# Designing A Blockchain Approach to Secure Firefighting Stations Based Internet of Things

Samaher A. Yousiff[1], Raad A. Muhajjar[2] and Mishall Al-Zubaidie[3,*]
[1]Energy Production for Southern Region, General Company of Electrical, Ministry of Electricity, Iraq
[2]Department of Computer Science, Faculty of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
[3]Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah, 64001, Iraq
E-mail: samaheraltumma@gmail.com, raad.muhajjar@uobasrah.edu.iq, mishall_zubaidie@utq.edu.iq
*Corresponding author

**Keywords:** BC, consensus algorithms, firefighting equipment, IoT, proof of authority, PoS, PoW, smart network, SHA-384

**Received:** October 31, 2023

*Although the idea of communication between devices is not new, its development has been rapid and significant since it helps people do their jobs more efficiently and keeps them fully informed of events at their homes and workplaces thanks to technology like the Blockchain (BC) based Internet of Things (IoT). However, this new technology suffers from security issues and the existing research has not addressed these issues in depth. In this paper, a simulation of the smart network of the firefighting station was made. BC technology was used with one of the consensus algorithms which was proof of authority (PoA) to make this network more secure and private, in addition to the use of a hash function such as secure hash algorithm 384 (SHA-384), which is a one-way encryption function and was used to verify the BC data integrity so that it was difficult to hack the data and thus be the data transmission process is more secure. Also, the Espressif 32 (ESP32) device was chosen for this project because it offers several useful characteristics, including Wi-Fi and the capacity for rapid data transmission. It was observed from the results obtained from the application of consensus algorithms that the firefighting station network was made more secure and the PoA algorithm was better in several aspects such as execution time (maximum 0.4 S) and memory used (maximum 610 KB). Finally, the proposed work that was applied to the firefighting station was good in terms of safety and privacy, as the work of this station became more efficient.*

*Povzetek: Predstavljen je razvoj varne IoT mreže gasilske postaje z uporabo bločne tehnologije in algoritma PoA za izboljšanje varnosti in zasebnosti.*

## 1 Introduction

This section is subdivided into fire science technology and firefighting stations and security issues.

### 1.1 Fire science technology

Each year, fire incidents result in the death or serious injury of numerous persons [1]. Since its discovery, fire events emerged, and they are directly correlated with the advancement and growth of human civilization. According to a world health organization (WHO) study, more than 300,000 individuals per year pass away from injuries caused by fire. However, disconcerting data reveals that low- and middle-income countries account for 95% of these deaths [2]. According to U.S. Bureau of Labor Statistics data from 2018, fires and explosions result in the deaths of 66 building employees each year [2]. The national fire protection association (NFPA) conducted five-year research (2010–2014) that found that after excluding one- and two-unit projects, home repair or construction projects caused $280 million in direct property destruction each year [3]. The advancement of fire science and technology has been extremely aided by the increased difficulties for fire safety brought on by economic development. Initially, the main goals of fire science and technology were to protect huge companies, buildings, and people from catastrophic fires [4]. In the area of monitoring and early detection for fire safety, extensive research has been done.

Numerous research studies have examined the detection of heat and smoke using a range of tools and techniques, including distributed temperature sensing (DTS), fiber optics connected to very early smoke detection apparatus (VESDA), linear infrared flammable gas detection, and dual infrared (IR/IR) spectral band flam detection [5, 6]. Some studies have concentrated on fire safety tracking and fire spotting, as well as preparing for evacuation from finished as well as ongoing structures and tunnels [7]. Fire safety management should be a top priority for every company, but it is especially critical in the construction

sector due to a variety of elements that frequently lead to major fire risks. First, many construction sites expose workers to combustible materials, and the presence of wind near unfinished structures can quickly start a fire. Second, the only preventive measures that building sites can use are portable firefighting equipment (PFE) or, occasionally, water tanks because they lack permanent and adequate fire protection systems. In this context, the occupational safety and health administration (OSHA) mandates that every construction project must have a site-specific safety plan that includes a fire prevention plan [8, 9]. The former was dealt with in a prior study utilizing a visual programming approach [10]. In the field of fire protection today, it is challenging to determine who is responsible based on the condition of the firefighting equipment after an accident because of the opaqueness of the maintenance of the equipment [11]. The majority of firefighting equipment on the market today manages identification information and usage status using obsolete handwritten recordkeeping. The industry has also embraced the technique of implementing a supervisory system to address the issue of the traceability of fire fighting equipment [12]. Manufacturers, dealers, and users of fire equipment can access the equipment information management system using the appropriate key [13] to sign in on behalf of their identities. With the use of Bluetooth and RFID technologies, they may also record and update the state of firefighting equipment. Employees can use and maintain information by logging on to the application using a 14-bit identity code to check the state of fire fighting equipment [12], which can successfully address challenges with data security, information sharing, and fire safety systems.

## 1.2 Firefighting stations and security issues

Some studies presented the technology of the IoTs with the BC and were applied to firefighting stations in government institutions such as electricity production, healthcare and agriculture companies, for the purpose of obtaining real data far from manipulation/tampering with it and delivering it to the control units correctly. The IoTs is a rapidly expanding field, and according to some recent research, there will be 26 billion IoT devices worldwide in 2020. The capabilities of IoT-restricted devices expand with the deployment of cutting-edge network technologies including cloud computing, fog computing and edge transparent computing [14]. One of the important things in the work of firefighting stations is sending the correct information to the control units, and since this data is transmitted through sensors distributed in important areas in companies and institutions, the data transfer process may be subject to change, whether by sabotage or a malfunction in one of the sensors [15, 16], especially, the work of these networks is centralized and thus leads to the exposure of these institutions and their employees to danger. Therefore, technology must be used that helps to transfer, maintain and ensure the transfer of data, and one of them is BC technology, which is a decentralized network where the data is distributed over all network nodes, so any change in the data, the transmitted or tampered data of one of the nodes is easily detected by the rest of the nodes when it is matched with its data.

The IoT is a central network that is controlled by a central server that is responsible for all transactions, and the rest of the network members are not entitled to participate in its work. When this central server is attacked [17], this causes the entire network to stop, so it lacks security in its work. There are technologies in charge to address this issue, the most important of which is BC technology, which is a distributed ledger, i.e. a decentralized network, where all participants in this network have the right to contribute to its work [18]. There are types of this technology, the most important of which is the public and private BC. The public BC is a network open to all. There is freedom of participation without restrictions, and this type is not preferred by companies because they prefer to form a network whose participating members are subject to certain conditions set by the institution and are limited to those working with it and refuse any participation by members outside this institution. The technology is the private BC, where the members of the network are selected by the company according to the conditions set by this institution.

An appropriate layer for an architecture that provides safe services for IoT devices is required in order to accommodate a large number of devices. The current architectures use a centralized system in which internet-connected IoT devices are linked to cloud servers. However, the rapid proliferation of IoT devices may lead to network problems such as bottlenecks, network congestion, bandwidth limitations, security risks, single points of failure, and service delays. A decentralized architecture is required to prevent these problems. There are certain decentralized large-scale systems already in existence, including peer-to-peer networks [19]. IoT devices employ RFID, wireless sensor networks (WSN), and other advancements in other technologies that detect, communicate, and act using already-existing network infrastructure that has been improved by IoT. As a result of the IoT, communicated machines are able to share data, exchange information with one another, and control goods remotely over the Internet, potentially without human intervention [20]. WSNs are among the technologies with the fastest growth rates as a result of the development of computer networks, wireless communication, and microelectronic mechanical systems [21]. One of the origins of the attack was the ”Internet of Things,” a term used to represent a network of connected devices that includes printers and other internet-connected gadgets [22]. These devices were targeted by the Mirai virus, which led to distributed denial of service (DDoS) assaults as well as brute force and collision threats. The frequency of attacks

on IoT devices increased in 2018, with 32.7 million occurrences being recorded. The key flaw in this situation was their dependence on a centralized cloud architecture as well as the lack of security protocols [23]. Addressing IoT security and privacy issues necessitates investigating and grasping the multiple components of the IoT architecture, identifying vulnerability areas in each section, and finding the proper solutions to detect any vulnerabilities. In October 2016, Dyn Inc., a DNS service, was targeted by a DDoS attack that Tens of millions of Internet protocol (IP) addresses were affected. The IoT is described as the fusion of the physical world with the Internet to create a smart, digitally managed environment. IoT technologies have improved and changed how people connect with the environment, each other, and their surroundings [20]. A decentralized alternative based on tamper-proof data exchange on a digital ledger might solve many of the issues with the centralized cloud approach. Every transaction on the chain may be signed, secured, and verified in BC systems. Editing or removing data blocks kept on the ledger is quite difficult. Although there are many different BC topologies available, they all follow the same core principles [23]:

- Transactions between the parties are signed using cryptography.
- Transactions are recorded using a decentralized approach on a peer-to-peer network on a distributed ledger.
- Agreeing with a decentralized strategy.

### 1.3 Main contributions

The following are the primary objectives of this study:

1. Ensuring the security of IoT-based firefighting stations by relying on BC procedures.
2. Implementing private BC and SHA-256/SHA-384 to meet the privacy and confidentiality of companies and institutions.
3. Using ESP32 devices to ensure the high performance of network devices, which is reflected in the overall performance of the network.
4. Applying PoA in BC transactions to meet the security requirements of firefighting stations.

### 1.4 Organization of research

Here is a characterization of the study route map: Section 1 includes a thorough overview. In Section 2, we investigate the related work about BC and IoT security. Section 3 presents the necessary prerequisites for the proposed approach. The scientific gap and solution are offered in Section 4. Section 5 of this manuscript describes our proposed approach. The outcomes of the suggested approach are examined in Section 6. Section 7 presents the study's conclusion. Future tendencies are introduced in Section 8.

## 2 Existing research related to the blockchain/IoT security

In this part of the paper, we will investigate existing research related to Firefighting station security when using BC and IoT, here we will explain the approaches used in this field and their drawbacks, see Table 1.
In order to handle fire events, Ali et al. [24] submitted a decentralized approach for access management, delegation and permission, with requests on event- and query-based delegation and permission for IoT applications. They also used BC technology to decentralize, protect, rely on, and verify delegation services. They used the PROMELA (process meta language) basic PROMELA interpreter model checker to investigate their suggested solution. The PROMELA model is also used to verify the mutual exclusion, verification and delegation characteristics stated in linear temporal logic (LTL). Nonetheless, they do not address the performance of networking devices when using IoT-BC which makes their approach slow when applying permission access and delegation.

Tukur et al. [25] suggested an edge-based, BC-enabled irregularity disclosure technique to guard against internal threats in firefighting station applications. The method starts by utilizing edge computing to bring treating nearer to the IoT devices, enhancing opportunity and reducing individual points of insufficiency. This reduces latency and bandwidth needs. Then, it integrates distributed edge with BC, which provides smart contracts, to execute the identification and rectification of irregularities in forthcoming sensor raw data. This draws on some parts of sequence-based irregularity disclosure. The evaluation of their method using datasets from actual IoT systems revealed that it accomplished the coveted outcome whilst preserving the data's integrity and availability, which is essential for the deployment of IoT platforms. They referred to the use of a hash function in their BC. However, they did not specify the message digest length, which is crucial for thwarting assaults.

Krishna et al. [26] discussed how wireless body area networks are used in conjunction with BC technology implementation methods employing sophisticated Solidity scripts and embedded programming to address firefighter issues. They asserted that the integration of implementation that was shown produced useful outcomes with BC technology in terms of cryptographic security techniques. Their approach relied on SHA-256 functions to prevent altered BC transactions, however, SHA-256 may not be sufficient to support high security sensitive applications such as firefighting stations.

To quickly handle the request for fire brigade response and safeguard claims against fire for the business owner in institutions, Kumar et al. [27] submitted a trusted service approach of the fire brigade and insurance claims solutions utilizing BC. In order to prevent significant fire damage, a

narrowband IoT-established network chopping is intended to relay actual-time data to the observation firefighting station. Additionally, a service queue length technique is used to choose the best fire station. On the Hyperledger Besu BC, a prototype of their strategy is created by the incorporation of Solidity-programmed smart contracts. However, their approach does not address the protection of BC transactions with hash functions which means that their approach could be vulnerable to the modification of transaction data by attacks.

Khan et al. [28] developed an integrated drone-based BC architecture in which drones, drone operators, firemen, and administrators are network users or nodes. All nodes in a distribution network can access data, ensuring continuous data exchange and reducing the problems posed by spatial distance. They came to a conclusion by talking about the challenges and possibilities of combining BC with other cutting-edge technology to control forest fires in distant areas. However, they did not analyze the performance of their approach, nor did they specify the type of BC used that most affects security.

A low-power IoT-based sensor network is created that can detect forest fires automatically and relay the position to a central observation station with push alerts in time of actual life. As a result, the spread of the fire and the damage it causes can be minimized [29]. This step enables the prompt alerting of firefighters and assists in the early detection of a fire. The suggested approach recognizes fires when smoke is present and when there is a significant rise in temperature. Additionally, the scheme records the humidity, temperature, rainfall, carbon dioxide, wind speed and light in various forest regions. Utilizing a long-range wireless transmitter, the sensor nodes communicate information to a hub, which then uses cellular Internet to transfer the information to the central observation station. However, their approach does not provide technology to secure their approach data in Firestation applications such as BC which is important in the management and security of these applications which makes their approach weak to threats attacks.

# 3 Necessary preliminaries for proposed approach

This section explains basic details related to the techniques and technology adopted in this research.

## 3.1 Component of internet of things

It is crucial to understand what the IoT is and how it works before learning about its components. The IoT, also referred to as the Internet of Everything, is a potentially revolutionary technological pattern that explains a variety of technologies, like short-range wireless communications, RFID, and search domains, that may connect real-world physical things to the environment of the Internet. The technology's methodology must also be understood. Data is sent from sensors or devices to the cloud server, where it is processed and converted into a language that the machine can understand. After the data has been processed, the results are converted into a language that the user can understand and are sent as a signal, message, or other form of communication [30]. As shown in Figure 1, an IoT system's five main components are nodes/sensors, connectivity, cloud, processing of data, and the user interface (UI) [31]:

**Nodes/Sensors**: These are fundamental IoT parts that gather information from IP-addressed devices. These devices could be as basic as monitors for the humidity and temperature in a room or as sophisticated as autonomous vehicles. These components frequently gather data related to the settings they have been given, like temperature or video. These sensors or gadgets work together as a unit rather than independently. Devices that may transmit data gathered from physical environments to the IoT ecosystem make up IoT structures [28].

**Connectivity**: Using local area network (LAN), Wi-Fi, satellite, Bluetooth, cellular, and other infrastructure technologies, sensors and other devices are linked to the cloud. As a result, IoT nodes connect to one another using common communication protocols as a consequence. For instance, Bluetooth low energy (BLE) and Wi-Fi are intended expressly for the applications of IoT. It is anticipated that the 5-generation (5G) cellular network will help the IoT by boosting capacity and speed [32]. The development of new techniques, e.g. edge computing, a modern paradigm for dispersed nodes, has been forced by the collection of huge amounts of data. In edge computing, processing and data are distributed where they are most required. Any data that the screened cloud can not treat, is transferred closer to the customer, decreasing the time of lag and boosting bandwidth. These devices or systems process the data, and only the most pertinent information is sent back to the central base for analysis [33].

**Cloud**: A vast network that accommodates IoT devices and apps is known as an IoT cloud. This comprises the servers and storage that are necessary for processing and real-time operations. An IoT cloud also includes the standards and services needed for connecting, managing, and securing diverse IoT devices and applications. Thanks to IoT clouds' on-demand, inexpensive hyperscale, businesses can take advantage of the huge potential of IoT without having to build the required infrastructure and services from scratch. To gather and process information from IoT nodes, such as sensors, and to remotely control the devices, the IoT cloud leverages cloud computing services. IoT cloud systems' scalability makes it possible to analyze massive volumes of data and to use analytics and artificial intelligence (AI) tools.

**Processing of data**: Data is handled by the software once it has been saved in the cloud. Before this data is of any

Table 1: Comparison of methods, findings and limitations of existing research

| Ref. | Methodology | Key findings | Limitations |
|---|---|---|---|
| [24] | BC with PROMELA | Verification of delegation and mutual exclusion | Applying for permission access and delegation reduces notably performance |
| [25] | Edge-based BC-IoT with irregularity disclosure | Data's integrity and availability are essential for the deployment of BC-IoT | Using hash message digest of unlimited length is a vulnerability for attacks |
| [26] | BC-SHA256 with Solidity scripts to compute sensors' data | BC-IoT to avoid attacking the transactions with intentional threats | SHA-256 is vulnerable to firefighting applications |
| [27] | Hyperledger Besu BC with narrowband IoT and a service queue length technique | Performance in terms of latency and throughput | No hash functions to prevent transaction modification |
| [28] | Drone-based BC architecture and physically unclonable functions | Conserving both power and the implementation area | Lack of analysis of BC performance and type |
| [29] | IoT-based sensor network to recognize fires | Record the humidity, temperature, rainfall, carbon dioxide, wind speed and light in various forest regions | No BC to manage and secure fire apps |

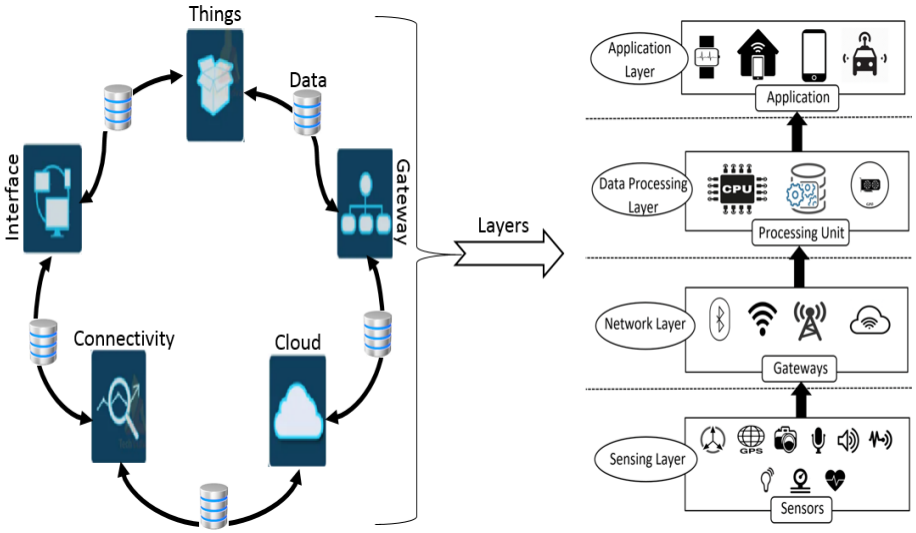


Figure 1: Components of IoT architecture

use, it must be carefully processed, filtered, and examined. Zettabytes of data are transmitted through each edge gateway prior to processing in order to prevent the system from becoming overloaded. Big data analytics uses cloud data analytics to evaluate production data at the highest level feasible by integrating corporate applications. IoT data is generated in real time and has a different structure. Massive volumes of IoT-created information need to be treated, assessed, and classified before they can be used in decision-making [34, 35].

**User interface (UI)**: Also, once it has been cleaned up and coordinated, the gathered information has to be utilized to notify the final clients. For instance, clients must be notified whenever the temperature in cold storage exceeds a certain point. This is made possible by using a user interface, which gives end users the chance to preview the data that has been collected. As a result, these end clients could respond to network inputs based on the applications of IoT [34, 36].

## 3.2 Blockchain technology

Blocks that have been cryptographically linked together form data structures known as BCs. It could serve as a secure historical ledger for the administration of data and transactions [37]. BC, the technology that powers Bitcoin, was first proposed by Satoshi Nakamoto. The security and immutability of BC have been proven to be two of its most important characteristics. Correspondingly, it could be a practical remedy for a variety of issues that traditional security schemes run into, such as privacy issues and centralized networks with bottlenecks and single points of breakdown [38]. Figure 2 illustrates the BC's structure. BC represents a technology that uses a peer-to-peer network to maintain an immutable distributed ledger. A consensus on the transaction statuses must be reached among network participants for transactions uploaded to a BC network to be valid. It is also critical to understand how this process works, which entails placing transactions in blocks with a variety of data, including nonce, timestamp, and prior hash, before using that data to strengthen the hashing of sensitive data. Next, under some circumstances, one of the consensus methods is used to pick up the node that will add this block to the BC [39]. The following are four fundamental properties of BCs [34]:

– **Ledger**: In order to give a thorough value-based history, advertising is documented in this fashion. BCs

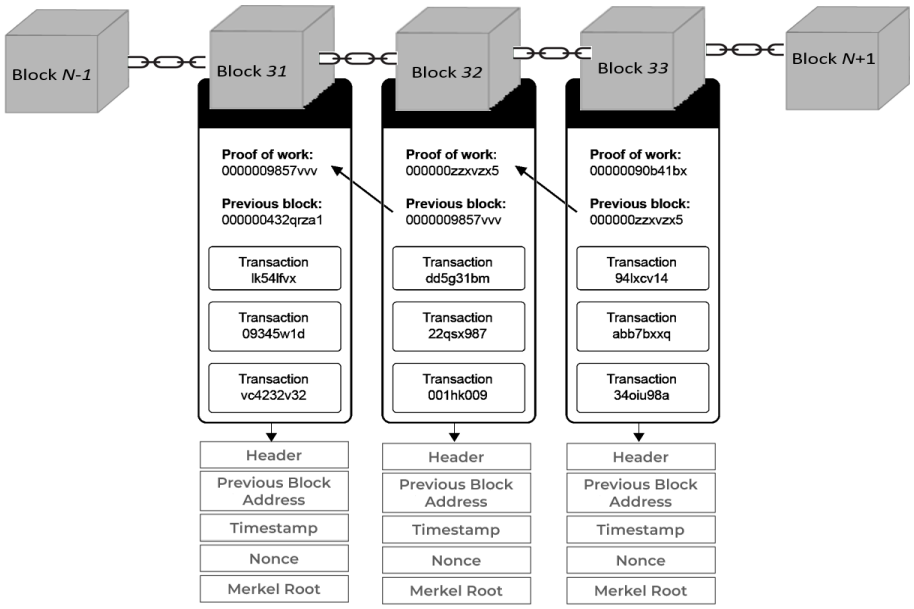


Figure 2: BC structure

do not have overruns, in contrast to conventional databases.

- **Secure**: No one can access the data recorded on a BC without authorization since it is encrypted.
- **Shared**: Each record involves numerous parties, which is why a hub member in a BC web.
- **Distributed**: To maximize flexibility and lower the likelihood of a successful assault, a BC can be dispersed and its node count can be altered. As the name implies, BC represents a collection of blocks with timestamps linked by cryptographic hash functions [40].

### 3.2.1 Hash function

A BC can be dispersed and its nodes can be added or removed to boost flexibility and lower the likelihood of a successful assault. As the name suggests, BC is a network of blocks with timestamps Interconnected by cryptographic hashes [41]:

1. Consent preimages of any length.
2. The computed image is the same for identical preimages.
3. Any preimage image has a set length that is easy to calculate.
4. Exhaustion is the only method to discover the preimage through the image.
5. It is difficult to locate a different preimage that matches the estimated image of a specific preimage.
6. The images before and after the modification are unrelated to one another; even little changes in the preimage result in significant changes in the image [42, 43].

### 3.2.2 Algorithm of consensus

The BC uses consensus techniques to make sure that every new block that is appended to the network is the only accurate representation of the data. A distributed/decentralized computer network has unanimity among all nodes. Because they guarantee the security and integrity of these distributed computing platforms, consensus algorithms are essential for BC networks [23]. There are many important consensus algorithms in BC:

**Proof of Work (PoW)**: It was the first technique used to arrive at an international consensus [44]. The PoW has historically been the most common method of reaching consensus inside BC designs. PoW makes it tough to create a legitimate block and connect it to a BC by searching for hash functions with difficulty proportionate to the network's processing power. After altering a block, a user must revalidate any further blocks. The more validations are required, the older the block that is being updated is. Even a newly validated block update is expensive since only a small number of miners or clusters of miners have the ability to manufacture fresh blocks every 10 minutes [23].

**Proof of Stake (PoS)**: It is a substitute strategy that was developed in response to criticism of PoW. With PoS, computing activity is replaced by a random selection process, and the likelihood of successful mining is inversely correlated with the number of validators. The likelihood of generating a block is influenced by the stake nodes' financial commitment to the network, or coin ownership.

**Proof of Authority(PoA)**: It was initially suggested as an extension to the Ethereum BC for monitoring Internet use

in response to the anxiety issues associated with PoW. The foundational principle of PoA is that only chosen, trusted nodes are permitted to produce new blocks. It is great for small networks and test nets despite centralizing the BC's total membership [45].

#### 3.2.3 Blockchain technology types

Public, private, consortium and hybrid BCs are the four categories [46].

1. Public BC: It allows for the observation of transactions by all users, but it conceals the identities of the initiating nodes [47]. A single entity does not govern this decentralized peer-to-peer network [47]. Figure 3 (a) describes the public BC [48].

2. Private BC: A BC with permissions establishes a set of privileges that users must possess in order to function on the network [46, 49]. The entity that owns this kind is the only one in control of block construction. A private BC is generally utilized by businesses to keep track of transactions or send information to a select group of consumers [20]. Figure 3 (b) describes the private BC [48].

3. Consortium BC: The BC network is controlled by a number of different entities in this semi-decentralized type. The private BC, which is administered by a single entity, is distinct from this. In this type of BC, multiple entities act as the central authority for information exchange and mining. BC technology is used by a number of sectors, including banking and government organizations [50]. Figure 3 (c) describes the consortium BC [48].

4. Hybrid BC: It refers to the integration of the two BC types, namely the private and the public BCs. By merging the best features of public and private BCs, this kind may achieve higher security and faster BC solutions. Due to the limitations of both private and public BC systems, hybrid BC allows the organization to have more influence over user preferences without having to make changes to their original desirations. Figure 3 (d) describes the hybrid BC [48].

### 3.3 Blockchain in IoT

The scientific community frequently uses WSNs, which are viewed as an essential part of ubiquitous computing because they have the ability to create and manage a wider range of data with higher resolution, the IoT has become a supporter of many areas. BC's features include decentralization, anonymity, persistency, and auditability [51]. Keep in mind that the special characteristics of BC may provide a remedy for IoT security problems. IoT systems have enhanced decentralization, resilience, security, and identity management. As a result, IoT networks can have a safe base thanks to the BC. Before being authorized and published to the distributed public ledger, transactions must first be validated by the majority of BC participants. This guarantees visibility and public visibility. Moreover, no central authority exists to sanction transactions or establish precise rules for participant communication or service access. Because most IoT application participants have to agree to authenticate transactions, there is a greater and more general level of trust [38, 52, 53]. Figure 4 illustrates IoT transaction data and how it could be protected by employing BC. Since the IoT composes a core network that transfers sensitive and essential data, security is one of the most crucial problems that must be resolved in this network. BC technology is one of the most crucial methods used to address security. When using the application programming interface (API) and the technology's built-in consensus methods, data is moved from the IoT to the BC network. After the data has been broken up into smaller pieces using the hash function, it is then saved in the form of blocks that will later be added to the BC after their validity has been confirmed by network nodes. Among the most important advantages of using the BC with the IoT are:

1. Making the IoT more secure, because the BC is a decentralized network, so the process of penetrating it is difficult.

2. It is more private, so it is preferred to be used in many companies and institutions.

On the other hand, there are some disadvantages in integrating the BC with the IoT, the most important of which are:

1. It needs high computing power.

2. It needs continuous energy because its work depends on the Internet, and in the event of any disconnection of the Internet, it leads to some problems.

## 4 Research gap and solution

This section explains the limitations, modelling and security requirements of Firefighting station systems.

### 4.1 Restrictions of existing construction fire safety administration practices

People have traditionally relied on themselves or neighbors to help with rescue and relief efforts in fire events in the distant past [34]. Several fires have broken out in construction sites over the past few years, many of which have resulted in significant property loss and fatalities [54]. To address the crucial issue of fire safety, several nations around the world have created various measures, such as updating fire safety codes and enforcing fire safety inspection procedures [55]. Falsifying and forging PFE paperwork or tags is a serious problem connected to the existing procedure, and multiple instances of this have been documented [56]. A building information modelling (BIM) relied on a strategy eligible of

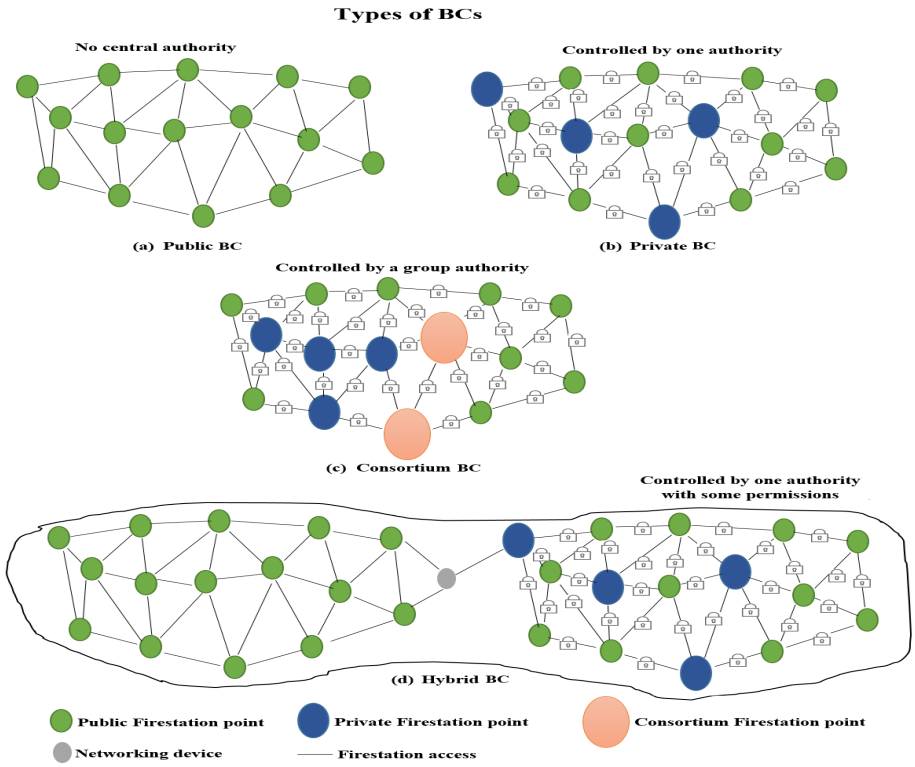


Figure 3: Types of BC networks for IoT

saving the essential data associated with these devices, such as manufacturer and device names, equipment type, maintenance personnel, exterior features, prior inspection/repair time, and other specifications, as well as the coordinates of the firefighting equipment's location, has been suggested to address this issue [9].

## 4.2 Constructing visual programming languages and information modeling languages

Construction is one of many worldwide businesses that a 51-percent assault (also known as a majority attack) is the most dangerous type of threat, in which a single miner can take control of the entire BC and make any transaction they choose. Although data are available in this situation, the attacker who controls the BC may be able to prevent transactions from taking place. This type of assault also compromises data security [40]. Several techniques to ensure security for IoT-BC applications have been proposed. Some have used machine learning techniques, while others have used more traditional methods [57]. BC technology has the potential to disrupt [58, 59] by providing distributed, encrypted, and ensure logging of electronic transactions data. Seven categories can be used to categorize previous initiatives to examine BC technology for various domains: smart homes, smart centres, smart cities, smart factories, smart transportation, smart governments, smart energy, organizational frameworks and business models, and BIM and construction administration [59].

The scope of the literature reviewed in this manuscript is restricted to research pertaining to buildings and construction, despite the fact that research on BC technology in the field of construction management is still in its early stages. This technology has the possibility to treat a few issues that block the construction industry from utilizing recent technologies such as BIM [60] by offering properties like disintermediation, confidentiality, non-repudiation, provenance tracking, change tracing, inter-organizational recordkeeping, and information ownership. For energy management, a hybrid strategy combining BC and BIM technology has been used to measure indoor temperature using IoT-based smart house devices [61]. To address one of the complex problems relating to the payment of wages to construction workers, a BC-based smart contract was introduced by Rofaida et al. (2023) [62]. However, no studies have been done yet that examine the application of BC technology in the process of checking and repairing construction gear, to the best of the authors' information. Optical character recognition (OCR) methods, on the other hand, involve preprocessing, segmentation, image acquisition, classification, feature extraction, and pattern recognition [61]. Numerous investigations have concentrated on character recognition through optical vision when using a BC and OCR. OCR technology attempts to translate any handwritten or typed text included inside an image into the text [61]; however, handwritten text recognition is more difficult than that of typewritten or printed text. In general, handwriting styles differ from person to person; hence, controlling these vari-

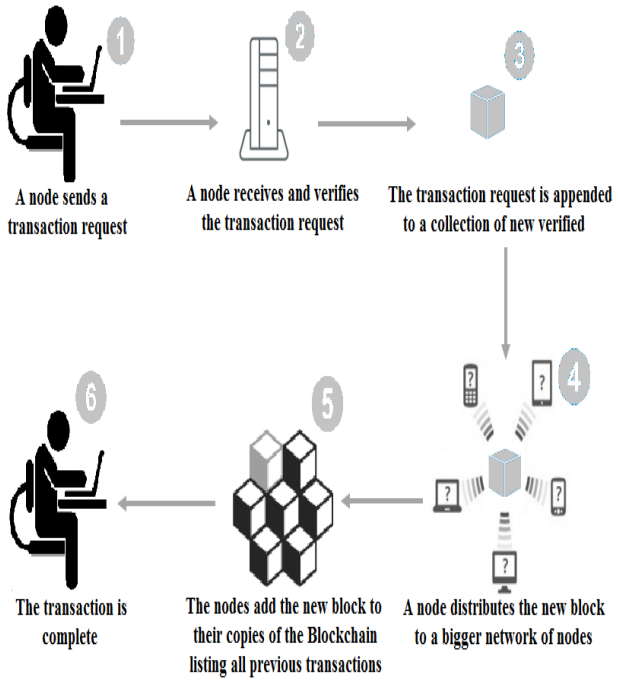


Figure 4: BC's work

ances is essential for OCR [63].

### 4.3 Security

An information system must traditionally meet three conditions to be secure:

- Confidentiality is one of the most important aspects of any business. Unauthorized access to the most sensitive data should be avoided.
- Integrity and reliability ensure that unauthorized parties cannot change or delete data. It is also common to include the requirement that if an authorized person messes with the information, the adjustments must be undo-able.
- Availability is when necessary, data can be accessed.

Regarding confidentiality, the previously addressed topic of their privacy is related to the section on transaction data. Existing IoT applications tend to consolidate connections in a server, a group of servers, or the cloud in terms of the architecture that supports the stored data. A strategy like this is workable as long as the centralized infrastructure's managers are reliable and the network is protected from both internal and external attacks [40]. A 51-percent assault (also famous as a majority threat) is the most dangerous kind of attack, in which a single miner could take control of the entire BC and make any transaction they choose. Although data are available in this situation, the attacker who controls the BC may be able to prevent transactions from taking place. This type of assault also compromises data security [40]. Several techniques to ensure security for IoT-BC applications have been proposed. Some have used machine learning techniques, while others have used more traditional methods [57].

## 5 Proposed approach methodology

This part of the research will explain the work details of the proposed approach.

### 5.1 General proposed framework

The proposed framework is presented in this section's general structure, which is divided into many phases, each of which serves a particular purpose. Since the outcome of one phase determines whether or not a user can move on to the next, these phases are interconnected. Components of our approach are temperature sensor, ESP32 device, server, PoA and network nodes. This effort involved simulating a firestation's smart grid as part of a power plant project. The ESP32 device was employed in this network due to its many benefits (such as Wi-fi capabilities, low energy, supporting Bluetooth, Rich PIO interface, dual-core, MicroPython compatibility, extremely cheap, MicroPython compatibility and supporting Arduino), and specific BC technology used to increase network security because it is appropriate for businesses and institutions. The PoA algorithm is one of the consensus algorithms used in BC. Also, the hashing function (SHA384) was utilized in this work. First, to raise the network's security, the simulation must be built on the IoT before the BC is connected. The phases of this proposed approach are depicted in Figure 5. The implementation of this work's mechanism is shown in the diagram. This IoT technique reduces the amount of time and effort needed to transfer information between nearby and distant locations, but it has a severe flaw that could affect the data being communicated over the Internet and render the station's personnel utterly unusable. Also, it results in a lack of electrical power supply, necessitating an increase in security for this system. It was determined to combine BC technology with IoT technology to more effectively secure the transmitted data after researching and analyzing the best ways to do so. As we already discussed, a simulation of the smart network of the firefighting station in the power-producing firms was created for this study since it contains temperature sensors placed in key locations.

According to the suggested project depicted in Figure 5. Wi-Fi is used for communication between the TX transmitter and the RX receiver, and the TX attached to the temperature sensors chooses the data at random. The data is subsequently sent to the server, which retains the information obtained from the TX before sending it to the RX. Processing carried out in the receiver RX to ascertain the values received from TX, such as information received: Value 20 such as the temperature. The parties that receive the information from the transmitter and pass it on to the receiver

also decide the server address. The data is kept in random memory throughout program execution. After that, it uploads the information it has just received to the BC network, which verifies it and adds it to the IoT network. By contrasting the current and prior temperatures, the verification process is carried out. If the discrepancy is large, the proper action will be performed. The functioning of the phases of proposed approach, linking temperature sensors, using ESP32 device, PoA algorithm and the secure hash algorithm (SHA384) function are demonstrated in the following subsections.

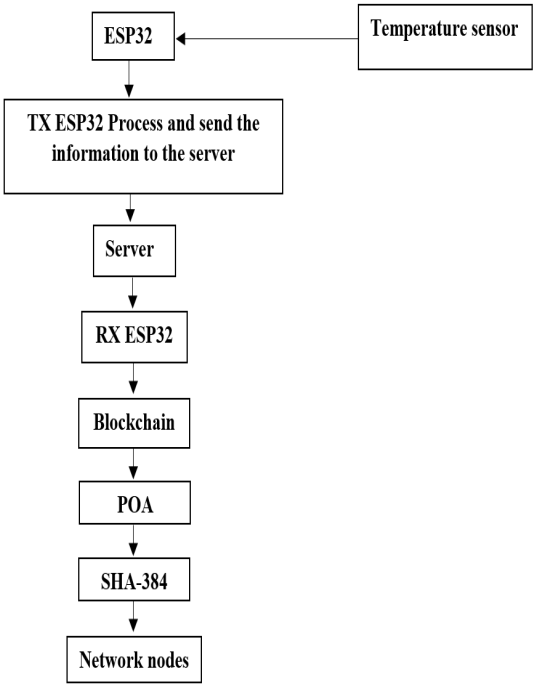


Figure 5: Methodology structure of proposed work

## 5.2 Phases of proposed approach

The phases of our work will be as follows:

1. Temperature data is collected by temperature sensors to measure temperatures at Firefighting stations. This data accuracy is an essential element in avoiding fire problems in production companies.

2. The use of EPS32 devices is characterized by benefits as mentioned in Section 5.1. These devices are characterized by high performance which will be useful in dealing with temperature sensor data collected.

3. Building IoT applications that transmit sensor data via EPS32 to servers. These applications include TX and RX processes to perform sending and receiving operations.

4. Server receives temperature sensors data based on IoT applications.

5. Collected information is directed to one of the BC algorithms (PoA) for review and validity testing after being transferred through the Internet to the receiving device (ESP32), depending on the method, before being shared with the network nodes.

6. Network nodes are the network end-edge devices that receive reports from firefighting station servers.

## 5.3 Linking temperature sensors

These sensors are located in the firefighting stations and the main control units of the electricity production company, where the two units are linked together. These sensors are with variable resistors or glass filled with a substance, so this glass breaks and this substance is released when the temperature rises above the normal rate, and thus an alarm is sent to the main control units, which send a signal to the firefighting stations to take the necessary action. Figure 6 shows the types of temperature sensors used. To link a temperature sensor with an ESP32, we will typically need a temperature sensor module that communicates with the ESP32. Listed below are basic points to link the temperature sensor with the ESP32 device:

- Select a temperature sensor: Choose a temperature sensor module that works with the ESP32 device. The DS18B20-digital, DHT11/DHT22-digital, and LM35-analog sensors are common choices. Make that the operating voltage and connection of the sensor are compatible with the ESP32 device.

- Connect the temperature sensor to the ESP32: Make the appropriate connections between the sensor module and the ESP32 depending on the sensor and communication. For I2C, connect the sensor's data and clock pins to the corresponding pins on the ESP32 device.

- Install the required libraries: Install the required libraries for the selected connection and the temperature sensor.

- Write the code: Open the development environment (e.g., Arduino IDE) and start a new project. Write the code to read data from the temperature sensor after importing the required libraries.

## 5.4 Using ESP32 device

The ESP32 is a microcontroller and Wi-Fi module combo that has many features and functionalities to offer. Due to its adaptability and low power consumption, it may be used in IoT applications. The following are some important points to keep in mind when researchers begin using our ESP32 device:

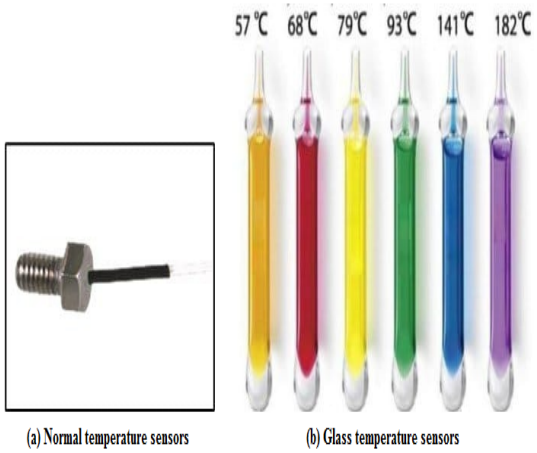


Figure 6: Temperature sensors of proposed methodology

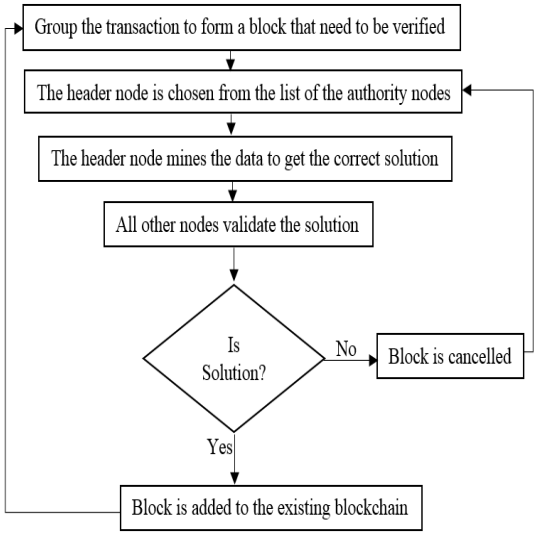


Figure 7: The PoA's work

– Set up the development environment: Install the necessary software tools, such as the Arduino IDE or PlatformIO, which provide an easy-to-use interface for programming the ESP32 device.

– Connect ESP32 to network device: Use a USB cable to communicate the ESP32 device to the network device such as a computer. Ensure that the device is properly recognized by the operating system.

– Select the appropriate board and port: In the development environment, select the ESP32 board we are utilizing from the list of available options. Also, select the correct serial port to establish a connection with the device.

– Write and upload code: Start by writing code utilizing the programming language supported by the researcher's chosen development environment. Researchers could find many example codes and libraries online to help them get started. Once the code is ready, upload it to the ESP32 using the upload button in the development environment.

– Observe the output: Depending on the code, the researcher can monitor the output of the ESP32 through the serial monitor in the development environment. This allows us to debug and verify that the code is running as expected.

– Test device: Connect ESP32 to the required temperature sensors, actuators, or other peripherals. Verify that the device is interacting correctly with these components.

## 5.5 Proof of authority algorithm

This subsection explains how the PoA algorithm works, as seen in Figure 7. According to the PoA approach, reliability or the number of previously contributed blocks is taken into consideration when selecting the header node that uploads the block. The network of choice has a list of nodes ranked by authority and dependability. When the other nodes have confirmed the data, this trustworthy node will seek for the correct hash, add the block, and then share the block with them. A different node is chosen for each epoch until every node on the list has finished adding blocks to the BC. The technique is then carried out once more. Upon confirmation by the other nodes, this trustworthy node will seek for the correct hash, add the block, and share it. Until each node on the list has finished adding blocks to the BC, a different node is selected for each epoch. At that point, the process is repeated. The block will be added after the node that acquired the hash, and data will be shared by each node in turn after that until all nodes have finished adding blocks. For example, when the program is first executed, node number (1) is chosen in order to obtain the correct hash prior to adding the block. This process will only be repeated once all nodes have finished adding blocks, so after the node obtained the hash, each node in the listing will append the block and engage the information in turn. For instance, when the program is run for the first time, node number (1) is selected to obtain the proper hash before adding the block. The selected node is known as the miner in this process, which is called mining. The block will be canceled if it is discovered that the data contributed to the block by the chosen node is inaccurate, and if these mistakes continue, the node will be removed from the list of nodes. Afterward, node number (2) will obtain the hash and include the block, and node number (3) will mine information to obtain the proper hash and include the fresh block to the BC. This method greatly accelerates program execution, which cuts down on the amount of time needed to share data among network nodes and conserves resources.

### 5.6 Secure hash algorithm

It is a one-way hash function, used with many technologies such as BC technology, where this function performs transaction hashing with a 384-bit digest. Thus, the length of the abstract is 96 after converting to the hexadecimal system. Although the process of hashing and obtaining the required digest takes more time and space than other functions such as SHA-384, it is more secure than SHA-224/256, so it is preferred in many applications. SHA-384 and SHA-256 are both cryptographic hash functions that belong to the SHA-2 family. While they share similarities, there are important differences between the two:

- Output size: SHA-384 produces a hash value with a size of 384 bits (48 bytes), while SHA-256 produces a hash value with a size of 256 bits (32 bytes). The larger output size of SHA-384 presents a higher level of security against collision attacks compared to SHA-256.
- Security strength: Due to its longer output size, SHA-384 offers a higher security strength than SHA-256. Security strength refers to the level of resistance against brute-force attacks. SHA-384 provides a higher resistance, making it more suitable for applications that require stronger security.
- Computational efficiency: SHA-256 is generally faster to compute compared to SHA-384. SHA-384's greater output size necessitates more processing power and may cause slower hashing performance.
- Application use cases: SHA-384 is typically used in applications that demand a higher level of security, such as production enterprises such as electricity in particular firefighting issues. SHA-256 is widely used in various applications and communication protocols.
- Compatibility: Both SHA-384 and SHA-256 are widely supported and implemented in modern cryptographic libraries and frameworks.

When choosing between SHA-384 and SHA-256, it is crucial to take into account the application's particular performance and security restrictions. If the application needs a higher level of security with an emphasis on resistance against collision attacks, SHA-384 is a suitable choice. Therefore, we choose to use an SHA-384 algorithm.

## 6 Our proposed results

In this section, we will explain our results in terms of performance and security.

### 6.1 Results of our proposed performance

In this part, the performance of our approach will be explained. The algorithms get more efficient as the hardware utilized at work becomes more efficient. A Fujitsu PC with a Core TM i5 M520 CPU running at 2.4 GHz and 6 GB of random memory was utilized to run the simulation. In addition to that, a microcontroller (ESP32) was used for its advantages, as it has Wi-Fi and is characterized by fast data transfer. As for the software components, the proposed system was programmed using the MATLAB 2021a language, due to its ease of programming and containing many libraries necessary for this work.

The results of PoA algorithms with IoT technology will be presented as the next step in order to enhance its efficiency and security. The number of blocks used for simulation in the proposed approach is 18 blocks. Figures 8, 9 and 10 show that the results were satisfactory in terms of execution time and memory use. Using this method in the network of firefighting stations included in the power plants project has increased security and efficiency. BC algorithms enhance IoT technology's security and performance while also boosting its capacity to share accurate and unmistakable information. Misinformation given by sensors may cause various issues when dealing with IoT itself. In this work, we simulated the smart network of the firefighting station in the power production company, as mentioned previously, and the following results were obtained in terms of PoA's nonce attempts, time of adding the block and PoA's used memory for both SHA-256 and SHA-384 as well as performance comparison.

#### 6.1.1 Nonce attempts

In this work, the nonce represents a number of iterations and attempts until the required solution is obtained by the network participants according to the difficulty conditions imposed in this work, as shown in Figure 8. As can be seen from the figure, our approach with SHA-384 can be better than using SHA-256 in terms of nonce iterations.

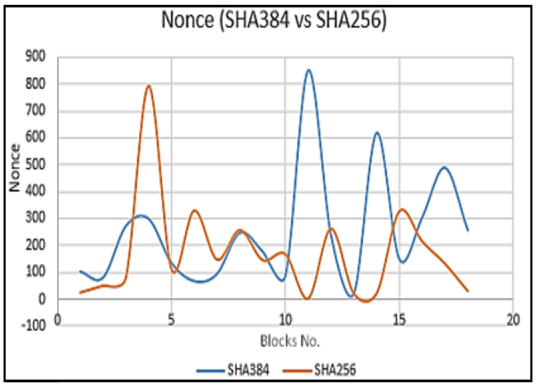


Figure 8: PoA's nonce iterations in both SHA256 and SHA384

#### 6.1.2 Times to add blocks

This subsection describes the creation time of each block after the data is transferred to the network nodes, and the

SHA256/SHA384 algorithm is applied to the block data and the required digest is obtained in the hexadecimal system, as shown in Figure 9 that shows times to add the blocks. Although sometimes our proposed approach with SHA256 provides an advantage over SHA384, our approach with SHA384 still provides an advantage over SHA256 in some block numbers (see Figure 9). This means that the performance of our approach with SHA384 can be suitable for firefighting station applications.

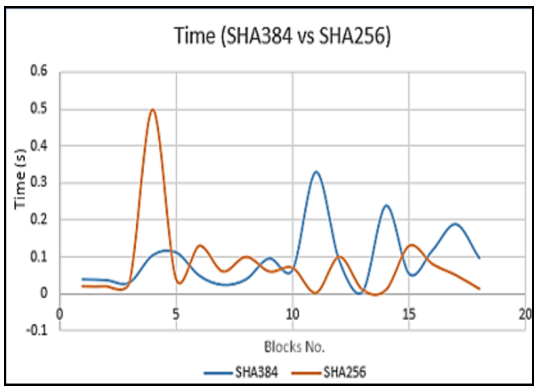


Figure 9: Times to add the blocks

### 6.1.3 Required memory size

This part of our research characterizes the size of the used memory in this work, although our proposed approach with SHA384 takes up more space than similar functions, however, it is more secure. The memory size with both SHA256 and SHA384 can be seen in Figure 10. We can sacrifice a little bit of memory, but we can not lose important information through hacks that can destroy the entire system or application.

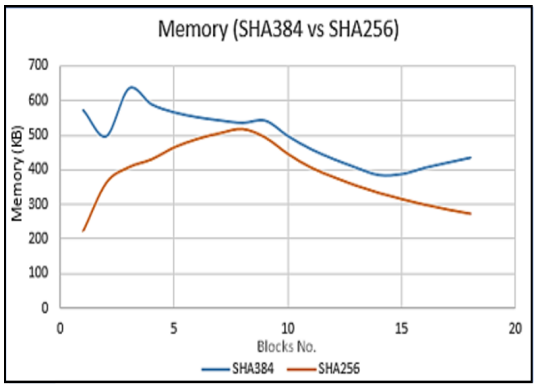


Figure 10: PoA's memory used

### 6.1.4 Performance comparison

Our approach theoretically provides better performance compared to [24], [25], [26], [27], [28] and [29] because our proposed approach uses EPS32 devices to support network performance of temperature sensors (as presented in Section 5.1) and thus support the performance of the network as a whole. Furthermore, [24] needs additional performance overhead to accomplish the licensing operations in their IoT-BC approach. Also, both [28, 29] do not rely on BC to secure IoT applications. Compared with our approach, it uses BC because it performs processing of firefighting station requests in fast processing time, thus its use in modern applications such as firefighting applications becomes inevitable and desirable.

## 6.2 Security analysis

There are types of attacks that many electronic systems and smart networks may be exposed to, and one of these attacks is a DDoS threat is a malicious trial to disrupt the normal flow to a target server, service, or network by flooding the target or its embracing infrastructure with an excessive amount of Internet requests. A DDoS will spread to other computers in the same network once it begins on one, leading to a catastrophic collapse. All network resources, including the technology that underpins a firm website, are subject to certain capacity limits that are used in this type of assault. The ultimate objective of an attacker is typically to entirely obstruct an online resource's normal operation. Users will not be able to access a website or application, if one exists. Additionally, the assailant might demand payment to halt the assault. A DDoS assault could occasionally be an effort to harm or harm the reputation of a rival business. Due to this, safety measures must be performed. Every day, more than 2000 DDoS attacks are recorded worldwide. DDoS attacks are to blame for a third of all outages. It can take a variety of shapes, including Smurfs, teardrops, and Pings of Death. DDoS assaults are seen as "weapons of mass destruction" online.

DDoS attacks are more challenging to protect against since no business can take enough security measures to be completely secure. But BC technology can face these attacks by making sure that all nodes have enough processing power, storage, and network bandwidth is the main defense against BC DDoS. According to the general rule, a BC network will be more resistant to a DDOS attack the more decentralized it is. Because it is decentralized, the BC network is protected so that transactions can go on even if certain nodes are offline for a period. Any node can fall offline due to a DDoS assault or another occurrence without taking over the entire network. There is also another type of attack such as brute force and collision that can target hash functions to expose or destroy information in firefighting stations. These attacks are not possible on our approach because it provides a long and unhackable message digest as we explained in Section 5.6.

Additionally, our approach provides better security when using SHA384 as explained in Section 5.6. When compared with all included searches in Section 2, our

approach is superior to all included searches in terms of security because it uses SHA384 which is capable of blocking DDoS, brute force, and collision attacks. For example, Krishna et al. [26] are based on BC-SHA256, Kumar et al. [27] are based on BC-Ethash with 256 bits. Tukur et al. [25], Ali et al. [24], Khan et al. [28], Khan [29] are mentioned because they used a hash function but did not specify the message digest length. This illustrates that our approach provides better security than existing research.

# 7 Conclusion

The use of an approach to reduce fire problems in electric power production companies is a priority for this sector. Also, any breakthroughs can greatly increase these problems. Our suggested design makes use of exclusive BC technology since it offers anonymity and security, works well with the IoT to boost efficiency, and is thus appropriate for electric power production businesses and organizations. This technology is different from the other encryption methods in that it employs a one-way encryption mechanism, we adopted SHA384, making it more secure and resistant to attacks than the others. It has been used at the firefighting station to make the procedure of sending data from sensors dispersed across the power plant's various locations to the control unit safer. Its implementation employs the PoA method, one of the BC's consensus algorithms, to test how quickly and how much memory it needs in a firefighting station. Because of its benefits in terms of performance, the ESP32 device was employed in this work. Also, a local server network was incorporated into this design for increased secrecy, and this tactic worked well for this work. Due to the requirement to work for various libraries that are useful in this task, picking the programming language was one of the most significant problems we encountered. Matlab 2021a was used to program this project since it is appropriate for our needs and provides the resources we need to create a network simulation. Based on the results of the performance analysis (use of ESP32 hardware) and security (blocking of DDoS, brute force and collision), our approach is superior to the research approaches included in Section 2 and thus our approach can be very suitable for firefighting station applications.

# 8 Future direction

Our proposal is directed to firefighting applications, as the user devices are limited, and therefore our proposal may not be suitable for other applications, such as e-education and e-health applications, which depend on a large number of user devices and sensors. In the future, we should examine the compatibility of our approach with different electronic applications. To develop our proposed approach, we will experiment with combining our suggested network with a different kind of BC, the consortium BC, to increase the security of the IoT. Since it is administered by a number of institutions rather than just one, this kind of BC may be suitable for many electric power companies or government organizations. To exchange data or conduct mining operations, each institution chooses a group of reliable nodes that are joined into a single network. Then, we intend to expand our security analysis on detailed types of DDoS attacks such as Slowloris, Zero-day, Volumetric, etc. Finally, we plan to support our approach by using GraphChain with BC to improve performance by supporting multi-nodes and multi-servers in parallel processing, this will improve network performance, especially servers that experiencing huge momentum from IoT-BC network requests.

## Conflict of interest

The authors declare that they have no conflict of interest.

## Data availability

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

# References

[1] M. Shokouhi, K. Nasiriani, Z. Cheraghi, A. Ardalan, H. Khankeh, H. Fallahzadeh, and D. Khorasani-Zavareh, "Preventive measures for fire-related injuries and their risk factors in residential buildings: A systematic review," *Journal of injury and violence research*, vol. 11, no. 1, p. 1, 2019. https://doi.org/10.5249\%2Fjivr.v11i1.1057

[2] B. o. L. Statistics, "Census of fatal occupational injuries (CFOI)-current and revised data," 2019.

[3] R. B. Campbell, *Fires in structures under construction, undergoing major renovation, or being demolished*. National Fire Protection Association Quincy, MA, 2017.

[4] J. Gehandler, "The theoretical framework of fire safety design: Reflections and alternatives," *Fire safety journal*, vol. 91, pp. 973–981, 2017. https://doi.org/10.1016/j.firesaf.2017.03.034

[5] D. Cram, C. E. Hatch, S. Tyler, and C. Ochoa, "Use of distributed temperature sensing technology to characterize fire behavior," *Sensors*, vol. 16, no. 10, p. 1712, 2016. https://doi.org/10.3390/s16101712

[6] P. Johnson, C. Beyler, P. Croce, C. Dubay, and M. McNamee, "Very early smoke detection apparatus (VESDA), david packham, john petersen, martin cole: 2017 dinenno prize," *Fire Science Reviews*, vol. 6, no. 1, pp. 1–12, 2017. https://doi.org/10.1186/s40038-017-0019-4

[7] M.-Y. Cheng, K.-C. Chiu, Y.-M. Hsieh, I.-T. Yang, and J.-S. Chou, "Development of bim-based real-time evacuation and rescue system for complex buildings,"

in *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, vol. 33. IAARC Publications, 2016, p. 1.

[8] N. Khana, D. Leea, A. K. Alia, and C. Parka, "Artificial intelligence and blockchain-based inspection data recording system for portable firefighting equipment," in *Proceedings of the International Symposium on Automation and Robotics in Construction, Kitakyushu, Japan*, 2020, pp. 27–28.

[9] S.-H. Wang, W.-C. Wang, K.-C. Wang, and S.-Y. Shih, "Applying building information modeling to support fire safety management," *Automation in construction*, vol. 59, pp. 158–167, 2015. https://doi.org/10.1016/j.autcon.2015.02.001

[10] N. Khan, A. K. Ali, S. Van-Tien Tran, D. Lee, and C. Park, "Visual language-aided construction fire safety planning approach in building information modeling," *Applied Sciences*, vol. 10, no. 5, p. 1704, 2020. https://doi.org/10.3390/app10051704

[11] V. Kodur and M. Naser, "Fire hazard in transportation infrastructure: Review, assessment, and mitigation strategies," *Frontiers of Structural and Civil Engineering*, vol. 15, pp. 46–60, 2021. https://doi.org/10.1007/s11709-020-0676-6

[12] X. Bao, "Fire equipment information traceability system based on blockchain," in *E3S Web of Conferences*, vol. 251. EDP Sciences, 2021, p. 03099. https://doi.org/10.1051/e3sconf/202125103099

[13] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, vol. 15, no. 1, p. 152, 2023. https://doi.org/10.3390/sym15010152

[14] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–7. https://doi.org/10.1109/GLOBECOM38437.2019.9013413

[15] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs," *Applied Sciences*, vol. 10, no. 6, p. 2007, 2020. https://doi.org/10.3390/app10062007

[16] D. Mahmudnia, M. Arashpour, Y. Bai, and H. Feng, "Drones and blockchain integration to manage forest fires in remote regions," *Drones*, vol. 6, no. 11, p. 331, 2022. https://doi.org/10.3390/drones6110331

[17] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications," *Security and Communication Networks*, vol. 2019, 2019. https://doi.org/10.1155/2019/3263902

[18] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "UTM-chain: Blockchain-based secure unmanned traffic management for Internet of drones," *Sensors*, vol. 21, no. 9, p. 3049, 2021. https://doi.org/10.3390/s21093049

[19] E. A. Soto, L. B. Bosman, E. Wollega, and W. D. Leon-Salas, "Peer-to-peer energy trading: A review of the literature," *Applied Energy*, vol. 283, p. 116268, 2021. https://doi.org/10.1016/j.apenergy.2020.116268

[20] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54 478–54 497, 2021. https://doi.org/10.1109/ACCESS.2021.3070555

[21] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics*, vol. 12, no. 4, p. 1011, 2023. https://doi.org/10.3390/electronics12041011

[22] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," *Future Internet*, vol. 15, no. 8, p. 262, 2023. https://doi.org/10.3390/fi15080262

[23] A. Pieroni, N. Scarpato, and L. Felli, "Blockchain and IoT convergence–A systematic survey on technologies, protocols and security," *Applied Sciences*, vol. 10, no. 19, p. 6749, 2020. https://doi.org/10.3390/app10196749

[24] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in Internet of things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, 2019. https://doi.org/10.1016/j.cose.2019.06.010

[25] Y. M. Tukur, D. Thakker, and I.-U. Awan, "Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, p. e4158, 2021. https://doi.org/10.1002/ett.4158

[26] 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

[27] S. Kumar, U. Dohare, O. Kaiwartya *et al.*, "FLAME: Trusted fire brigade service and insurance claim system using blockchain for enterprises," *IEEE Transactions on Industrial Informatics*, pp. 1–8, 2022. https://doi.org/10.1109/TII.2022.3212172

[28] S. Khan, A. P. Shah, S. S. Chouhan, S. Rani, N. Gupta, J. G. Pandey, and S. K. Vishvakarma, "Utilizing manufacturing variations to design a tri-state flip-flop PUF for IoT security applications," *Analog Integrated Circuits and Signal Processing*, vol. 103, no. 3, pp. 477–492, 2020. https://doi.org/10.1007/s10470-020-01642-9

[29] T. Khan, "Ultra-low-power architecture for the detection and notification of wildfires using the Internet of things," *IoT*, vol. 4, no. 1, pp. 1–26, 2023. https://doi.org/10.3390/iot4010001

[30] K. M. Harahsheh and C.-H. Chen, "A survey of using machine learning in IoT security and the challenges faced by researchers," *Informatica*, vol. 47, no. 6, 2023. https://doi.org/10.31449/inf.v47i6.4635

[31] TeachVidvan, "Architecture of IoT," 2022, https://techvidvan.com/tutorials/architecture-of-iot/.

[32] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "IoT-BSFCAN: A smart context-aware system in IoT-cloud using mobile-fogging," *Future Generation Computer Systems*, vol. 109, pp. 368–381, 2020. https://doi.org/10.1016/j.future.2020.03.050

[33] I. F. Akyildiz and A. Kak, "The Internet of space things/cubesats: A ubiquitous cyber-physical system for the connected world," *Computer Networks*, vol. 150, pp. 134–149, 2019. https://doi.org/10.1016/j.comnet.2018.12.017

[34] I. Al_Barazanchi, A. Murthy, A. A. Al Rababah, G. Khader, H. R. Abdulshaheed, H. T. Rauf, E. Daghighi, and Y. Niu, "Blockchain technology-based solutions for IoT security," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 53–63, 2022. https://doi.org/10.52866/ijcsm.2022.01.01.006

[35] B. Shang, S. Liu, S. Lu, Y. Yi, W. Shi, and L. Liu, "A cross-layer optimization framework for distributed computing in IoT networks," in *2020 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 2020, pp. 440–444. https://doi.org/10.1109/SEC50012.2020.00067

[36] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in Internet of things (IoT)-enabled smart-cities: An overview," *Computers & Electrical Engineering*, vol. 87, p. 106776, 2020. https://doi.org/10.1016/j.compeleceng.2020.106776

[37] M. J. Baucas, S. A. Gadsden, and P. Spachos, "IoT-based smart home device monitor using private blockchain technology and localization," *IEEE Networking Letters*, vol. 3, no. 2, pp. 52–55, 2021. https://doi.org/10.1109/LNET.2021.3070270

[38] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of things (IoT): A survey," *Sensors*, vol. 22, no. 3, p. 1094, 2022. https://doi.org/10.3390/s22031094

[39] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, pp. 58 822–58 835, 2019. https://doi.org/10.1109/ACCESS.2019.2914675

[40] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018. https://doi.org/10.1109/ACCESS.2018.2842685

[41] H. Zhang, W. Lang, C. Liu, and B. Zhang, "A blockchain-based security approach architecture for the Internet of things," in *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, vol. 1. IEEE, 2020, pp. 310–313. https://doi.org/10.1109/ITNEC48623.2020.9084997

[42] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system," *International Journal of Environmental Research and Public Health*, vol. 16, no. 9, p. 1490, 2019. https://doi.org/10.3390/ijerph16091490

[43] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and secure ECDSA algorithm and its applications: A survey," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 11, pp. 7–35, 2019. https://doi.org/10.17762/ijcnis.v11i1.3827

[44] A. A. Brincat, A. Lombardo, G. Morabito, and S. Quattropani, "On the use of blockchain technologies in wifi networks," *Computer Networks*, vol. 162, p. 106855, 2019. https://doi.org/10.1016/j.comnet.2019.07.011

[45] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*. IEEE, 2020, pp. 35–40. https://doi.org/10.1109/ICAICT51780.2020.9333488

[46] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?" *International Journal of Production Economics*, vol. 211, pp. 221–236, 2019. https://doi.org/10.1016/j.ijpe.2019.02.002

[47] W. Mougayar, *The business blockchain: Promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.

[48] Komodo, "4 types of blockchain technology explained," 2021, https://komodoplatform.com/en/academy/blockchain-technology-types/.

[49] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and informatics*, vol. 36, pp. 55–81, 2019. https://doi.org/10.1016/j.tele.2018.11.006

[50] M. Wazid, A. K. Das, S. Shetty, and M. Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things," *IEEE Access*, vol. 8, pp. 88 700–88 716, 2020. https://doi.org/10.1109/ACCESS.2020.2992467

[51] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251–279, 2019. https://doi.org/10.1016/j.jnca.2018.10.019

[52] A. S. Musleh, G. Yao, and S. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86 746–86 757, 2019. https://doi.org/10.1109/ACCESS.2019.2920682

[53] G. S. Shyaa and M. Al-Zubaidie, "Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography," *Applied Sciences*, vol. 13, no. 12, p. 7085, 2023. https://doi.org/10.3390/app13127085

[54] V. Kodur, P. Kumar, and M. M. Rafi, "Fire hazard in buildings: review, assessment and strategies for improving fire safety," *PSU research review*, vol. 4, no. 1, pp. 1–23, 2020. http://dx.doi.org/10.1108/PRR-12-2018-0033

[55] H. Zhang, D. Yang, V. W. Tam, Y. Tao, G. Zhang, S. Setunge, and L. Shi, "A critical review of combined natural ventilation techniques in sustainable buildings," *Renewable and Sustainable Energy Reviews*, vol. 141, p. 110795, 2021. https://doi.org/10.1016/j.rser.2021.110795

[56] N. Khan, D. Lee, C. Baek, and C.-S. Park, "Converging technologies for safety planning and inspection information system of portable fire-fighting equipment," *IEEE Access*, vol. 8, pp. 211 173–211 188, 2020. http://dx.doi.org/10.1109/ACCESS.2020.3039512

[57] C. Nartey, E. T. Tchao, J. D. Gadze, E. Keelson, G. S. Klogo, B. Kommey, and K. Diawuo, "On blockchain and IoT integration platforms: Current implementation challenges and future perspectives," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–25, 2021. https://doi.org/10.1155/2021/6672482

[58] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE access*, vol. 8, pp. 21 091–21 116, 2020. https://doi.org/10.1109/ACCESS.2020.2968985

[59] K. Tsoulias, G. Palaiokrassas, G. Fragkos, A. Litke, and T. A. Varvarigou, "A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems," *IEEE Access*, vol. 8, pp. 130 952–130 965, 2020. http://dx.doi.org/10.1109/ACCESS.2020.3006383

[60] Z. Turk and R. Klinc, "Potentials of blockchain technology for construction management," *Procedia engineering*, vol. 196, pp. 638–645, 2017. https://doi.org/10.1016/j.proeng.2017.08.052

[61] Q. Lu, L. Chen, S. Li, and M. Pitt, "Semi-automatic geometric digital twinning for existing buildings based on images and CAD drawings," *Automation in Construction*, vol. 115, p. 103183, 2020. https://doi.org/10.1016/j.autcon.2020.103183

[62] K. Rofaida, M. Derdour, M. A. Ferrag, and M. M. Bouhamed, "Prschain: A blockchain based privacy preserving approach for data service composition," *Informatica*, vol. 47, no. 9, 2023. https://doi.org/10.31449/inf.v47i9.5081

[63] N. S. Rani, T. Vasudev, M. Chandrajith, and N. Manohar, "2d morphable feature space for handwritten character recognition," *Procedia Computer Science*, vol. 167, pp. 2276–2285, 2020. https://doi.org/10.1016/j.procs.2020.03.280