Computers, Materials & Continua
DOI: 10.32604/cmc.2023.034331
Article

A Blockchain-Based Architecture for Securing Industrial IoTs Data in Electric Smart Grid

Samir M. Umran[1,2], Songfeng Lu[1,3], Zaid Ameen Abduljabbar[1,4] and Xueming Tang[1,*]

[1]School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, China
[2]Iraqi Ministry of Industrial and Minerals, Iraqi Cement State Company, Baghdad, 10011, Iraq
[3]Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518057, China
[4]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
*Corresponding Author: Xueming Tang. Email: xmtang@hust.edu.cn
Received: 14 July 2022; Accepted: 22 September 2022

Abstract: There are numerous internet-connected devices attached to the industrial process through recent communication technologies, which enable machine-to-machine communication and the sharing of sensitive data through a new technology called the industrial internet of things (IIoTs). Most of the suggested security mechanisms are vulnerable to several cybersecurity threats due to their reliance on cloud-based services, external trusted authorities, and centralized architectures; they have high computation and communication costs, low performance, and are exposed to a single authority of failure and bottleneck. Blockchain technology (BC) is widely adopted in the industrial sector for its valuable features in terms of decentralization, security, and scalability. In our work, we propose a decentralized, scalable, lightweight, trusted and secure private network based on blockchain technology/smart contracts for the overhead circuit breaker of the electrical power grid of the Al-Kufa/Iraq power plant as an industrial application. The proposed scheme offers a double layer of data encryption, device authentication, scalability, high performance, low power consumption, and improves the industry's operations; provides efficient access control to the sensitive data generated by circuit breaker sensors and helps reduce power wastage. We also address data aggregation operations, which are considered challenging in electric power smart grids. We utilize a multi-chain proof of rapid authentication (McPoRA) as a consensus mechanism, which helps to enhance the computational performance and effectively improve the latency. The advanced reduced instruction set computer (RISC) machines ARM Cortex-M33 microcontroller adopted in our work, is characterized by ultra-low power consumption and high performance, as well as efficiency in terms of real-time cryptographic algorithms such as the elliptic curve digital signature algorithm (ECDSA). This improves the computational execution, increases the implementation speed of the asymmetric cryptographic algorithm and provides data integrity and device authenticity at the perceptual layer. Our experimental results show that the proposed scheme achieves excellent performance, data security, real-time data processing, low power consumption (70.880 mW), and very

low memory utilization (2.03% read-only memory *(RAM)* and 0.9% flash memory) and execution time (0.7424 *s*) for the cryptographic algorithm. This enables autonomous network reconfiguration on-demand and real-time data processing.

Keywords: Smart grids; industrial IoTs; electric power system; blockchain technology; IoT applications; industry 4.0; decentralization applications

1 Introduction

Smart grid (SG) technology is a new version of the old electrical grid [1] that utilizes smart computer systems and applications to efficiently control and manage the transfer of data. These data are normally transferred in two ways: from internet-connected devices (also known as the internet of things (IoTs)) to the central control room (CCR), and vice versa. Communication between the assets in the network can directly enhance the performance, data management, and stability of the system, and can reduce the cost of the electric power supplied [2]. The use of SGs is growing fast due to the increase in demand for innovation in the conventional electric power system, which is becoming less suitable to meet the new requirements and challenges of the industrial environment and other sectors. Electrical SGs are used to control and manage smart meters (SMs), smart technologies, efficient resource management, circuit breaker (CB) events, and renewable energy resources [3]. By adopting SG technology, we can provide an efficient mechanism of communicating between different electric power suppliers, and hence can achieve flexibility in the transmission of power between different networks to provide stability and continuity of the power supply [4].

Wireless communication technology is widely adopted for local communication in SGs [5]. Since IoT devices are involved, several cybersecurity attacks may be launched against existing networks [6]. Traditional IoT architectures depend on a centralized form, represented by cloud services that provide storage, analysis, and powerful computational services. However, it still suffers from security and privacy issues, bottlenecks, and single authority of failure [7]. The growth of IIoT networks is increases exponentially, which raises the amount of sensing data and then increases the computational task in the centralized system. With high-performance applications as in the industrial sector (SGs), centralized architecture becomes an inconvenient choice [8]; it is exposed to cybersecurity threats more than decentralized architecture. The attackers work to exploit the vulnerable points within the communication system to achieve their goals, imagining the nonexistent faults that can lead to disruption of the whole power generation and transmission network [9–11]. Internet-connected CBs have many advantages and have become economically important, especially with the availability of automation equipment and recent communication technologies. In the normal case, an overhead electric CB is located far from the CCR [5]. The SG paradigm introduces new challenges in terms of security [6], such as physical attacks, cyber-attacks, and catastrophic issues, which are also considered major forms of threats to SGs [12,13]. Hence, cyber-security threats have become the most crucial factor affecting whether SGs are adopted [14].

Blockchain technology comes to provide an ideal solution to all of the aforementioned issues found in IIoT networks. Blockchain technology is a distributed ledger technology that enables the features of the immutable, transparent log, time-stamped, hashed, and authenticated records of transactions (as illustrated in Fig. 1). Blockchain establishes mutual trust between network participants in an untrustworthy industrial environment without the services of third parties, which then reduces the potential risk of data leakage and man-in-the-middle (MITM) attacks [15]. Blockchain technology is

adopted in many industrial applications such as supply chains, retailers, energy sectors, smart cities, and manufacturing, which is shifting the industrial sector to a new level of security, scalability, and privacy through its unique features. The overall system capacity of BC (for services) improved with increasing the number of nods [15]. With BC technology, the system will stay stable while one or more nodes are attacked or become offline. Therefore, BC has better performance and excellent resistance to external attacks and fault tolerance than conventional systems [16].

In our proposed architecture (as illustrated in Fig. 3), we exploited the unique features of BC technology and smart contracts to build a secure, trusting, lightweight, scalable, and decentralized architecture for the industrial sector. The overhead circuit breaker network of SGs of the Al-Kufa/Iraq power plant was taken as an industrial environment. We adopt the ultra-low-power and high-performance STM32 board-based ARM Cortex-M33 Microcomputer (internet-friendly) and ECDSA at perceptual layer to provide device authentication and data integrity at the physical layer. In addition to utilizing the McPoRA as an authentication mechanism, which efficiently reduces the latency, prevents the 51% attack, releases mining fees, has low energy consumption, high throughput, and scalability, it can efficiently authenticate new blocks as it has a very low execution time and improves the computational performance [17].

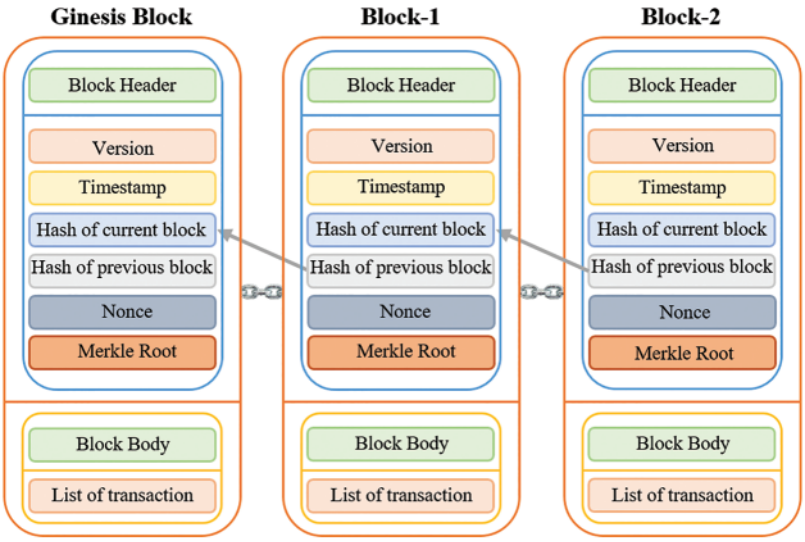

Figure 1: The main structure of blockchain technology

1.1 Motivation

In the context of electric SGs, recently developed power feeders utilize modern CBs that can automatically re-close an electric circuit based on events reported by the sensors. These techniques are used to boost the power quality, optimize the supply voltage, and reduce the cost. The wireless communication between these re-closer CBs provides numerous benefits and reduces the feeders' breakout time [18]. The IIoTs devices are considered resource-constraint devices, and large networks contain hundreds of devices that provide sensitive data, which requires an efficient, scalable, and trusted solution against cyber-security threats. Security concerns become a crucial factor. Without an efficient, scalable, lightweight, and trusted security system, the IIoT networks become useless. The most recent proposed solutions are not suitable for IIoTs requirements.

In this paper, we introduce a lightweight, scalable, and trusted security architecture for the electrical SG of the Al-Kufa power plant in Iraq, based on blockchain (BC) technology/smart contracts. The integration of IIoT devices into overhead CBs with BC technology/smart contracts can ensure the security, scalability, immutability, and trust system due to the distributed ledger used in the BC [19] that provides immutability and decentralization features of the system architecture.

1.2 Contributions

The main contributions of our proposed architecture are as follows:

(1) It provides an efficient and secure architecture that can guarantee the security of data transmission between private BC network participants and CBs in an SG environment. It can also protect the system from both internal and external attackers.

(2) It integrates BC technology with IIoT devices to provide a trusted, secure, scalable, access control, transparent log, and decentralized security scheme for an electrical SG environment.

(3) It provides two-stage data encryption, in the physical layer and the BC service layer. It also offers low computational complexity and high performance, due to the adoption of the ultra-low power consumption and high-performance ARM Cortex-M33 microprocessor in the physical layer.

(4) It successfully eliminates the need for external trusted authority services and the corresponding revocation list mechanism due to the adopted smart contract and hence achieves very low computational and communicational costs with increased system security and performance.

(5) The adoption of multi-chain proof of rapid authentication (McPoRA) as a consensus algorithm helps our scheme to run 4000 faster than traditional proof of work (PoW) and 55 times faster than proof of authentication (PoAh). In addition, the use of smart contracts increases the speed of the autonomously executed system.

(6) It provides real-time data processing and CB status monitoring, which enables automatic network reconfiguration during the occurrence of faults and handover of the demand to other available feeders during any abnormal events.

(7) It is the first work that utilizes BC technology/smart contracts in the realm of data security for electric CBs in an electrical SG.

The rest of this article is organized as follows. In Section 2, we present a literature review of related works that deal with securing data of electric smart grids in the industrial sector. In Section 3, we describe the application field and potential security risks with the proposed solution. In Section 4, we provide a detailed discussion of the proposed architecture for electric smart grids that contain three main layers as in Fig. 3. In Section 5, we present the proposed system work flow and the registration steps with the required algorithms, which control the users and devices registration; the process of data storage. The blockchain architecture for the electric smart grid of the Al-Kufa power plant is discussed in detail in Section 6. The performance analysis of our proposed architecture from the perspectives of cryptography, ECDSA Execution time, memory usage, and power consumption, presented in section 7. While in Section 8, we presented a detailed comparison between our proposed schemes with other alternative schemes, which consist of tens of criteria, as in Table 6. Finally, Section 9 concludes this article.

2 Related Works

An SG relies on the global internet network to connect the IIoT devices in the energy sector, also known as the internet of energy (IoE) [20] makes it more susceptible to many kinds of cyber security attacks. The IIoT improves industrial processes in many aspects and enables real-time data processing, collection, and storage. Due to the sensitivity of the data of IIoT in electrical SGs, the possibility of attackers exploiting data can lead to many risks, such as disruption to the whole network or control system, stoppage of the electric power plant and outage of transmission lines, theft of power, and damage to network equipment. The BC technology can benefit the energy system in two main ways: by changing the system architecture from a centralized model to a decentralized one and by providing a high level of security thanks to the nature of BC design [13]. After an extensive search of related work in many available databases, we found only one [11] dealing with the security of SGs in the context of the electric power transmission sector by securing the data of smart CBs. Here, we review the most similar techniques that are used in the SG sector to secure information. Most of these schemes do not address the problem of securing sensitive information in control systems to enable real-time processing and autonomous network reconfiguration.

Sadhukhan [21] developed a new mutual authentication scheme between consumers and substations based on elliptic curve cryptography (ECC) with trifling operations for an SG environment. Li [13] proposed a BC-based architecture for SGs in which the consumers could be fully involved in the energy system (ES) and trace the details of their energy bills. The authors demonstrated the stability of their ES and reduced energy wastage. Tolba [22] worked to overcome false data flow and proposed a cybersecurity-assisted authentication method for SGs that depended on pre-estimated energy requirements of the meters and previously acquired information. This scheme also provided authentication-dependent security. Aziz et al. [11] presented an efficient, lightweight authentication scheme that achieved real-time automatic network reconfiguration in the event of a fault occurring. Their scheme provided a flexible mechanism for electrical utilities, with reduced overall computational overhead and resistance to some common attacks, as a hash function was adopted for integrity purposes. Privacy was ensured by adopting a symmetric algorithm.

Ghafouri et al. [23] designed a detection and alleviation system that worked against cyber-physical attacks on wide-area management (WAM) systems and their components in electrical SGs. The authors studied the problems of voltage stability after an electrical disturbance and cyber-attacks against the WAM. The authors generated a suitable algorithm, which specialized in fixing these issues. Singha [16] worked on overcoming the high computation and communication costs of existing techniques, intending to control the negative impacts of flash workloads and proposed a deep learning and homomorphic encryption-based privacy-preserving data aggregation model. Fotohi [24] built a secure communication system between participating devices on a BC platform and introduced an authentication technique for each node using an identity-based signature (IBS). The proposed approach helped to increase the security of the devices and networks.

Khalid et al. [8] developed a decentralized, lightweight BC structure to ensure the security of peers. Their scheme had an overlay network that achieved a distributed mechanism and in this way, the nodes jointly controlled the BC management. The proof of concept (PoC) algorithm was adopted, which has high-energy requirements. However, this was not suitable for low computational power and resource-constrained devices. The overall system was susceptible to many security threats. Danish et al. [25] adopted a decentralized low range wide area network (LoRaWAN) procedure framework to develop a BC technology-based approach. Their framework (Ethereum BC) utilized PoC as a consensus mechanism. Nakamura et al. [26] aimed to verify the possession and validity of the tokens used for

access control and utilized a smart contract approach. In addition, to address the issues of storing and managing the capability tokens assigned to the related subjects, a smart contract was created for each object. The proposed scheme managed the tokens using units of access rights or actions. Unlike traditional approaches, this scheme successfully managed the tokens in units of subjects. This achieved more flexibility in delegation and ensured consistency between the information stored in the tokens and the delegation information. Sangaiah et al. [27] worked to reduce energy consumption and to make their model more resilient and proposed an energy-aware adversary model with lower energy consumption than the traditional model.

From the above, we note that most of the reviewed schemes depend on a traditional approach involving complex cryptographic algorithms, cloud services and an external trusted third party to provide their security architecture. Most of these architectures are not suitable for the IIoT devices that are utilized with our application, as these are classified as resource-constrained, low power consumption and low computational power. Although these schemes successfully address several security threats, they are still susceptible to other security and cybersecurity risks such as denial of service (DoS), forgery, Sybil, impersonation, modification, MITM attacks and single node crashes and bottlenecks, as discussed in detail in Table 6 and Section 8. They also depend on complex schemes such as public key infrastructure (PKI) [28,29], which imposes high computational and communication costs for signature generation and verification [11], suffers from low performance, involves high execution time, power consumption, resources, storage and bandwidth sizes.

In addition, the majority of these works, even those using BC-based approaches, deal with the problem of security for electrical SGs from the perspective of data recording, billing information, management and sharing information on power consumption with customers. Moreover, most of the authors of these studies have not focused on securing sensitive data of control systems in SGs, which are responsible for the generation and transmission of electrical power in secure environments. Only [11] deals with electric CBs and their security authentication and privacy issues, their scheme is susceptible to secret key compromise and eavesdropping [30].

In our scheme, we propose a lightweight, scalable, decentralized and trust security architecture for securing the sensitive data that is transferred between the overhead CBs (peer-to-peer (P2P)) and the CCR in a secure industrial environment, in the context of the SGs of the Al-Kufa power plant. The outdoor CBs of power transmission lines (feeders) send their events to the CCR and vice versa through a private network; to control and reconfigure the power network and CBs wirelessly through a global internet network with a secure environment. A secure framework is achieved by realizing the integration of the BC technology/smart contract with IoT devices in the industrial sector to satisfy all of the security requirements of SGs. This integration helps the electrical power SG to control CB events, to reconfigure the network according to demand and the event of power transmission line in a secure and trustworthy environment, and to protect the feeders from various problems.

3 Electric Circuit Breaker in a Smart Grid

The IIoT devices such as an interconnected circuit breaker are a vital component of an electrical distribution network that can provide excellent protection for the network equipment against various kinds of faults [31]. In addition, connecting CBs to a CCR enables remote network observation and real-time monitoring of the network loads, which are distributed on the available feeders according to the demand. In these electric feeders, many faults can occur, such as line-to-line (L2L), line-to-ground (L2G), two-line-to-ground (2L2G), and three-line (3L) faults, leakage currents, bird or tree contact, and catastrophic failures.

The interconnected CB is an innovative technology that enables the ability to make the right decision using real-time sensors' data processing to isolate the faulty line and protect the healthy overhead lines, electric equipment, and loads from short circuit currents or unbalanced voltages; can protect the power plants and feeders from overloads, imbalance and shutdown problems. Through this communication mechanism, CBs can send sensitive data related to their status to the CCR. The CCR then generates a suitable response promptly and sends commands to the CBs to connect or disconnect the feeders as depicted in Fig. 2; this enables the network reconfiguration ability to hand over the demand to other available feeders [32].

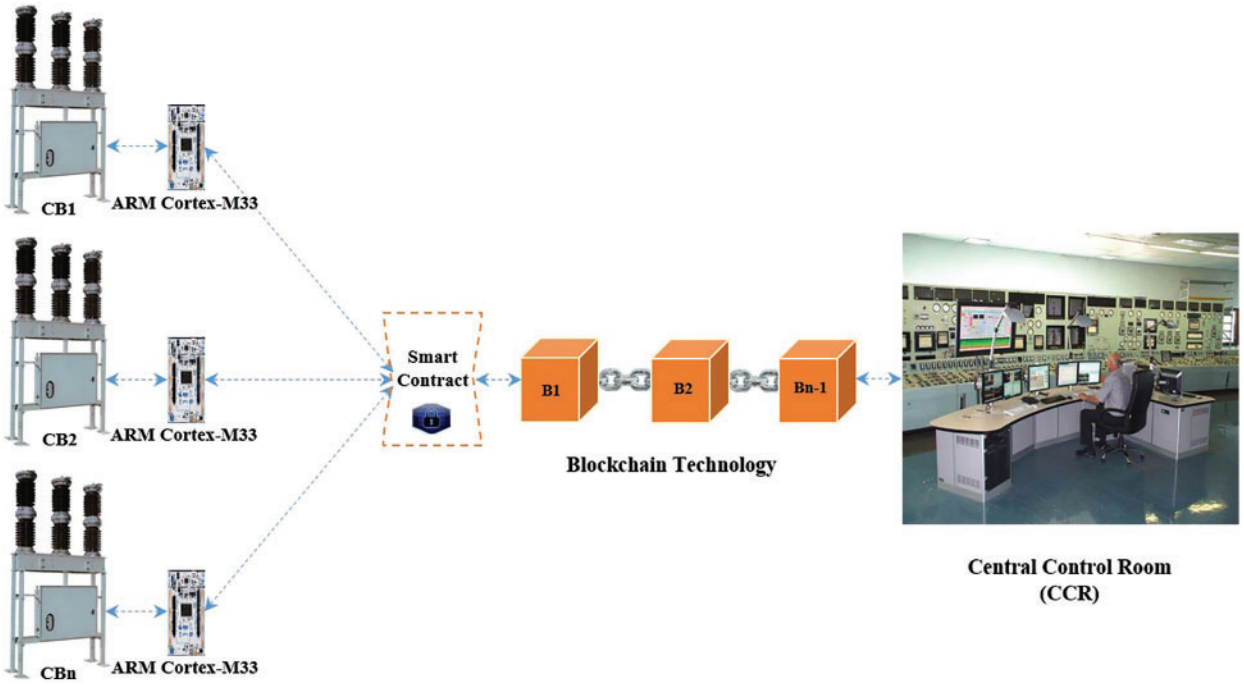

Figure 2: Overhead electric CBs communication through ARM Cortex-M33

The adoption of IoT in SGs can lead to many security risks and increases the possibility of sensitive data leakage, as attackers can exploit these points of vulnerability to carry out actions that may lead to stoppage of power plants, damage to electric equipment, outage of power feeders and power theft to achieve illegal goals [32]. In view of this, we cannot use internet network (IoT) infrastructure without building an efficient, lightweight, scalable, trusted and secure scheme to ensure the security of sensitive transferred data and its assets in an SG environment.

4 Proposed Architecture for Secure Data of Overhead CB Based on Blockchain Technology

The electrical SG consists of three main sectors: power generation, power transmission, and power distribution. In our work, we take the power transmission sector as an application area due to its importance and lack of research in this area. Any fault in this sector can cause serious direct effects on the other two sectors, such as shutting down the power plant, damaging the generators, and destroying electrical equipment. In this case, the supply of electrical power to many of the branches or loads should be shut off. Therefore, the security of an IIoT in an SG system is a crucial aspect that should

be considered to achieve the goals of SGs, without a trusted and secure architecture, IIoT network in SGs becomes useless.

Our work provides a scalable, trusting and secure architecture that provides a secure communication channel between faraway overhead circuit breakers through the internet network. Thus, it improves the electric network operation; reduces the power cutting off time from loads and enables automatic network reconfiguration during the occurrence of faults and handover of the demand to other available feeders during any abnormal events.

The emergence of BC technology with its unique features has helped in finding a reliable, secure structure that can efficiently resist various known attacks [13,33]. Then can improve the security, privacy, authenticity, and data availability of the whole electrical SG system, especially when IoT devices are used in smart industry applications. Fig. 3 illustrates the proposed secure architecture for the Al-Kufa power plant, which was selected as an industrial application, it consists of three layers: a physical layer, a BC service layer, and the application layer. In addition, our architecture can be applied in several other contexts in other industrial fields.

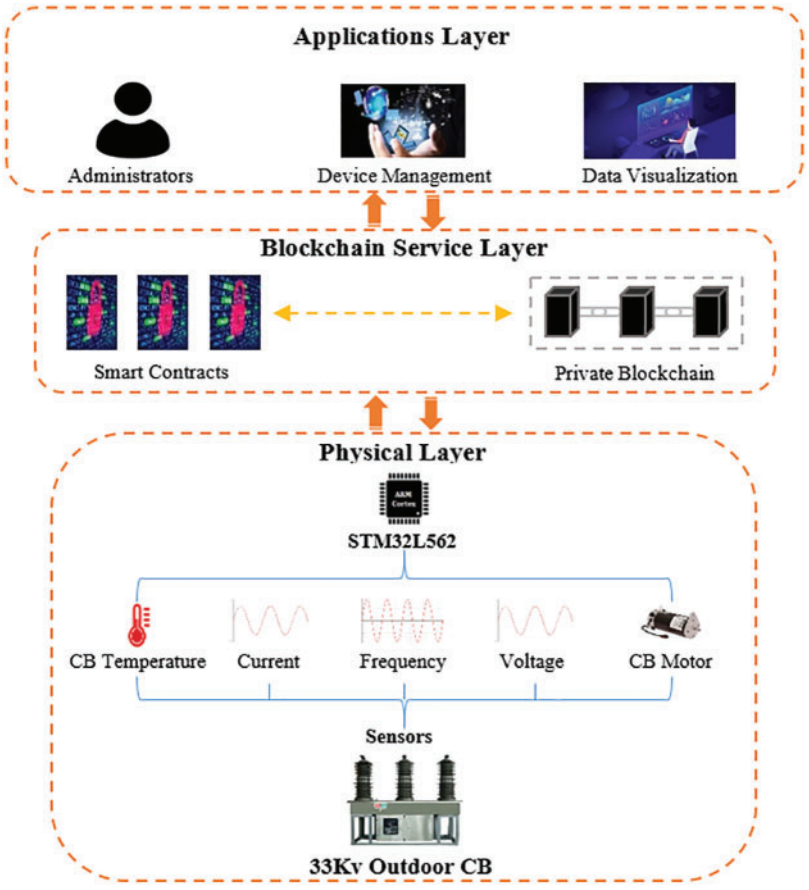

Figure 3: The proposed secure architecture for the Al-Kufa power plant

4.1 Physical Layer

In the physical layer of our proposed architecture, there are various sensors embedded inside the controllers of the overhead CBs, which record the current, voltage, frequency, voltage and current deferential, CB events (on, off), direct current (D.C) voltage, leakage current, inrush current, temperature and SF6 gas leakage as illustrates in Fig. 3.

In our scheme, all of these sensors are interfaced with the IoT-friendly ARM Cortex-M33 microcontroller, which is characterized by high performance and ultra-low power consumption [30,34]. This is particularly suitable for resource-constrained devices that require high security, high performance, and low power consumption. It is also efficient and effective for IIoT applications and represents an excellent choice for a cryptographic algorithm such as ECC and ECDSA [35]. The microcontroller first receives raw data from sensors and pre-processes it, generates the digital signature, and public and private keys and then encrypts the data using an efficient, high-speed implementation of ECDSA at the device level before sending it to the BC service layer [36].

4.2 Blockchain Service Layer

Blockchain is a decentralized, distributed, time-stamped, transparently logged, traceable and shared database ledger, which can provide a trusted system with excellent resistance to most cybersecurity attacks [37,38]. The use of BC technology/smart contracts can create an environment with a high level of protection for a control system and real-time data processing through its unique features of decentralization, high security, immutability, access control and privacy. In our scheme, the BC service layer receives the encrypted data from the physical layer and then writes the proposed transactions in the form of a smart contract. After this, the BC system checks the validation of these proposed transactions before authenticating them. Only validated transactions will be authenticated and obtain permission to be added to the BC network as a new block, and others will be denied. The device authentication mechanism uses public and private keys, which are generated by the ECDSA that also provide a digital signature, which has low complexity, very fast execution and low storage needs [36]. The National Institute of Standards and Technology has certified the use of ECDSA for industrial applications [9,35].

4.2.1 Blockchain-Smart contracts

To achieve a high level of security, we adopted a system based on private BC/smart contracts in our architecture rather than a public or consortium BC. This was because a private BC is most suitable for the industrial sector [39] and provides robust architecture, which does not involve continuously adding new participants to the network as in a public BC. Blockchain technology enables P2P communication between network participants. Through this mechanism, only authorized nodes that have permission to access the private network, can add new transaction proposals and read the details of a transaction (efficient access control). Unlike centralized architectures, this decentralized approach fully eliminates the need for third-party services [40,41], which is a significant drawback of a centralized architecture due to the potential for single node crashes, the bottleneck problem, leakage of sensitive data, higher requirements for bandwidth size and longer delays. The irreversible nature of smart contracts prevents an unauthorized node from making any changes to the BC ledger (immutability) [42]. Our scheme provides an efficient, trusted and lightweight security architecture to ensure data confidentiality, integrity and availability. In addition, our work is the first one in the area of overhead CB data security for electrical SGs that utilize BC technology.

As mentioned above, the BC network in our architecture receives the data from STM32L562 development board at the physical layer in the form of encrypted data; this efficiently increases the security of the sensitive data provided by CBs and the overall security of the electrical SG system by adding another stage of encryption at the device level. By adopting BC technology/smart contracts with an efficient consensus algorithm (McPoRA), our scheme offers immutability, time-stamping, information backtracking, efficient access control, lightweight, trust, decentralization and real-time data processing; provides security for the sharing of CBs sensor's data that can efficiently resist to most common cybersecurity threats. Even if an unauthorized user was to access the BC network, there would be no way to read, modify or delete data (resist internal and external malicious actions). In addition, all BC ledgers use the hashing function mechanism SHA-256 and asymmetric encryption (ECC) [36] that is already adopted in the BC architecture; the digital signature adopted with IoT-friendly STM32 board based on ARM Cortex-M33 microcontroller in the physical layer of our scheme. Since dependency on third-party services is eliminated, consensus algorithms become an important part of the BC in terms of authenticating and validating new blocks [40,41].

4.2.2 McPoRA Consensus Mechanism

McPoRA was utilized as an authentication mechanism in our architecture to efficiently authenticate new proposed transactions. There are limitations to the use of BC technology, such as energy-constrained devices, scalability, computational complexity, and latency. For IIoT applications, the most important factor is latency [43]. Numerous BC consensus algorithms have been designed according to the field of application, including PoW, proof of stake (PoS), proof of authority (PoA), proof of authentication (PoAh), proof of importance (PoI), and proof of block and trade (PoBT), which are the most widely adopted algorithms.

Nevertheless, very few of these consensus algorithms can be used with low-computational power IIoT applications, such as PoAh and proof of physical unclonable functions (PUF) enabled authentication (PUF Chain) [44].

McPoRA efficiently reduces the latency and prevents the 51% attack, which can be launched against most traditional consensus mechanisms such as PoW, PoS, PoC, and DPoS [45]; release mining fees, has low energy consumption, high throughput and scalability, and can efficiently authenticate new blocks as it has a very low execution time [17]. We analyzed the McPoRA consensus algorithm from several different perspectives. In terms of latency, McPoRA is a lightweight approach and was designed to deal with resource-constrained devices such as those in IIoT applications [44]. A comparison with the most commonly adopted consensus mechanisms such as PoW, PoI, PoA, PoAh, and Proof-of-Proof (PoP) proves that the McPoRA algorithm is faster than all of these traditional algorithms; for instance, it is faster than PoW and PoAh by factors of 4000 and 55, respectively [17] as discussed in Table 1.

Table 1: Detailed comparison of McPoRA with traditional consensus algorithms.

Consensus algorithms	Authentication time (ms)	Ledger	Miners	Validation	Blockchain type	Data structure
Proof of work	240,000	Full	✓	Hash cash	Public	BC
Proof of importance	60,000	Full	✓	Accounts importance	Public	BC

(Continued)

Table 1: Continued

Consensus algorithms	Authentication time (ms)	Ledger	Miners	Validation	Blockchain type	Data structure
Proof of authenticity	5000	Full	✓	PoS	Permissioned	BC
Proof of PUF-Enabled authentication	192.3	Full	✓	Predefined keys verification	Private	BC
McPoRA	3.9	Portion	X	UID verification	Private	Multi-Chain

From the perspective of security, McPoRA provides an effective security solution for IoT structures when used in decentralized IIoT applications. Our scheme can address the problems of instability related to network connectivity and can prevent Sybil, impersonation, DoS, distributed DoS (DDoS) and 51% attacks, which can be launched against the existing BC consensus mechanism [38, 45] by avoiding the dependency on mining process to authenticate new blocks [43]. We adopted authenticating the node with the predefined IDs in the secure unique identification list (SUIL) [46]. From the perspective of scalability, it can alleviate several issues such as the latency and high requirements for processing power and storage capacity of the traditional BC [43]. By avoiding the use of mining and a full ledger that leads to a reduction in process complexity, the McPoRA consensus algorithm successfully increases the speed of authentication for new data. The McPoRA algorithm consists of four essential parts, which are the SUIL, the dynamic blocks list (DBL), transactions and block content as described in Algorithm 1.

From the perspective of resource utilization, McPoRA requires limited resources, whereas conventional consensus algorithms require much more [17]. From the perspective of speed, in DBL feature, with each block, there are two arcs attached that allow for two blocks to be authenticated using only one block. This approach enables speeding up the process of authentication. With this mechanism, more blocks can therefore be authenticated quickly when increasing the number of blocks that are added to the multi-chain. Moreover, from the perspective of the area of application, it was designed especially for IoT and cyber-physical system (CPS) applications.

Algorithm 1: McPoRA Consensus Algorithm steps.

Input: Data (D) provided from electric (CBs)
Output: Authenticated (ab) or Discarded (db) Blocks
Terms: number of authenticated blocks is (bcn), the number of nodes is (n)
Start:
  Nodes (CBs) creates block ab
  BFA runs by nods {BFA = Block Filtration algorithm}
    if $bci = 0$ in DBL. Then,
      take $ab1$ and $ab2$ with $bci = 0$
    else
      take $ab1$ and $ab2$ with $bci = 0$ and $bci = 1$
End
Take $ab1$ and $ab2$ randomly

(Continued)

Algorithm 1: Continued

Two previous blocks identify as a location (*li*) by node
  if *UDI* in $a\bar{b}2$ and $a\bar{b}1 \neq$ UDIs in SUIL
    Discard
  else
    Authenticate
End
CBs broadcasts block *ab*
$ab \longrightarrow DBL$
  if *bci* for each *ab* in DBL = n, then
    Reduce
  else
    Leave
End

4.3 Application Layer

The application layer represents the top layer of our proposed architecture; offers an efficient mechanism for enabling secure interaction between authorized users and authenticated smart CB devices as shown in Fig. 3. Via this interaction, authorized users can observe the grid, device manager, and control system, can visualize data and can reconfigure the feeders in real-time, based on the data provided by the embedded IIoT devices (STM32L562) to the CCR. The administrator is responsible for generating a unique ID for each new network participant (only user) and sharing it with the BC members to register this new proposed ID if it has not previously existed as described in Algorithm 2.

5 Proposed Scheme Working Flow

Our architecture is specifically designed to provide an efficient, lightweight, secure, scalable architecture with real-time data processing, low power consumption, and a distributed trust mechanism. It enables autonomous sharing of sensors' data between the CBs themselves and between each CB and with the central CR. The status of the transmission lines is controlled through the integration of BC technology/smart contracts (SC) with IIoT devices such as the STM32L562 development board, which we designed to be embedded into the electrical CBs in an SG environment in the Al-Kufa power plant. In our scheme, each network participant (user or device) has a unique ID that is issued in advance and registered in the BC network, which helps in the registration and authentication steps as described below.

5.1 Initialization of the System

The system initialization process involves the registration of private BC network participants such as users and IoT devices (CBs), which enables re-authentication. The registration procedure is divided into two steps in our scheme: the registration of users and the registration of CBs as described in Algorithm 2 below.

Algorithm 2: New nods registration process.

Start:
System admin checks the node kind:
if (Node == User) Then:
Generate users unique ID: (User ID == SA79@Industrial + some of users attributes)
Share the generated IDs to blockchain members
if (User ID not already exist in BC network == True)
Then execute McPoRA consensus algorithm,
SC allow the registration of new user ID in BC,
BC generate and return ID certificates to BC members
else
Deny proposed transaction
Admin notification is issued
Return error ( )
else
ARM Cortex-M generate a new device unique ID
Device ID == (Circuit breaker of feeder 1 + Unique board number)
STM32L562 sends the information to the BC nods,
BC nodes process the proposed registration request
if (CBs ID does not exist in the BC network == True)
Then Execute (McPoRA) algorithm,
Register a new devise ID in the BC network,
Notify BC participants by sharing a new device ID certificate
else
Deny proposed transaction
Then notify nods to Return error ( )
End

We classified the new nod registration into two steps, the first step represents the user registration while the second step represents the device registration. In the user registration process, the administrator issues a new unique ID and matches it with pre-stored some users attributes such as fingerprint, eye print or voiceprint for each user (for one-time use). The issued ID with the user attribute is then sent to the BC members as a proposed transaction for registration. The BC nodes check the existence of this new user (ID and attribute) in the BC network using a smart contract, which allows for the registration of a new transaction only if it does not already exist. After executing the consensus algorithm (McPoRA), the registration of a new user in the BC network is completed and shared with all network participants. The administrator receives the new user certificate from the BC, which is generated based on the user's private key. Otherwise, the proposed transaction is denied and the administrator is notified with an error message.

In the second step, the physical layer of our scheme contains many CBs, which are installed to control the electrical power feeders. The STM32 development board is based on an ARM Cortex-M33 interface with various embedded sensors inside each overhead circuit breaker, which are responsible for providing encryption of sensitive data to the blockchain service layer. All of these devices must be registered with the private BC network in advance to provide authentication and registration issues in the BC network.

The microcontroller is responsible for generating a new ID and transactions for device registration requests to the BC nodes. The verification process of the device ID is based on a smart contract; the consensus algorithm (McPoRA) is responsible for the execution and authentication of the new device ID in the BC network after checking the existence of the device ID in the BC, the new certificate is then shared with the BC participants. Otherwise, the proposed transaction is denied and the administrator is notified with an error message. Algorithm 2 describes the process of new nod registration in detail.

5.2 Storage of Circuit Breaker Sensors Data

The last step in our scheme involves the storage of sensitive sensor data, which is passed to the BC network from registered and authenticated sensors only via the ARM Cortex-M33 microcontroller as clear in Fig. 4, the data storage process begins when new data are received by the STM32L562, which is responsible for pre-processing the received data, checking the registration device ID to verify or deny it, and then executing the ECDSA that generates the public and private keys. After encrypting the received data and before sending it to the next layer, a storage request was sent to the BC network for the proposed transaction.

After the consensus algorithm is executed, the authenticated transaction obtains permission from the smart contract to store encrypted data inside the BC network, each participant user in the BC network is working either as a server (provides storage capacity) or a client. Algorithm 3 summarizes the data collection and storage process.

Algorithm 3: CBs sensors data storage.

Start:
ARM Cortex-M33 start pre-process of CB sensors data
ARM Cortex-M33 sends the processed information to the blockchain Network
ARM Cortex-M33 verifies the device through its advanced Registration ID
if (Device authentication = = true)
Then execute ECDSA
Generate public and private keys (to transfer data to the next layer securely)
Submit proposed transaction to blockchain nods for data storage
if (McPoRA = = true)
Then store CBs encryption data inside the blockchain network
else
Return error ( )
else
Deny proposed transaction
Return error ( )
End

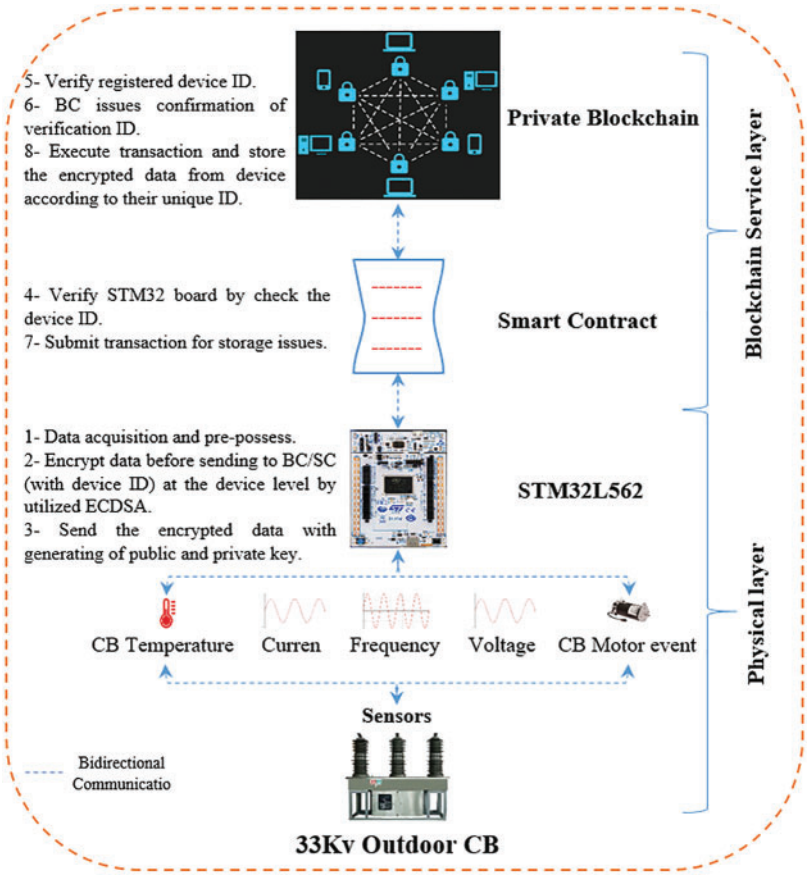

Figure 4: Electric CBs data acquisition and storage process

6 A Blockchain-Based Secure Smart Grid of the Al-Kufa Power Plant

The power capacity of the Al-Kufa power plant/Iraq is 30 MVA, and it consists of six power generators (each of 5 MVA), which are connected to provide the required power on demand. There are nine overhead power feeders with different voltages (6.6, 11, and 33) kV, which are connected between the power plant and loads at different distances from the power plant as depicted in Fig. 5. The power plant is also connected to the Iraqi main electrical power network (via two overhead lines) to boost the stability of the supply to the 30 MVA power plant, especially during the starting periods of high-power loads such as the slip-ring motors used in the cement and raw mills (0.97, 1.9, three of 3.4, four 1.7 MW) at the Al-Kufa and Al-Najaf cement factories. The Al-Kufa power plant feeds the Al-Najaf cement plant, and the Al-Kufa cement plant (two feeders), a limestone quarry, the Al-Najaf gas power plant (two feeders), a residential area (two feeders), and an external water treatment station. All of these power feeders contain outdoor overhead CBs, which are installed at the sending and receiving ends of transmission lines to allow each feeder to observe and control the network status. Wireless communication technology is used to enable communication between smart devices in industrial applications through the global internet network, and to provide real-time data processing, control and monitoring. The security of such networks has become a crucial factor, without a trusted

security system, the wireless communication technology in SGs becomes useless, as sensitive data can be exploited by attackers to control and disrupt the whole system.

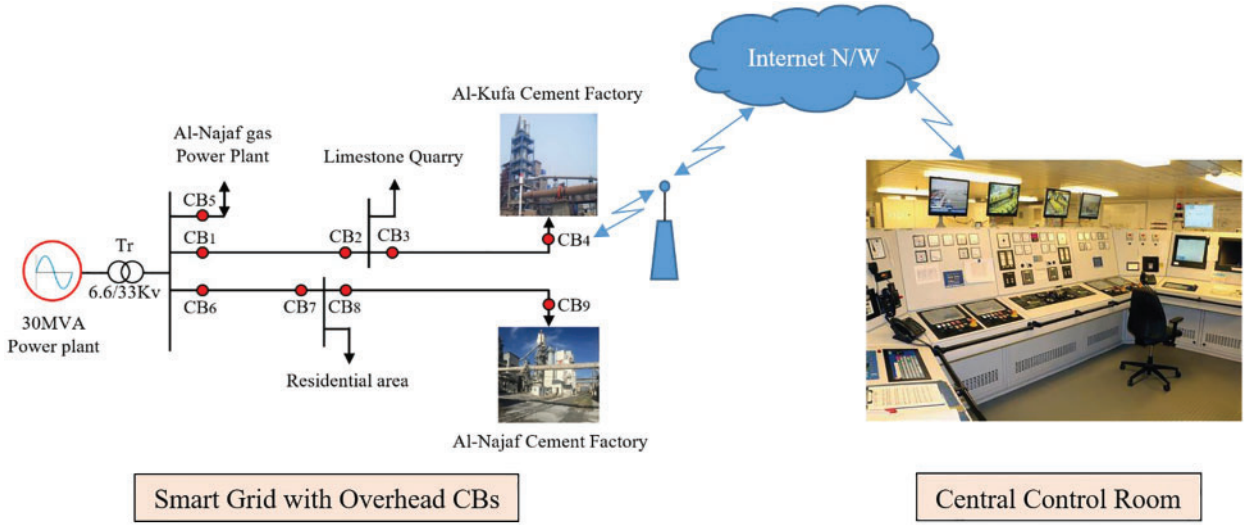

Figure 5: Al-Kufa power plant grid

In our work, we designed an efficient, lightweight, scalable, resource-constraint friendly and trusted security architecture for electrical power transmission lines as an important part of electrical SGs. Our architecture can successfully realize the integration of BC technology with IoTs in the industry sector and provides a trusted security framework for the sensitive data that is transferred between smart CBs and the CCR in an electrical SG. It also enables the autonomous operation of CBs (switching on or off) according to power feeder events.

Our scheme consists of three main layers, the physical layer, the BC service layer and the application layer as discussed in detail in Section 4. All transactions are hashed using SHA-256, time-stamped, and encrypted with ECC; this provides a high level of security, immutability and a secure environment that can effectively resist most potential cybersecurity attacks on power transmission lines in electrical SGs, such as Sybil, impersonation, replay, key compromise, DoS, DDoS, MITM and modification attacks [9,45].

The integration of BC technology with IIoT devices achieves high performance and an excellent security environment for IoT networks in SGs. In our work, the use of a smart contract enables BC network participants to realize the exchange of information without the need for a trusted third-party service and provided the immutability feature, which means that the collected data cannot be changed or modified by an attacker, or even by the network participants themselves (internal or external attacker). Moreover, our scheme enables the CBs to react rapidly to new events (autonomously), which effectively enhances the power quality, boosts the stability of the voltage, reduces the wastage of electrical power, protects devices and network equipment from damage, and increases the economic benefits.

7 Performance Analysis

We evaluated our proposed architecture from the fourth perspectives of cryptography, execution time, memory usage and power consumption.

7.1 Performance of the ARM Cortex-M33 for Asymmetric Cryptography

In our work, we adopted an ARM Cortex-M33 microprocessor for its numerous features in terms of ultra-low power consumption, high performance and support from the STMicroelectronics library. It is also certified for industrial use (in IoT applications) by the national institute of standards and technology for cryptographic algorithms [36]. These features make it an ideal choice for real-time processing applications [35].

We implemented the asymmetric encryption algorithm at the physical layer of our architecture and evaluated the performance of ECDSA with four selected Cortex-M series (M3, M4, M7, and M33) using the X-CUBE-CRYPTOLIB library (simulator) [36]. We computed the execution time, memory usage and power consumption for each one, based on the mean ($\overline{X}$), standard error (δX) and standard deviation ($\delta\overline{X}$), as shown in Tables 2 and 3. The X-CUBE CRYPTOLIB library was used in our implementation, which helped to achieve the requirements of the application in terms of data gathering, integrity, confidentiality, availability, non-repudiation and authentication.

The presented results in the next subsection show that the ARM Cortex-M33 and M7 microprocessors were the ideal selection, particularly for the case of real-time cryptography, as used in IIoT applications. The M33 was the best choice for the implementation of cryptographic algorithms in real-time and gave an enhanced performance for IIoT applications due to its low execution time, high RAM capacity and lowest flash memory usage for ECDSA. It also achieved a lower power consumption than the M7.

Table 2: Execution time for ECDSA with different M-series.

Processor	$\overline{X}$ (s)	δX (s)	$\delta\overline{X}$ (s)
M3	21.0815	0.004	0.0013
M4	1.1236	0.000	0.000
M7	0.9256	0.000	0.000
M33	0.7424	0.000	0.000

Table 3: ECDSA RAM usage for Cortex-M-series.

Processor	Total size (byte)	Used size (byte)	Usage %
M3	16 K	8.02 K	50.01
M4	256 K	8.04 K	3.14
M7	512 K	8.05 K	1.57
M33	786 K	16.02 K	2.03

7.2 Execution Time

Execution time can be defined as the exact time required or consumed by a cryptography algorithm (such as ECDSA) for encryption, decryption, and key creation. Our implementation used an HP Pavilion laptop with a Core (TM) i7-7700HQ CPU (2.80 GHz, 16 GB RAM, 64 bits) for simulation in the STM library. We repeated the execution process for ECDSA for each selected microprocessor (M3, M4, M7, and M33) 10 times as clear in Fig. 6. Then recorded the results and computed the mean value $\overline{X}$ as shown in Table 2.

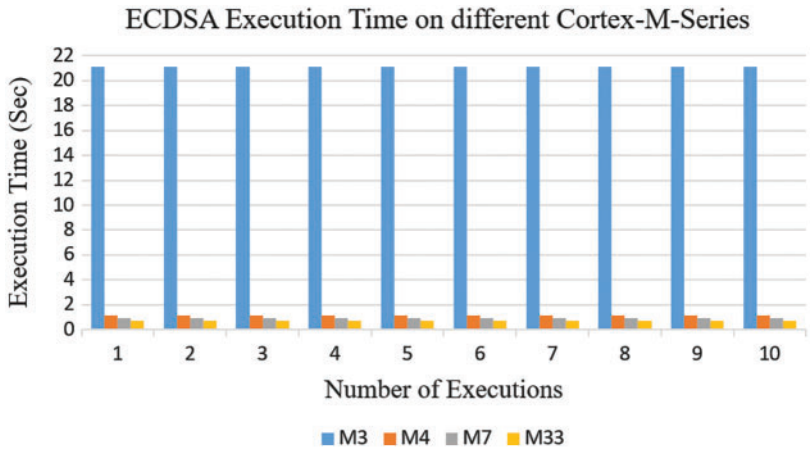

Figure 6: Execution time of ECDSA on STM32L562

From the results, we found that the lowest execution time for ECDSA was obtained with the M7 and M33 processors due to their high performance (making these the optimal selections), while we found the highest value of execution time for another series. We selected the M33 processor for our scheme in order to strike a balance between the three factors of execution time, memory usage, and power consumption as described in detail in the following subsections.

7.3 Memory Usage (RAM, Flash Memory)

Memory usage is also an important factor and represents the percentage of use of the RAM and ROM for our implementation of the ECDSA. We analyzed the Map file that was generated automatically by the toolchain, which provides a detailed analysis of the RAM and ROM utilization. From the Map file, we can find many data types such as Code, RO-Data, RW-Data, and ZI-Data with their details related to size and exact locations. We calculated the RAM and flash memory usage based on Eqs. (1) and (2) [47] as shown below:

$$\text{RAM\_Usage} = \text{ZI} - \text{Data} + \text{RW} - \text{Data} \tag{1}$$

$$\text{ROM\_Usage} = \text{Code} + \text{RO} - \text{Data} + \text{RW} - \text{Data} \tag{2}$$

Memory usage percentages are highly dependent on the sizes of the RAM and flash memory, which differ according to the development board used. We were not aiming to achieve very low percentage values, but only acceptable ones that would provide a balance between the use of the RAM and flash memory, execution time and power consumption.

RAM: This differs according to the processor series, each of which has a different RAM capacity. Our experimental results from ECDSA show that in comparison with the total capacity, the M3 processors had a high rate of RAM usage (using 50% of the available total capacity). The M4, M7, and M33 processors are provided with large amounts of RAM, which helped to give lower proportions of RAM usage, as summarized in Table 3.

Flash memory: This memory holds the main code; it is usually larger than the RAM and holds many types of code and data. The results obtained for the ROM usage for ECDSA are given in Table 4. From the experimental results, we can see that the Cortex-M3 processor has a high rate of flash memory usage in comparison to its total capacity (20.57%). The M4, M7, and M33 processors have larger sizes of flash memory and therefore smaller usage percentages of their total capacity when executing tasks. From Tables 3 and 4, we can adapt the M33 microprocessor due to its high RAM capacity and flash memory. From the perspective of RAM, M7 and M33 had the highest capacity, and we selected M33 for its total RAM size(786 Kb) as it was larger than M7 by (35%) and used only 2.03% of its full capacity. From the perspective of flash memory, the microprocessor M33 is the optimal one due to its lower percentage (0.98%) usage than the other processors as clear in Table 4.

Table 4: ECDSA Flash memory usage for Cortex-M-series.

Processor	Total size (byte)	Used size (byte)	Usage %
M3	128 *K*	26.33 *K*	20.57
M4	2048 *K*	25.17 *K*	1.229
M7	2048 *K*	27.45 *K*	1.34
M33	2048 *K*	20.24 *K*	0.98

7.4 Power Consumption

With the resource-constrained devices found in IIoT applications, electrical power consumption becomes a very important factor. Efficient devices are required to achieve the lowest possible power consumption. In our scheme, we used the ultra-low power consumption ARM Cortex-M33 for data pre-processing and encrypting the data received from the CB sensors before transferring it to the CCR.

The power consumption is the exact required time to execute the ECDSA by the M33 Microcontroller, and is calculated based on Ohms Law as shown in Eqs. (3) and (4) below:

$$\mathrm{I} = \frac{\mathrm{V}}{\mathrm{R}} \tag{3}$$

where I represents the Microprocessor current during the execution time, V represents the Microprocessor supply voltage (5.0 V). While R represents the Microprocessor resistance (1.0 Ω).

$$\mathrm{P} = \mathrm{V} \times \mathrm{I} \tag{4}$$

The average power consumption for the Microprocessor calculated by running the ECDSA 10 times as clear in Fig. 7. From the results presented in Table 5, we note that all of the processors (M3, M4, M7 and M33) had low power consumption, and can all be considered energy-efficient in terms of implementing ECDSA. We adopted M33 as it had a lower power consumption rate than the other options.

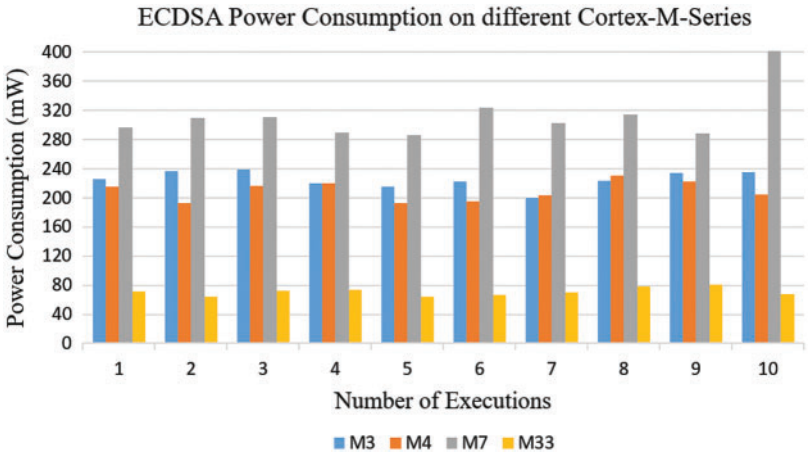

Figure 7: Power consumption of ECDSA with different M-series

Table 5: Cortex-M power consumption for ECDSA.

Processor	$\overline{X}$ (mW)	δX (mW)	$\delta\overline{X}$ (mW)
M3	224.867	11.364	3.371
M4	209.010	14.17	4.480
M7	302.827	14.5	3.905
M33	70.880	5.332	2.309

8 Performance Comparison with Alternative Schemes

From the related work reviewed in Section 2, we found that only one researcher had addressed the issue of security of SGs in the electrical power sector/smart CBs [11], in a study which dealt with the smart CBs and their security authentication using a hash function for authentication, and a symmetric algorithm for privacy issues. The author of the study paid more attention to the authentication speed (in terms of sending and receiving times) than to resistance to potential security attacks. In addition, although several of the articles reviewed in section 2 adopted BC technology [11,24,26]. They focused only on the features of BC in terms of data recording and backtracking; did not address the other features of BC technology regarding ensuring secure, trusting, scalable, and decentralized architecture for the industrial environment, which provides system scalability, access control, immutability, distributed applications, information backtracking and data integrity of a control system.

They also did not provide a clear method for protecting the sensor's data at the control and protection devices of SGs at the device level. Table 6 shows a detailed comparison of the various methods identified in the literature review with our scheme in terms of the BC platform used, the cryptographic scheme, type of mechanism, type of consensus mechanism, computation cost, authentication time, access control, potential security attacks, and dependency on third parties.

Table 6: Performance comparison of our scheme with other works.

Author	Blockchain platform	Cryptography scheme	Mechanism	Consensus mechanism	Computational cost	Authentication consuming time (ms)	Access control	Potential security attacks	3rd party dependency
[8]	Public	ECC & SHA-256	Decentralized	PoC	Middling	Middling	Yes	E, I, J, K, M, N, O	No
[11]	–	SKA	Centralized	-	Middling	Low (14.10)	Yes	A, B, C, D, E, F, G, H, O, P, Q	No
[13]	Ethereum	SHA-256	Semi-Decentralized	-	Low	Middling	No	A, B, C, E, I, J, M, K, O	Yes
[21]	–	ECC	Centralized	-	High	Middling	No	A, B, C, D, E, F, G, H, I, J, K, L, O	Yes
[25]	Ethereum	SHA-256	Decentralized	PoC	High	High	No	C, E, F, G, I, J, M, N	Yes
[26]	Ethereum	–	Centralized	ABI	High	High	Yes	A, B, E, F, G, J, K, O	No
[Our Scheme]	Private	ECC & SHA-256 & ECDSA	Decentralized	McPoRA	Lightweight	Lowest (3.9)	Yes	No	No

Note: ***A: Single node crash, B: Bottleneck, C: MITM, D: Impersonation, E: Sybil, F: DoS, G: DDoS, H: Repudiation, I: Anonymity, J: Privacy, K: Authentication, L: Tamper, M: 51%, N: Double spending, O: Confidentiality, P: Key Compromise, Q: Eavesdropping.***

The first criterion in our comparison is the BC platform. The authors of [20,21] depended on a traditional approach in the building of their security scheme by adopting an open-source platform; this is used in most schemes to provide an appropriate quality of service but depends entirely on a trusted third party or central authority, such as that described in [13,21]. In general, this external dependency can expose the whole system to many kinds of security risks such as single-node crashes and bottlenecks, and also can slow down the execution of the whole network due to the increase in the number of mutual authentication messages between the internal network and the trusted authority, which increases the power consumption of the network components and exhausts the bandwidth.

In our scheme, we adopted a decentralized architecture based on BC technology to build our private network, which fully eliminates the need for trusted third-party services, thus eliminating related problems such as the continuous issuing of authenticated certificate and revocation lists, latency, bandwidth size, single point of failure, and bottlenecks. This decentralized approach makes it more feasible for use with resource-constrained devices in industrial environments such as in electrical SGs.

The second criterion in our comparison was the cryptography scheme used to ensure transactions and user identities. Several cryptographic schemes were adopted in the works reviewed above, such as the advanced encryption standard (AES) [48], ECDSA [9], IBS [24], and PKI [28] all of which have certain advantages and disadvantages. ECC and a session key agreement (SKA) were adopted by the authors of [21] and [11] respectively, which are vulnerable to eavesdropping and key compromise. These schemes did not adopt the BC platform/decentralized application as used in [13,8,26]. The authors of [13,25] used SHA-256, whereas the author of [8] utilized both ECC and SHA-256 cryptography. In contrast, we utilized ECDSA for its efficiency, low memory requirements and low computational complexity to provide encrypted data at the physical layer before sending it to the BC service layer, in addition to the ECC and SHA-256 method that is adopted in the BC structure to ensure transactions.

The third criterion of our scheme was the mechanism used. The authors of [20,21,26] adopted a centralized architecture, while the authors of [13,8,25] adopted a decentralized approach. In our work, we adopted a decentralized mechanism to provide distributed collaborating processing, distributed databases, continuous service availability and scalability, which efficiently increases the system performance, and data availability and helps to eliminate the drawbacks of single node crashes and bottleneck problems. All users in the network have a full copy of transactions, which are time-stamped and hashed to prevent tampering.

The fourth criterion in our comparison was the consensus mechanism, which is responsible for controlling the process of adding new proposed transactions to the BC network after the validation and authentication process by utilizing a specific consensus algorithm. Due to the presence of resource-constrained devices in the IoT and the associated scalability issues, the consensus mechanism becomes a crucial factor, it must be lightweight. The authors of [13] did not discuss the consensus mechanism they adopted, while the studies in [11,21] did not adopt BC technology. The authors of [8,25] used PoC in their work, while the scheme in [26] depended on the application binary interface (ABI) as shown in Table 6.

Most of these traditional consensus mechanisms are not compatible with resource-constrained devices; the PoC algorithm has high-energy requirements, meaning that it is not suitable for low-power computational devices [9]. In our scheme, we used McPoRA as a consensus algorithm, which has the lowest energy consumption for block authentication [17] and is faster than other consensus algorithms as clear in Table 1. It was specially designed to reduce the latency and the consumption of energy for each transaction by achieving the lowest possible validation and authentication time.

The fifth criterion was energy consumption, which depends on the efficiency and performance of the IIoT devices used, and the type of consensus mechanism and encryption method. Most of the schemes reviewed here can be considered inefficient in terms of power consumption. In our scheme, we utilized the energy-efficient McPoRA as a consensus mechanism, which eliminated third-party dependency; and the efficient, lightweight ECDSA with the ultra-low power consumption and high-performance ARM Cortex-M33, which helps to reduce the computation process and hence the power consumption even further. From the experimental results (Table 5), it is clear that our scheme is more energy-efficient than the alternatives.

The sixth criterion in our comparison was the computational cost, as this represents a very important factor that depends on the type of system architecture, the encryption methods used, and the consensus mechanisms adopted. Most traditional security schemes depend on a centralized architecture, which used complex algorithms such as PKI [28,49], PoW, PoS, and PoC [8,25], and rely on a trusted third party in the verification and authentication process [13,21,25]. All of these schemes can be classified as having high computational and communicational costs.

In our architecture, we adopted a decentralized mechanism and a lightweight consensus algorithm (McPoRA) to reduce the computational and communicational burden. In addition, we used the SHA-256 hashing mechanism, which results in improved scalability and reduced complexity. The ECDSA was used, as this algorithm is characterized by efficiency, low memory requirements and low computational complexity. Our experimental results (as in Table 6) show that we achieved the lowest execution time and lowest computational cost.

The seventh criterion in our comparison was the time required to complete the verification and authentication process for new proposed transactions; this affects the performance of the proposed scheme and depends on the performance of the consensus algorithm, the resources used, the execution time, and the energy efficiency. The experimental results showed that our framework provided a high throughput of transactions per second and achieved the lowest execution time (3.9 ms) in comparison with the scheme in [11], which aimed to secure CB data in SGs and required 14.10 ms for data authentication. We carried out a comparison of the authentication time only between our schemes and the model in [11], as this was the only one closely related to our work (dealing with CB data in SGs). The scheme in [21] required 17.87 ms, while the authors of the other schemes (as in Table 6) did not compute the authentication time.

The eighth criterion of our comparison was access control, which can be considered an efficient and effective way to address illegal access issues. Access control refers to the process of identifying who can access the system and for what purpose. Industrial IoT resources are susceptible to illegal access by unauthorized users, which can threaten the safety of the system [13,26] and take over the process of starting or stopping power plants, circuit breakers, machines and equipment [11]. It can be seen from Table 6 that the authors of [13,21,25] did not consider access control in their schemes, while the authors of [11,8,26] did provide access control mechanisms.

In our work, we provide efficient access control by adopting private BC technology/smart contracts and an efficient consensus algorithm as an effective solution to prevent unauthorized access to the sensitive data of overhead CBs and the overall electrical SG system through a private network [50], meaning that our model is resistant to many malicious threats and attacks. The emergence of BC technology is one of the most promising technologies for reaching a common consensus in a distributed environment. The use of a consensus mechanism can ensure robust and trustworthy access control that is resistant to tampering and can therefore support successful applications such as Bitcoin [26]. In decentralized schemes such as the one in our work, instead of a single server, the majority of the nodes

are responsible for access control processing; this means that even if an attacker succeeds in exploiting a vulnerable point in one node, further action is impossible as each of the network participants has a copy of all encrypted and hashed transaction. Due to its numerous desirable features, BC faces increasing interest in terms of achieving decentralized and trustworthy access control for IoT applications.

The ninth criterion of our comparison was the potential for security attacks, in which attackers aim to exploit the vulnerable points in the system to reach their goals. The authors of [8] used PoC as a consensus algorithm, and the overall system is susceptible to Sybil, confidentiality, anonymity, privacy, authentication, double spending, and 51% attacks [9,45,51]. The author of [11] adopted a conventional encryption mechanism (SKA) and a centralized architecture, the overall system is susceptible to single node crashes, bottleneck, MITM, impersonation, Sybil, DoS, DDoS, repudiation, confidentiality, key compromise and eavesdropping attacks.

While the scheme in [13] depended on a trusted third party, semi-centralized architecture and miners for authentication purposes and did not provide an access control mechanism, the overall system is susceptible to single node crashes, bottleneck, MITM, Sybil, anonymity, privacy, 51%, authentication and confidentiality attacks. As discussed in detail in Table 6.

The authors of [21] adopted a centralized mechanism and did not provide access control, the overall system is susceptible to single node crashes, bottleneck, MITM, impersonation, Sybil, DoS, DDoS, repudiation, anonymity, privacy, authentication, tampering and confidentiality attacks. The authors of [25] used PoC as a consensus algorithm and depended on a trusted third party, also did not consider access control, meaning that the overall system is susceptible to MITM, DoS, DDoS, anonymity, privacy, double spending, 51% and Sybil attacks [9,45,51]. While the scheme in [26] depended on a centralized mechanism and utilized ABI as a consensus mechanism, and was therefore susceptible to numerous security threats such as single-node crashes, bottlenecks, and MITM, repudiation, confidentiality, privacy, Sybil, DoS, DDoS and authentication attacks [24].

Our architecture was efficiently resistant to all of the aforementioned cybersecurity attacks as it was based on a private BC and smart contracts; used a double layer of encryption at the perceptual layer by adopting ECDSA to encrypt data at the device level before sending it to the BC service layer. It also used the efficient, fast and lightweight McPoRA consensus algorithm. In BC technology, all transactions are also hashed using SHA-265, encrypted with ECC and timestamped [9], which helps to prevent attackers from being able to change, modify or steal sensitive data. In SGs, cybersecurity is the biggest challenge [52], according to the guidelines issued by NIST [48].

The last criterion of our comparison was a dependency on a third party. The authors of [13,21,25] built their authentication schemes around a trusted third party, as discussed above, an approach which exposes the whole system to security vulnerabilities and computational overheads. In our scheme, we eliminate any external dependencies by adopting BC technology/smart contracts and an efficient consensus algorithm to validate and authenticate new proposed transactions. In addition, our architecture provides an efficient solution to cybersecurity threats by satisfying its three fundamental requirements (availability, integrity, and confidentiality). Firstly, availability is achieved through the use of a decentralized architecture and a distributed database, in which all users have a copy of all transactions, which are continuously updated. The second requirement is integrity, which is achieved by the use of BC/smart contracts to provide immutability, time stamping, information backtracking, and tamper-proofing for all ledgers. The third requirement is confidentiality, which is achieved in the physical layer and the BC service layer in which all transactions are hashed and encrypted, and only a validated and authenticated transaction can be added to the BC network. In addition, this provides a balance between information security and computation time.

9 Conclusion

The security and privacy of the communication and control system between the overhead electric CBs and the CCR in an electrical SG is a crucial factor. In this work, we have proposed an efficient, trusted, scalable, decentralized, low power consumption and lightweight authentication and privacy-preserving scheme with a high level of security based on the use of private BC technology/smart contracts. Thus, it offers data integrity, availability, and authenticity, tamper-proofing, information backtracking, efficient access control and trusted security architecture for the overhead electric CBs data in the Al-Kufa power plant.

Our scheme adopted a lightweight and efficient asymmetric cryptography algorithm, which efficiently reduces the communication and computation overhead through the utilization of the STM32L562 development board (TrusZone) that achieves the lowest execution time for the cryptographic algorithm (ECDSA), memory utilization, and power consumption compared to other schemes. In addition, the data encryption strategy at the perceptual layer provides a high level of data security. Moreover, the McPoRA consensus algorithm helps to reduce latency, avoid the 51% attacks, releases mining fees, requires low energy consumption, and gives high throughput and scalability. The experimental results show that the proposed scheme reduces the computational and communicational burden and efficiently resists most potential cybersecurity threats that making it an ideal solution for the resource constraint devices in an industrial environment.

Funding Statement: This work is supported by the National Key R&D Program of China under Grand No. 2021YFB2012202, and the Key Research Development Plan of Hubei Province of China under Grant No. 2021BAA171, 2021BAA038, and the project of Science Technology and Innovation Commission of Shenzhen Municipality of China under Grant No. JCYJ20210324120002006 and JSGG20210802153009028.

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

References

[1] Y. Arafat, L. Tjernberg and P. A. Gustafsson, "Remote switching of multiple smart meters and steps to check the effect on the grid's power quality," in *2014 IEEE PES T&D Conf. and Exposition*, Chicago, IL, USA, IEEE, pp. 1–5, 2014.

[2] T. W. Jones, J. Mendon and C. Inacio, "Measuring electric energy efficiency in portuguese households: A tool for energy policy," *Management of Environmental Quality: An International Journal*, vol. 26, no. 3, pp. 407–422, 2015.

[3] Y. Liu, T. Liu, H. Sun, K. Zhang and P. Liu, "Hidden electricity theft by exploiting multiple-pricing scheme in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2453–2468, 2020.

[4] E. Hossain, I. Khan, F. Un-Noor, S. Sikander and M. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[5] P. R. D. Araujo, R. H. Filho, J. J. Rodrigues, J. P. M. Oliveira and S. A. Braga, "Infrastructure for integration of legacy electrical equipment into a smart-grid using wireless sensor networks," *Sensors*, vol. 18, no. 5, pp. 1312, 2018.

[6] H. Karbouj and S. Maity, "On using TCBR against cyber switching attacks on smart grids," in *2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia)*, Melbourne, VIC, Australia, IEEE, pp. 665–669, 2016.

[7] W. Ren, X. Wan and P. Gan, "A double-blockchain solution for agricultural sampled data security in internet of things network," *Future Generation Computer Systems*, vol. 117, no. 4, pp. 453–461, 2021.

[8] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq *et al.,* "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.
[9] S. M. Umran, L. Song, Z. A. Abduljabbar, J. Zhu and J. Wu, "Secure data of industrial internet of things in a cement factory based on a blockchain technology," *Applied Sciences*, vol. 11, no. 14, pp. 6376, 2021.
[10] C. W. Long, L. C. Huang and J. Tao, "Blind false data attacks against ac state estimation based on geometric approach in smart grid communications," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6298–6306, 2017.
[11] I. T. Aziz, H. Jin, I. H. Abdulqadder, Z. A. Hussien, Z. A. Abduljabbar *et al.,* "A lightweight scheme to authenticate and secure the communication in smart grids," *Applied Sciences*, vol. 8, no. 9, pp. 1508, 2018.
[12] G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.
[13] Y. Li, R. Rahmani, N. Fouassier, P. Stenlund and K. Ouyang, "A blockchain-based architecture for stable and trustworthy smart grid," *Procedia Computer Science*, vol. 155, no. 3, pp. 410–416, 2019.
[14] A. Dua, N. Kumar, M. Singh, M. S. Obaidat and K. -F. Hsiao, "Secure message communication among vehicles using elliptic curve cryptography in smart cities," in *2016 Int. Conf. on Computer, Information and Telecommunication Systems (CITS)*, Kunming, China, IEEE, pp. 1–6, 2016.
[15] Z. Li, R. Y. Zhong, Z. -G. Tian, H. -N. Dai, A. V. Barenji *et al.,* "Industrial blockchain: A state-of-the-art survey," *Robotics and Computer-Integrated Manufacturing*, vol. 70, no. 1, pp. 102124, 2021.
[16] P. Singh, M. Masud, M. S. Hossain and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Computers & Electrical Engineering*, vol. 93, no. 1, pp. 107209, 2021.
[17] A. Alkhodair, S. Mohanty, E. Kougianos and D. Puthal, "Mcpora: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Limassol, Cyprus, IEEE, pp. 446–451, 2020.
[18] D. P. Bernardon, V. J. Garcia, L. L. Pfitscher, M. Sperandio, L. N. Canha *et al.,* "Smart grid concepts applied to distribution network reconfiguration," in *2012 47th Int. Universities Power Engineering Conf. (UPEC)*, Uxbridge, UK, IEEE, pp. 1–6, 2012.
[19] F. Hawlitschek, B. Notheisen and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electronic Commerce Research and Applications*, vol. 29, no. 31, pp. 50–63, 2018.
[20] J. Krenge, M. Scheibmayer and M. Deindl, "Identification scheme and name service in the Internet of Energy," in *PES Innovation Smart Grid Technologies Conf. (ISGT)*, Washington, DC, USA, IEEE, pp. 1–6, 2013.
[21] D. Sadhukhan, S. Ray, M. S. Obaidat and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart grid communication using elliptic curve cryptography," *Journal of Systems Architecture*, vol. 114, no. 11, pp. 101938, 2021.
[22] A. Tolba and Z. Al-Makhadmeh, "A cybersecurity user authentication approach for securing smart grid communications," *Sustainable Energy Technologies and Assessments*, vol. 46, no. 9, pp. 101284, 2021.
[23] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi *et al.,* "Detection and mitigation of cyber-attacks on voltage stability monitoring of smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5227–5238, 2020.
[24] R. Fotohi and F. S. Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," *Computer Networks*, vol. 197, no. 3, pp. 108331, 2021.
[25] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif *et al.,* "Securing the LoRaWAN join procedure using blockchains," *Cluster Computing*, vol. 23, no. 3, pp. 2123–2138, 2020.
[26] Y. Nakamura, Y. Zhang, M. Sasabe and S. Kasahara, "Exploiting smart contracts for capability-based access control in the internet of things," *Sensors*, vol. 20, no. 6, pp. 1793, 2020.

[27] A. K. Sangaiah, D. V. Medhane, G. -B. Bian, A. Ghoneim, M. Alrashoud *et al.,* "Energy-aware green adversary model for cyber-physical security in industrial system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3322–3329, 2019.
[28] M. Maier and N. Ghazisaidi, "FiWi Access Networks," United State of America, Cambridge University Press, New York, 2011. [Online]. Available: https://www.cambridge.org/9781107003224.
[29] M. Wen, J. Lei, Z. Bi and J. Li, "EAPA: An efficient authentication protocol against pollution attack for smart grid," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1082–1089, 2015.
[30] IMB documentation. [Online]. Available: https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-public-key-cryptography.
[31] T. Aziz, H. Jin, I. H. Abdulqadder, R. M. Imran and F. M. Flaih, "Enhanced PSO for network reconfiguration under different fault locations in smart grids," in *2017 Int. Conf. on Smart Technologies for Smart Nation (SmartTechCon)*, Bengaluru, India, IEEE, pp. 1250–1254, 2017.
[32] O. Badran, S. Mekhilef, H. Mokhlis and W. Dahalan, "Optimal reconfiguration of distribution system connected with distributed generations: A review of different methodologies," *Renewable and Sustainable Energy Reviews*, vol. 73, pp. 854–867, 2017.
[33] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PerCom workshops)*, Kona, HI, USA, IEEE, pp. 618–623, 2017.
[34] STM32 family of 32-bit microcontrollers based on the Arm® Cortex®-M processor. [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html.
[35] Arm ltd, "Microprocessor cores and technology," 2020. [Online]. Available: https://www.arm.com/products/silicon-ip-cpu.
[36] Stmicroelectronics, "X-cube-cryptolib: Stm32 cryptographic firmware library software expansion for stm32cube (um1924)," 2020. [Online]. Available: https://www.st.com/en/embedded-software/x-cube-cryptolib.html.
[37] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah *et al.,* "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181, no. 9, pp. 103007, 2021.
[38] D. Prashar, N. Jha, S. Jha, G. P. Joshi and C. Seo, "Integrating IoT and blockchain for ensuring road safety: An unconventional approach," *Sensors*, vol. 20, no. 11, pp. 3296, 2020.
[39] M. U. Hassan, M. H. Rehmani and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.
[40] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in *2019 IEEE Int. Conf. on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, IEEE, pp. 1–5, 2019.
[41] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, 2018.
[42] N. Teslya and I. Ryabchikov, "Blockchain platforms overview for industrial IoT purposes," in *2018 22nd Conf. of Open Innovations Association (FRUCT)*, Jyvaskyla, Finland, IEEE, pp. 250–256, 2018.
[43] T. F. Chiang, S. Y. Chen and C. F. Lai, "A tangle-based high performance architecture for large scale IoT solutions," in *2018 1st Int. Cognitive Cities Conf. (IC3)*, Okinawa, Japan, IEEE, pp. 12–15, 2018.
[44] S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUF chain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.
[45] S. Sayeed and H. M. -Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. 9, no. 9, pp. 1788, 2019.
[46] A. Ahi and A. V. Singh, "Role of distributed ledger technology (DLT) to enhance resiliency in internet of things (IoT) ecosystem," in *2019 Amity Int. Conf. on Artificial Intelligence (AICAI)*, Dubai, United Arab Emirates, IEEE, pp. 782–786, 2019.

[47] How to monitor flash and RAM usage after compilation?. [Online]. Available: https://devzone.nordicsemi.com/nordic/nordic-blog/b/blog/posts/rom-and-ram-management.
[48] N. Kumar, V. M. Mishra and A. Kumar, "Smart grid and nuclear power plant security by integrating cryptographic hardware chip," *Nuclear Engineering and Technology*, vol. 53, no. 10, pp. 3327–3334, 2021.
[49] A. A. Khan, V. Kumar, M. Ahmad and S. Rana, "LAKAF: Lightweight authentication and key agreement framework for smart grid network," *Journal of Systems Architecture*, vol. 116, no. 2, pp. 102053, 2021.
[50] B. Krishna, P. Rajkumar and V. Velde, "Integration of blockchain technology for security and privacy in internet of things," *Materials Today: Proceedings*, pp. 1–5, 2021. https://doi.org/10.1016/j.matpr.2021.01.606.
[51] S. M. H. Bamakan, A. Motavali and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, no. 10, pp. 113385, 2020.
[52] G. Dileep, "A survey on smart grid technologies and applications," *Renewable Energy-Elsevier*, vol. 146, no. 1, pp. 2589–2625, 2020.