m for Blockchain Networks.

Output: Find the Signature $\partial[\,]$.

Process:

1: h $\leftarrow SHA_{512}(m)$, $h_{hd} \leftarrow$ *Hexdecimal Symbols*

2: $string_{index}[\,]$

3: hexadecimal symbols ← according to the smart application information m.

2: ***for*** *hexadecimal symbols*

5: ***do***

6: *String* ← ″ ″;

7: ***for*** $\boldsymbol{x}_{0\rightarrow 127}$

8: ***do***

9: ***if*** $h_{hd}[x] =$ = hexadecimal symbols;

10: ***then*** *String* ← *String* + *x*;

11: ***endif***

12: ***endfor***

13: $string_{index}$ .merge(*string*); /* Merging all strings

14: ***endfor***

15: *Summation_String_index*[];

16: ***for*** $(string_{index})$

17: ***do*** $(Summation \leftarrow 0)$

18: ***for*** $(x\ in\ string_{index})$

19: ***do*** $Summation \leftarrow Summation + int\ (x)$

20: ***endfor***

21: *Summation_String_index.merge*(*Summation*); /* Sum of Index string values

21: ***endfor***

22: $\partial[\,]$;

23: ***for*** $x_{0\rightarrow 15}$

24: $Z \leftarrow G_{pr}[x],\ Zf \leftarrow Z[0:127],\ Zt \leftarrow Z[128:255],\ Zu \leftarrow Z[256:383],\ Zy \leftarrow Z[384:511];$ /* Divide four parts of element

25: ***for*** $f = 1 \rightarrow Summation\_String\_index[x]$

26: ***do*** Zf ← $SHA_{256}(Zf)$

27: ***endfor***

28: ***for*** $y_{0\rightarrow(128-Summation\_String\_index[x]}$

(continued).

29: ***do*** $Zy \leftarrow \mathrm{SHA}_{256}(Zy)$;
30: ***endfor***
31: $\partial i.merge(Zf, Zt, Zu, Zy)$;
32: ***endfor***

Generate Signature G_s: The signer has a huge responsibility; it follows some steps and generates a signature for the Blockchain network. For this purpose, the hash of the information (h) is first computed, and we used the SHA-512 hash function with Eq. (8) (h has a total of 128 hexadecimal symbols).

$$h = h_{hd} = 128\ Hexadecimal\ Symbols \tag{8}$$

h_{hd} is dependent on string_index_list (16 different strings). It is denoted by L with Eq. (9).

$$L = \sum_{i=0}^{15} string_{index_i} \tag{9}$$

Then, the signer (Miner Node) calculates the summation of the digits (Summation_string_index) in every string_index with Eq. (10) [18]:

$$T = \sum_{i=0}^{15} Summation\_String\_index_i = digit_{Summation\_String\_index_i Summation(String\_index_i)} \% 128 + 1 \tag{10}$$

Finally, with the help of Summation_string_index, the signer produces signature ∂ according to information (m), which is collected by the edge node of the proposed architecture. The signer (Miner Node) then computes the hash of every private key value (G_{pr}). It is equal to Summation_string_index.

With Eq. (11), the signer will generate the final hash outputs with individual signature. It is denoted by V and is the combination of two forward private sign FG_{pr} and two backward private sign BR_{pr} [18].

$$V = \sum_{i=0}^{15} \{\partial_i = SHA_{256}^{Summation\_String\_index_i}\ (g_{pr_{k_i}}[0, \frac{g_{pr_{k_i}}}{2}]) + SHA_{256}^{129-Summation\_String\_index_i}(g_{pr_{k_i}}[\frac{g_{pr_{k_i}}}{2}, g_{prki}])\} \tag{11}$$

Example:

We have a hash of information h with hexadecimal symbols according to Eq. (8).

H = 678abc1234808de3457f490....	**0**.....**0**.....**0**.....**0**.....				9f123.....	(128_hd)
index	12	23	78	91	98	119
$string_{index_i}$	12	23	78	91	98	119

$$Summation\_String\_index_i = (1+2+2+3+7+8+9+1+9+8+1+1+9)61\%128+1 = 62$$

$$\partial_i = FG_{pr_i}(0:127)^{62},\ FG_{pr_i}(0:127)^{128-62=66}\ ||BG_{pr_i}(256:383)^{62}, BG_{pr_i}(384:511)^{128-62=66}$$

Signature Verification S_V: The next step of the OTS scheme is signature verification (S_V) in the Blockchain network for a smart city. $S_v(G_{pub}, \partial, m)$ returns the value of 1 if ∂ is a valid signature on

message m for public key G_{pub}. For this verification, the verifier *(Miner Node)* computes the Summation_string_index values according to the same step above (*Generate signature Gs*). The verifier (Miner Node) verifies the signature by more than 50% and generates verification key (V_k) with the help of signature, a combination of two forward signatures (F∂), and two backward signatures (B∂). Eq. (12) shows the signature verification process. Finally, the verifier compares his/her own verification key with the signer public key. If it is equal to 1, the signature is accepted [18].

$$V_k = \sum_{i=0}^{15}\{V_{ki} = SHA_{256}^{128-Summation\_String\_index_i}\left(\partial_i\left[0,\frac{\partial_i}{2}\right]\right) + \mathrm{SHA}_{256}^{Summation\_String\_index_i}\left(\partial_i\left[\frac{\partial_i}{2},\partial_i\right]\right)\} \tag{12}$$

Algorithm 3: Signature verification Sv

Input: Provide S_v (G_{pub}, ∂, m) public keys, Signature, and smart application's information.

Output: Check whether the Signature is valid or not.

Process:

1: According to the Algorithm 2 use Summation_string_index list and $V_k[\,]$;
2: ***for*** $x_{0\to 15}$
3: ***do*** $A \leftarrow \partial[\mathrm{x}])$ /* Signature Verification with public key computation by Miner Nodes
4: $Af \leftarrow A[0:127],\ At \leftarrow A[128:255],\ Au \leftarrow A[256:383],\ Ay \leftarrow A[384:511]$ /* Divide four parts of signature element
5: ***for*** $f_{0\to(128-Summation\_String\_index[x]}$
6: ***do*** $Af \leftarrow \mathrm{SHA}_{256}(Af)$
7: ***endfor***
8: ***for*** $y_{0\to(128-Summation\_String\_index[x]}$
9: $Ay \leftarrow \mathrm{SHA}_{256}(Ay)$
6: ***endfor***
7: $V_k.merge(Af,\ Ay)$;
8: ***endfor***
9: ***if*** $\sum_{i=0}^{15} V_k[i] == 1 == \mathrm{G_{pub}}$ /* Final steps for verification
10: ***then*** *Sucess verification*
12: ***else*** *Failed Verification*
13: ***end if***

The OTS scheme-based blockchain architecture provided decentralization, security, and privacy. After signature verification, we can say that it offers a secure environment for smart city applications because it utilizes blokchain ledger in the fog layer. The security and privacy of the proposed architecture and experimental evaluation are discussed in the next section.

4 Experiment and Performance Evaluation

This section presents the experimental and performance evaluation of the proposed Architecture for Energy-Efficient IoT in Edge Infrastructure. It has three subsections: Quantitative analysis, Security and privacy analysis, and Comparative analysis with existing research.

4.1 Quantitative Analysis

In this subsection, we evaluate the effective performance of the proposed architecture and algorithms with simulation such as computing cost, and communication cost. Permissioned blockchain Hyperledger fabric (Version 1.2), docker container (2.0.5), Ubuntu Linux (14.04.6 LTS) with virtual CPU were employed for the simulation setup. For the Hyperledger Fabric blockchain, 4–40 GB internal memory was the minimum requirement. Node.js v8.9.1 (6.8.0 version) was installed for checking the performance of various node tests. The computing and communication costs of the proposed architecture are evaluated in this section.

Table 2: Comparison of security and privacy analysis with existing research

Parameters research work	Confidentiality	Data integrity	User anonymity	Decentralization	Security against malicious users	Security against man-in-the-middle attack
Zhang et al. [31]	✓	No	✓	No	No	✓
Shahid et al. [18]	✓	✓	No	No	✓	No
Wu et al. [32]	No	✓	No	No	✓	No
Lu et al. [33]	✓	✓	No	✓	No	No
Kaur et al. [23]	No	✓	✓	✓	No	No
Proposed Work	✓	✓	✓	✓	✓	✓

Computing Cost: The evaluation of computing cost is dependent on the total bits exchanged with a registered user and on signature verification in Blockchain networks. The average time required for hash code is 0.32 msec, the signature generation time is 21.82 msec, the signature verification time is 38.92 msec, and the asymmetric encryption/decryption time taken is 22.72 msec as shown in [34]. It has three phases, including Generate keys G_k, Generates signature $G_{s,}$ Signature Verification S_V for the calculation of overall computing cost.

- *Generate keys:* According to Algorithm 1, one hash code operation, and one asymmetric encryption/decryption for private and public keys are used. Thus, the total computing time cost is (0.32 + 22.72) = 23.04 msec for this phase.
- *Generate signature*: One hash code operation, one asymmetric encryption/decryption, and signature generation are utilized for this phase with Algorithm 2. Thus, (0.32 + 22.72 + 21.82) = 44.86 msec as the total computing time used for this phase.

- *Signature Verification*: One hash code operation, one asymmetric encryption/decryption, and signature certification is employed in this phase. Thus, (0.32 + 22.72 + 38.92) = 61.96 msec as the total computing time cost for this phase. Finally, we calculate the overall computing time for blockchain networks according to all algorithms as (23.04 + 44.86 + 61.96) = 129.86 msec.

At this point, a performance analysis of the proposed architecture is conducted when the number of transactions increases. Thus, the computing time for signing and verifying the signature linearly varies according to the no. of transactions as a reference as shown in Fig. 4a.

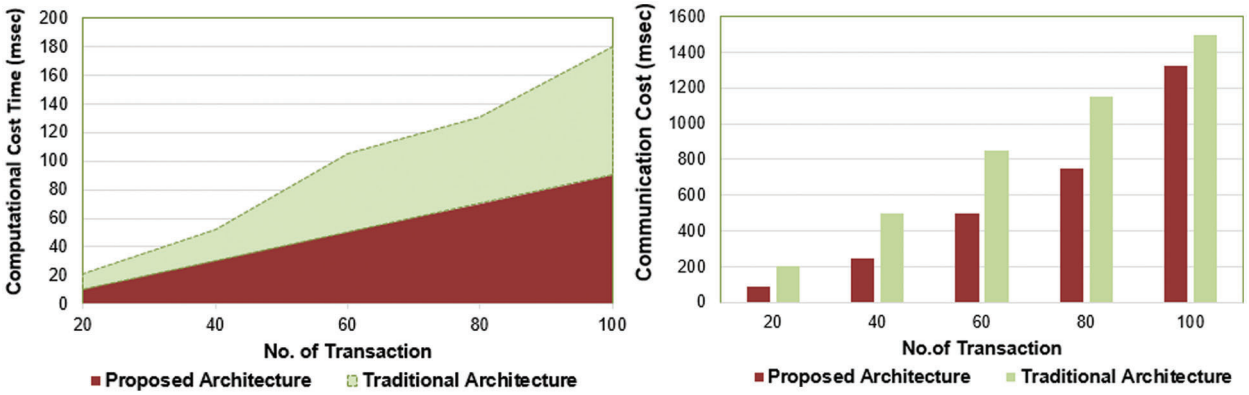

Figure 4: (a): Computing cost time analysis concerning No. of transactions (b): Communication cost analysis concerning no. of transactions

Communication Cost: Let user identity be 32 bits, SHA hash output be 256 bits, random nonce be 16 bits, timestamp be 16 bits, and encryption/decryption identification be 32 bits long, with checksum values of 256 bits. It is described in [34] as well. The communication cost also follows the Generate keys G_k, Generate signature G_s, Verify Signature S_V phases.

- *Generate keys:* The total communication cost for this phase is (32 + 4 + 256 + 16 + 16 + 32) = 356 bits as required. User identity, registration, SHA hash output, random nonce, timestamp, and encryption/decryption identification functions are used.
- *Generate signature*: For this phase, the total communication cost is (32 + 4 + 256 + 16 + 16 + 32) = 356 bits, which is utilized. User identity, registration, SHA hash output, random nonce, timestamp, and encryption/decryption identification functions are provided.
- *Signature Verification*: The total communication cost for this phase is (32 + 4 + 256 + 16 + 16 + 32 + 256) = 612 bits, which is required in signature verification.

Thus, the overall communication cost of the proposed architecture is (356 + 356 + 612) = 1324 bits. It is better to compare with existing studies according to the number of transactions, as shown in Fig. 4b.

4.2 Security and Privacy Analysis

This subsection analyzes security and privacy with various parameters, including confidentiality, data integrity, user anonymity, decentralization, security against malicious attack, and man-in-the-middle attack for Edge Infrastructure. As already discussed in Section 3, the OTS scheme based blockchain is deployed at the fog layer of the proposed architecture for security and privacy purposes. Tab. 2 shows the security and privacy analysis *vs.* existing studies.

Confidentiality: The proposed architecture satisfies the property of confidentiality because the blockchain is the collection of blocks, each of which connects to the previous blocks by a hash function. Any user wishing to transfer the information from one node to another, first encrypts the data with public and private keys (Algorithm 1), and plain text is converted into the ciphertext; the user then generates a signature (Algorithm 2) and finally verifies the signature (Algorithm 3) and matches the A's private key and signature. Finally, add the block in the blockchain network. The receiver user decrypts data through signature verification in the advanced applications for a smart city.

Data Integrity: Actually, we know that the data integrity of the information follows the three steps of creation, transmission, and storage. Note, however, that alteration of data follows the steps of insertion, deletion, and substitution. Digital signature or signature verification deviates from the property of the alteration of data in the network [35]. We are using a signature verification algorithm (Algorithm 3) to check for the modification of data in the proposed algorithm. Blockchain networks already support the data integrity of information in the blockchain network, but the OTS scheme provides more security to communicate the information with the Blockchain network.

User Anonymity: Through the use of the proposed architecture, the property of user anonymity is supported. Efficient, secure communication of user information among various financial applications and is difficult, hiking up the cost of malicious user authentication functionality. Any user of a smart enterprise or a company wishing to communicate the information to another user first completes the registration process in the blockchain network by generating private and public keys (Algorithm 1). When signature verification is done, including the addition of block in the blockchain network, the receiver will get the information with the help of the proposed architecture.

Decentralization: The proposed architecture supports decentralization because it uses the concept of Blockchain. The Blockchain network already enhances the three properties of data integrity, decentralization, and transparency. Algorithms 1, 2, and 3 provide more security and privacy with a decentralized, secure distributed blockchain network.

Security against malicious users: We are utilizing the distributed network in Blockchain with an OTS scheme that follows the protocols of key generation, signature generation, and signature verification. It is like the registration and verification steps for use of the Blockchain network by a new user. When any malicious user wants to access this network, it will not follow the aforesaid steps and forgery is computationally impossible [36]. Therefore, the proposed architecture can be said to provide security against a malicious user.

Security against Man-in the Middle attack: The proposed architecture provides security against the man-in-the-middle attack because it maintains the secure exchange of the public key and generation of secure public and private keys with Algorithm 1, finally verifying the signature by minor nodes in the Blockchain network. Therefore, the proposed architecture can be said to offer security and privacy against the aforesaid attack for advanced smart applications.

According to the security and privacy analysis, we are providing a secure environment in smart applications in edge infrastructure with the use of the proposed architecture. This architecture satisfies the properties, including confidentiality, data integrity, user anonymity, decentralization, security against malicious attack, and man-in-the-middle attack for energy-efficient IoT in edge infrastructure for a smart city.

4.3 Comparative Analysis with Existing Research

This subsection discusses various existing research and compares them with the proposed architecture using some parameters, such as key technology, security architecture/framework, approach, and key consideration. Tab. 3 shows the comparative analysis with existing research. The proposed research provides more security and privacy with energy efficiency for Energy-Efficient IoT in Edge Infrastructure for a smart city through OTS scheme-based blockchain at the fog layer. It uses a distributed network and

enhances the three properties, including data integrity, decentralization, and transparency. It also incurs less computing resource cost and realizes scalability and centralization in advanced applications in a smart city.

Table 3: Comparison with existing research studies

Research work	Year	Key technology	Security methods	Applications	Approach/Procedure	Key considerations
Kim et al. [22]	2019	Blockchain, IoT	Distributed	Smart energy	Proposed Blockchain of Things (BoT) model to overcome the security vulnerability of existing IoT devices	IoT vulnerability
Kaur et al. [23]	2018	AI, IoT	Centralized	Smart city	Designed Green IoT architecture for reducing energy consumption at each stage of IoT smart city application	Energy saving
Sukjaimu et al. [25]	2018	Green IoT	Centralized	Information-centric networks	Proposed a congestion control mechanism to mitigate the network congestion rate for the Green IoT Sensor	Congestion control
Patil et al. [27]	2017	Blockchain, Green House	Distributed	Smart farming	Provided a lightweight blockchain-based secure framework for smart greenhouse farming	Security, privacy
Singh et al. [28]	2020	Blockchain, IoE	Distributed	Smart city	Presented Blockchain and Fog-based secure architecture for the Internet of Everything (IoE) in smart cities	Security for smart city
Linde et al. [30]	2018	PQ Blockchain	Centralized, Distributed	No application	Constructed PQ scheme and compared with traditional scheme	Security
Our contribution	2020	OTS Scheme, blockchain, energy efficient IoT	Distributed	All smart advanced applications	Providing more security with OTS scheme based Blockchain for Energy-Efficient IoT in Edge Infrastructure	More security and privacy with energy efficiency

5 Conclusion

We proposed OTS scheme-based secure architecture for Energy-Efficient IoT in Edge Infrastructure for smart city applications. Blockchain technology is known to provide security and privacy with a distributed network. Nonetheless, we used the OTS scheme for providing more security and privacy in terms of confidentiality, user anonymity, data integrity, and others. Three algorithms, Generation Keys, Generate

Signature, and Signature verification used to provide such security in sustainable smart city advanced applications, including smart manufacturing, smart industries, smart healthcare, and more. The comparison with existing researches also demonstrated security and privacy, key technologies, key considerations, and others. We evaluated the performance of the proposed architecture as the computing and communication costs for the network. Finally, we compared it quantitatively, including security, and privacy, and performed comparative analysis with existing research studies as various traditional parameters. The performance result of the proposed architecture is better than the other approaches providing more security and privacy.

Funding Statement: This study was supported by the Advanced Research Project funded by SeoulTech (Seoul National University of Science and Technology).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Lee, S. Rathore and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–14, 2020.

[2] K. Gafurov and T. M. Chung, "Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 797–819, 2019.

[3] M. Framingham, "The growth in connected iot devices is expected to generate 79.4ZB of data in 2025," 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[4] S. Tanwar, S. Tyagi and S. Kumar, "The role of Internet of Things and smart grid for the development of a smart city," in *Intelligent Communication and Computational Technologies*. Singapore: Springer, pp. 23–33, 2018.

[5] S. K. Singh, Y. S. Jeong and J. H. Park, "A deep learning-based iot-oriented infrastructure for secure smart city," *Sustainable Cities and Society*, vol. 60, 102252, 2020.

[6] D. M. Park, S. K. Kim and Y. S. Seo, "S-mote: Smart home framework for common household appliances in IoT network," *Journal of Information Processing Systems*, vol. 15, no. 2, 2019.

[7] S. K. Routray and K. P. Sharmila, "Green initiatives in IoT," in *2017 Third Int. Conf. on Advances in Electrical, Electronics, Information, Communication and Bioinformatics*, Chennai, India, IEEE, pp. 454–457, February 2017.

[8] I. Mistry, S. Tanwar, S. Tyagi and N. Kumar, "Blockchain for 5G-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, pp. 106382, 2020.

[9] S. K. Singh, S. Rathore and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2019.

[10] V. Mohammadi, A. M. Rahmani, A. M. Darwesh and A. Sahafi, "Trust-based recommendation systems in internet of things: A systematic literature review," *Human-Centric Computing and Information Sciences*, vol. 9, no. 1, pp. 21, 2019.

[11] A. E. Azzaoui, S. K. Singh, Y. Pan and J. H. Park, "Block5GIntell: Blockchain for ai-enabled 5G networks," *IEEE Access*, vol. 8, pp. 145918–145935, 2020.

[12] P. K. Sharma, N. Kumar and J. H. Park, "Blockchain technology toward green IoT: Opportunities and challenges," *IEEE Network*, vol. 34, no. 4, pp. 263–269, 2020.

[13] H. Shu, F. Chen, D. Xie, L. Sun, P. Qi *et al.,* "An aggregate signature scheme based on a trapdoor hash function for the internet of things," *Sensors*, vol. 19, no. 19, pp. 4239, 2019.

[14] M. Maksimovic, "Greening the future: Green internet of things (G-IoT) as a key technological enabler of sustainable development," in *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, vol. 30, Springer, Cham, pp. 283–313, 2018.

[15] X. Jiang, M. Liu, C. Yang, Y. Liu and R. Wang, "A blockchain-based authentication protocol for WLAN mesh security access," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 45–59, 2019.

[16] C. Li, P. Wang, C. Sun, K. Zhou and P. Huang, "WiBPA: An efficient data integrity auditing scheme without bilinear pairings," *Computers, Materials & Continua*, vol. 58, no. 2, pp. 319–333, 2019.

[17] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng *et al.,* "Research on public opinion propagation model in social network based on blockchain," *Computers Materials & Continua*, vol. 60, no. 3, pp. 1015–1027, 2019.

[18] F. Shahid, I. Ahmad, M. Imran and M. Shoaib, "Novel one time signatures (nots): A compact post-quantum digital signature scheme," *IEEE Access*, vol. 8, pp. 15895–15906, 2020.

[19] J. Cha, S. K. Singh, Y. Pan and J. H. Park, "Blockchain-based cyber threat intelligence system architecture for sustainable computing," *Sustainability*, vol. 12, pp. 6401, 2020.

[20] B. Borja, A. Ramon, M. Diego and S. P. Alvaro, "Trust provision in the Internet of Things using transversal blockchain networks," *Intelligent Automation and Soft Computing*, vol. 25, no. 1, pp. 155–170, 2019.

[21] W. B. Shi, J. Q. Wang, J. X. Zhu and Y. P. Wang, "A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation," *Intelligent Automation and Soft Computing*, vol. 25, no. 1, pp. 171–181, 2019.

[22] S. K. Kim, U. M. Kim and J. H. Huh, "A study on improvement of a blockchain application to overcome vulnerability of iot multiplatform security," *Energies*, vol. 12, no. 3, pp. 402, 2019.

[23] G. Kaur, P. Tomar and P. Singh, "Design of cloud-based green iot architecture for smart cities," in *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Cham: Springer, pp. 315–333, 2018.

[24] J. Yang, W. Xiao, C. Jiang, M. S. Hossain, G. Muhammad *et al.,* "Ai-powered green cloud and data center," *IEEE Access*, vol. 7, pp. 4195–4203, 2018.

[25] R. Sukjaimuk, Q. N. Nguyen and T. Sato, "A smart congestion control mechanism for the green iot sensor-enabled information-centric networking," *Sensors*, vol. 18, no. 9, pp. 2889, 2018.

[26] X. He, K. Wang, H. Huang, T. Miyazaki, Y. Wang *et al.,* "Green resource allocation based on deep reinforcement learning in content-centric IoT," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 3, pp. 781–796, 2018.

[27] A. S. Patil, B. A. Tama, Y. Park and K. H. Rhee, "A framework for blockchain-based secure smart green house farming, " in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, pp. 1162–1167, 2017.

[28] P. Singh, A. Nayyar, A. Kaur and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, pp. 61, 2020.

[29] F. K. Shaikh, S. Zeadally and E. Exposito, "Enabling technologies for green Internet of Things," *IEEE Systems Journal*, vol. 11, no. 2, pp. 983–994, 2018.

[30] W. V. D. Linde, P. Schwabe, A. Hülsing, Y. Yarom and L. Batina, "Post-quantum blockchain using one-time signature chains," Radboud University, Nijmegen, The Netherlands, Technical Rep, pp. 1–62, 2018.

[31] Y. Zhang, D. He and K. K. R. Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in iot," *Wireless Communications and Mobile Computing*, vol. 2018, no. 2, pp. 1–9, 2018.

[32] B. Wu, Q. Li, K. Xu, R. Li and Z. Liu, "Smartretro: Blockchain-based incentives for distributed IoT retrospective detection," in *2018 IEEE 15th Int. Conf. on Mobile Ad Hoc and Sensor Systems (MASS)*, Chengdu, China, pp. 308–316, 2018.

[33] X. Lu, Z. Guan, X. Zhou, X. Du and L. Wu, "A secure and efficient renewable energy trading scheme based on blockchain in smart grid," in *2019 IEEE 21st Int. Conf. on High-Performance Computing and Communications; IEEE 17th Int. Conf. on Smart City; IEEE 5th Int. Conf. on Data Science and Systems (HPCC/Smart City/DSS)*, Zhangjiajie, China, pp. 1839–1844, 2019.

[34] A. Jindal, G. S. Aujla and N. Kumar, "Survivor: A blockchain-based edge-as a-service framework for secure energy trading in sdn-enabled vehicle-to grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.

[35] J. C. S. Sicato, S. K. Singh, S. Rathore and J. H. Park, "A comprehensive analyses of intrusion detection system for iot environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020.

[36] A. Elbir, H. O. Ilhan and N. Aydin, "The implementation of optimization methods for contrast enhancement," *Computer Systems Science and Engineering*, vol. 34, no. 2, pp. 101–107, 2019.