Journal Pre-proof

A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things

Shahid Latif, Zeba Idrees, Jawad Ahmad, Lirong Zheng, Zhuo Zou

PII: S2452-414X(20)30065-0
DOI: https://doi.org/10.1016/j.jii.2020.100190
Reference: JII 100190

To appear in: *Journal of Industrial Information Integration*

Received date : 7 September 2020
Revised date : 24 November 2020
Accepted date : 29 November 2020

Please cite this article as: S. Latif, Z. Idrees, J. Ahmad et al., A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, *Journal of Industrial Information Integration* (2020), doi: https://doi.org/10.1016/j.jii.2020.100190.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2020 Elsevier Inc. All rights reserved.

Journal Pre-proof

Highlights

A Blockchain-based Architecture for Secure and Trustworthy Operations in the Industrial Internet of Things

Shahid Latif,Zeba Idrees,Jawad Ahmad,Lirong Zheng,Zhuo Zou

- This study realizes the great potential of integrating blockchains with the IoT in a manner suitable for smart industrial environments.
- This study proposes a lightweight, easily expandable, and decentralized private blockchain-based IIoT network.
- A secure blockchain-based architecture is presented for industrial operations that include user and device registration, storage of sensor and actuator data, and client services.
- To ensure high performance and reduce the computational complexity of the blockchain, we introduce a blockchain service layer that contains two modules. First, lightweight nodes that perform asymmetric cryptography in real time with ARM Cortex-M processors are applied. Second, a highly scalable and IoT friendly consensus mechanism proof of authentication (PoAh) is deployed in the main blockchain network.
- The performance of the proposed framework is evaluated by using several metrics such as used consensus algorithms, resource utilization, energy efficiency, and service execution time.
- Finally, the implementation of the proposed technique in a fruit processing plant is presented as an industrial experiment.

Journal Pre-proof

Journal Pre-proof

A Blockchain-based Architecture for Secure and Trustworthy Operations in the Industrial Internet of Things

Shahid Latif[a], Zeba Idrees[a], Jawad Ahmad[b], Lirong Zheng[a,*] and Zhuo Zou[a,*]

[a]State Key Laboratory of ASIC and System, School of Information Science and Engineering, Fudan University, Shanghai, China
[b]School of Computing, Edinburgh Napier University, Edinburgh EH11 4DY, U.K.

ARTICLE INFO

Keywords:
Blockchain
Cybersecurity
Distributed Ledger
Industrial Internet of Things
Smart Industry

ABSTRACT

The industrial Internet of Things (IIoT) plays an important role in the industrial sector, where secure, scalable, and easily adopted technologies are being implemented for the smart industry. The traditional IIoT architectures are generally based on centralized architectures that are vulnerable to a single point of failure and to several cyber-attacks. Blockchain technology is frequently adopted in the modern industry because of its security and decentralization. This paper proposes a blockchain-based architecture that ensures secure and trustworthy industrial operations. A private and lightweight blockchain architecture is proposed to regulate access to valuable sensor and actuator data. To enhance the computational performance of the proposed architecture, real-time cryptographic algorithms are processed using a low-power ARM Cortex-M4 processor, and a highly scalable, fast, and energy-efficient consensus mechanism proof of authentication (PoAh) is deployed in the blockchain network. Extensive experiments and analysis proved the effectiveness of the proposed framework for smart industrial environments. Finally, we transform a conventional fruit processing plant into a secure and smart industrial platform by implementing the proposed architecture.

1. Introduction

Modern technologies and innovative concepts such as big data, artificial intelligence (AI), cloud computing, and cyber-physical systems have sparked a revolution in the industrial sector [1]. The integration of the Industrial Internet of Things (IIoT) with smart industry has shifted industrial operations to a new level [2]. The IIoT dramatically changes several industrial processes by providing facilities and introducing new systems and business models [3], [4]. IIoT platforms offer several services to modern industries, including high-speed connectivity, edge and cloud computing, big data analysis and application development[5]. These services enhance existing industrial processes by optimizing production processes, improving customer services, and reducing manufacturing costs using emerging and cutting-edge techniques [6], [7]. The current industry trends and initiatives are targeted at realizing the fourth industrial revolution by connecting the existing industrial environments to Internet services [8], [9].

The existing IoT systems are generally built on centralized architectures in which cloud-based servers provide data analysis and information processing facilities. Despite good management and strong computational capabilities, the security and privacy challenges of such architectures are increasing as the number of IIoT networks expands. One of the main disadvantages of a centralized solution is that in the case of a single point of failure, the complete network may be exposed to an attacker [10]. Therefore, these solutions are not recommended for high-performance applications [11]. As IIoT networks have expanded, a significant increase in sensing data has also occurred, which increases the burden on centralized verification systems and can lead to the instability of complete systems [12].

The security and privacy challenges in the IIoT can be overcome by using blockchain technology. Emerging blockchain technologies have gained great attention from academia and industry. A blockchain is a decentralized ledger technology (DLT) that secures data through cryptographic techniques. Blockchain technologies can also store and process information in a distributed manner. Thus, blockchains have great potential to significantly improve the performance of existing IIoT platforms [13]. Together with blockchains, big data, IoT, AI, and smart robotic technologies are shifting industrial operations to a new level. In the future, the blockchain-enabled IIoT will play very important roles in multiple areas, including smart manufacturing, transportation, logistics, healthcare, the energy sector, and many others [13].

1.1. Motivation and contributions

IIoT systems have different requirements than cryptocurrencies. Therefore, the integration of blockchain with the IIoT is still a challenging task. First, IoT devices have a resource-constrained nature. Second, large IIoT networks contain hundreds of devices that demand a sufficient scalable security solution. To address these challenges, this paper proposes a lightweight, highly scalable, and private blockchain-based architecture for the IIoT network. The major contributions of the proposed architecture are as follows.

- This study realizes the great potential of integrating blockchains with the IoT in a manner suitable for smart industrial environments.

*Corresponding authors: Zhuo Zou (zhuo@fudan.edu.cn) ,Lirong Zheng (lrzheng@fudan.edu.cn)
ORCID(s): 0000-0002-6368-2729 (Shahid Latif); 0000-0002-7918-0440 (Zeba Idrees); 0000-0001-6289-8248 (Jawad Ahmad); 0000-0001-9588-0239 (Lirong Zheng); 0000-0002-8546-1329 (Zhuo Zou)

Journal Pre-proof

- This paper proposes a lightweight, easily expandable, and decentralized private blockchain-based IIoT network.
- To ensure high performance and reduce the computational complexity of the blockchain, we introduce a blockchain service layer that contains two modules. First, lightweight nodes that perform asymmetric cryptography in real time with ARM Cortex-M processors are applied. Second, a highly scalable and IoT friendly consensus mechanism proof of authentication (PoAh) is deployed in the main blockchain network.
- The proposed architecture is used to perform several industrial operations, including user and device registration, sensor and actuator data storage, and client service tasks, in a trustworthy manner.
- The performance of the proposed framework is evaluated by using several metrics such as used consensus algorithms, resource utilization, energy efficiency, and service execution time.
- Finally, the proposed framework is implemented in a fruit processing plant as an industrial experiment.

The remainder of this article is organized as follows. Section II discusses the existing blockchain technologies for IIoT systems. Section III presents the details of the proposed architecture. Section IV describes the working mechanism of proposed platform. Section V presents a detailed discussion on system performance. Section VI discusses the implementation of the proposed technique for fruit processing plants. Finally, Section VII provides a brief conclusion.

2. Related works

Over the last decade, the IIoT has developed into a key technology that has gained substantial attention from researchers seeking to enhance industrial processes [14]. The IIoT has proved its effectiveness in several sectors in terms of accurate real-time information processing, sustainable practices, predictive maintenance, etc. Blockchain technologies can provide transparency, traceability, and respect for human rights in industrial environments [15]. In this section, we present an overview of some recent studies related to blockchain applications for IIoT.

In 2008, Nakamoto introduced a blockchain-based digital currency system named Bitcoin [16]. IIoT and Bitcoin systems have many similarities, including massive numbers of varied nodes, frequent data exchanges, and strict security and privacy requirements. Therefore, blockchain technology can enhance the performance of the IIoT in secure and efficient ways. Cao et al. [17] introduced a blockchain-based quality traceability system for the steel industry to overcome challenges of information traceability and low transparency in steel products. Using this system, various production companies, logistics firms, and consumers can gain secure access to steel product information. Furthermore, consumers can understand the real production processes and efficiently trace the quality of steel products. Scalability is a critical issue that can become a hurdle to the use of blockchain technology in generic IIoT systems. To meet the high throughput requirements, Liu et al. [18] proposed a novel framework based on deep reinforcement learning for blockchain-enabled IIoT systems. The experimental results showed that the proposed scheme significantly improved the performance of the target blockchain-based IIoT system. However, because of the power-intensive nature of blockchain technologies, they are not suitable for energy-constrained IoT devices. To address this challenge, Huang et al. [19] introduced a credit-based proof-of-work consensus algorithm for a blockchain scheme. An extensive evaluation proved the effectiveness of the proposed scheme for an IIoT system. He et al. [20] proposed a blockchain-based IIoT device software status monitoring system. To ensure the software integrity information, this system used blockchain as a distributed ledger for storing snapshots of the software status. The authors evaluated their proposed scheme in terms of response delay, resistance to intrusions, and scalability. Some previous blockchain schemes for IIoT have had problems such as low security, high management costs, and supervision difficulties in data transmission techniques. To address these problems, Liang et al. [21] introduced a fabric blockchain-based data transmission technique for IIoT networks and a dynamic secret sharing mechanism that improved the security and reliability of data storage and transmission. Khalid et al. [22] proposed a decentralized authentication mechanism for lightweight IoT devices based on fog computing and a public blockchain that is applicable to several scenarios. Their experiments demonstrated the proposed mechanism's superior performance compared to other state-of-the-art schemes. Shen et al. [23] presented a blockchain-assisted secure device authentication scheme for cross-domain IIoT networks. They specifically introduced consortium blockchain to develop trust in different domains. In addition, along with authentication, their identity mechanism preserved the privacy of IoT devices, ensuring that devices remain anonymous.

2.1. Limitations of existing research

In an industrial control system (ICS), security is a major challenge in the IIoT paradigm [24]. Blockchain offers a secure mechanism for ICSs because of its decentralized nature, which can overcome a wide range of cybersecurity problems. However, the existing research has several drawbacks. First, the real-time integration of blockchain technologies into IIoT networks dramatically increases the computational complexity because of the various cryptographic schemes and consensus algorithms used. In recent studies, this factor has not been deeply considered with respect to real-time industrial environments. Second, the scope of recent studies is limited because most researchers have considered blockchain technology only for efficient sensor data recording in the industrial environment and have not ad-

Journal Pre-proof

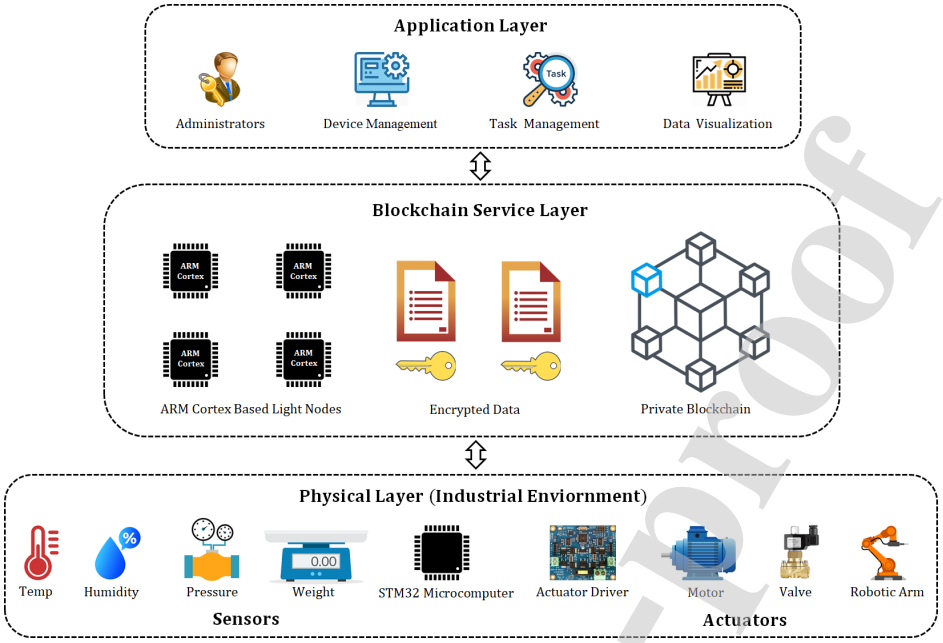

Figure 1: Proposed blockchain architecture for the IIoT.

dressed the applicability of blockchain for other industrial operations. Third, the feasibility of the existing schemes for implementation at the device level has not been discussed. Finally, several studies have used open-source platforms for blockchain services; however, the use of third-party services can sometimes create savior problems. To overcome all these challenges, we propose a secure, lightweight, flexible, and decentralized blockchain-based architecture for smart industry. In addition, we demonstrate the feasibility of the proposed system by implementing it for a fruit processing plant.

3. Blockchain-based architecture for the Industrial Internet of Things

Integrating blockchain with the IIoT system increases the security of the overall system. The blockchain includes all the security and privacy characteristics that are essential for an IoT-enabled smart industry. The proposed architecture for a smart industrial environment is presented in Figure 1. The architecture is flexible and allows developers to modify it according to their industry's requirements. The following subsections briefly describe all the layers in the proposed architecture.

3.1. Physical layer

In a smart industrial environment, the physical layer consists of sensors, actuators, and microcomputers. In the proposed architecture, we consider 4 types of sensors: temperature, humidity, pressure, and weight sensors. All these sensors are interfaced with ultralow-power STM32 development boards that transmit sensed data to the blockchain service layer after performing some required preprocessing. Three actuators— DC gear motors, solenoid valves, and robotic manipulators—are considered in this architecture. To efficiently control and communicate these actuators through the blockchain service layer, intelligent actuator drivers also form a part of the physical layer.

3.2. Blockchain service layer

The blockchain service layer contains all the important modules that organize the common services needed to provide the required blockchain technology features. In the proposed architecture, this layer is further subdivided into two sections: lightweight nodes and private blockchain.

3.2.1. Lightweight nodes

In the proposed mechanism, the lightweight nodes are not used for main data storage; instead, they are specifically designed for the high-speed implementation of asymmetric cryptographic algorithms. This section was developed using STM32F427 development boards, which contain low-power ARM Cortex M4 processors. A complete series of modern processors exists that are suitable for IoT applications, but the ARM Cortex-M series is an excellent choice for implementing cryptographic algorithms [25]. In the proposed scheme, the elliptic curve digital signature algorithm (ECDSA) is used to generate public and private keys and device authentication mechanisms. ECDSA is an ideal choice because of its low complexity and low storage requirements.

The STMicroelectronics X-CUBE-CRYPTOLIB library provides strong support for implementing several standard cryptographic algorithms with the ARM Cortex-M series processors. The NIST Cryptographic Algorithm Validation Program approved and certified ECDSA for industrial applications [26]. Rather than establishing a single node, we

Journal Pre-proof

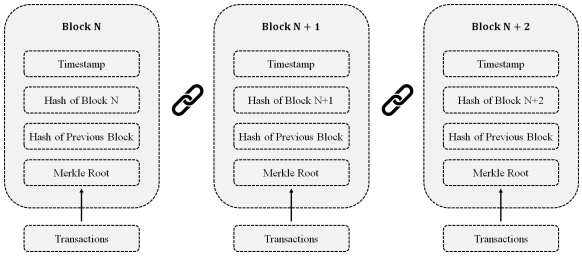

Figure 2: Block structure for the proposed mechanism [2].

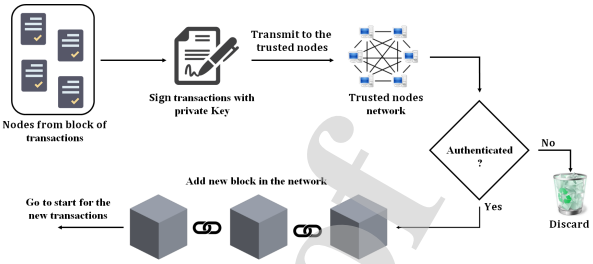

Figure 3: The proof of authentication (PoAh) consensus algorithm.

develop several nodes that provide access to the blockchain network for users and devices. Using multiple distributed nodes reduces the pressure compared to using a single node and prevents system failures from occurring due to a single crashed node. Therefore, this design is a highly suitable solution for integrating blockchain technology with real industrial environments.

3.2.2. Private blockchain

The proposed blockchain mechanism is built on a private network that provides access to authorized users only. The blockchain network is a distributed ledger that maintains the transactions and operation records inside an industrial environment. This ledger contains a chain of cryptographically linked blocks that are an integral part of the blockchain system. Each block consists of a timestamp, hash value, hash value of the previous block, and Merkle root. The block architecture of the proposed scheme is presented in Figure 2. These blocks also enable peer-to-peer networking and data transmission in decentralized networks.

External clients and applications can obtain access to the ledger and modify it according to their requirements by using smart contracts. These contracts contain preset logic and mathematical function-based code. Smart contracts provide client access to the blockchain network without the involvement of a third party by executing autonomously [27]. These contracts are irreversible; therefore, it is very difficult for an unknown person to make changes in the blockchain [28]. Immutability is a property of the blockchain that does not allow transactions in the ledger to be modified by an unauthorized person.

3.2.3. Consensus algorithm

The consensus process allows new transactions to be added to the blockchain. Researchers have used various consensus algorithms, such as algorithms based on proof of work (PoW), proof of stake (PoS), proof of concept (PoC), and proof of activity (PoA). In the proposed architecture, we use 'proof of authentication' (PoAh) to update the blockchain. The block diagram of the PoAh consensus algorithm is presented in Figure 3 [29]. At the beginning of the process, network participants generate transactions with collected data to create a block. In the second step, nodes sign the transaction with a private key and broadcast to the network. When a block is received in the network then trusted nodes find the source public key for signature verification. After successful signature verification, the trusted nodes evaluate the Media Access Control (MAC) address and compares it with the received one for the second round of evaluation. After successful authentication, validated blocks are broadcasted by the trusted nodes with PoAh identification. Subsequently, individual users in the network verify the PoAh information to add blocks into the chain. After acceptance of a valid block, the user computes a hash value to link the next block and retrieves the previous block hash value to save into the current block [29]. The technical steps of the PoAh consensus algorithm are presented in Algorithm 1. The PoAh approach follows a traditional blockchain working model with lightweight block verification [29]. It eliminates the reverse hash function used in the PoW approach to make the transaction process light in weight. As a result, blockchains can be efficiently integrated with resource-constrained devices in the Industrial Internet of Things.

Algorithm 1: Execution process of the PoAh

Inputs: All the nodes in the network follows ECDSA.
Outputs: Validated blocks that are added to the blockchain.

```
begin
    Nodes combine multiple transactions to form the blocks.
    Nodes sign blocks and broadcast to the network.
    The trusted node verifies the signature with the source public key.
        if (Block Authentication = = true)
            A trusted node broadcasts the authenticated block to the network.
            Add this new block in the blockchain.
        else
            Discard the invalid block.
end
```

3.2.4. Application layer

The application layer is the top layer of the architecture. It provides different interfaces to users who can then control devices by visualizing the data using physical devices. This layer provides several services, including administration, user management, data visualization, task management, and so on.

Journal Pre-proof

4. Working process of the proposed architecture

The proposed architecture is designed to enable secure operation management in smart industrial environments. These operations include system initialization, sensor and actuator data storage, and client services that perform industrial operations in a trustworthy manner. All these operations are briefly described in the following subsections.

4.1. System initialization

During the initialization phase, user clients and corresponding IoT devices are registered in the blockchain network. This process is required to allow the re-authentication of users and devices. The registration process is further divided into two phases: user registration and device registration. These registration processes are explained below.

4.1.1. User registration

In this phase, first, a system administrator generates a new unique ID for a client. Then, the admin sends this ID to the blockchain node in the form of a transaction proposal. The blockchain node first verifies the existence of this ID in the network using a smart contract. If the ID already exists, then the transaction is denied, and a notification is issued to the admin. When the ID is not already available in the network, then the smart contract allows the transaction. After the PoAh mechanism is executed, a new block is generated that is distributed among all the blockchain nodes. If the user is successfully registered, the blockchain generates a user ID certificate using its private key and sends it to the admin. Administrators can extract certificate information by using their own private keys. The user registration process is presented in Figure 4. The execution of the this process is further elaborated in Algorithm 2.

Algorithm 2: User Registration

```
1   begin
2     Admin generates a unique ID for the client.
3     User ID: SHAHID314
4       if (User_ID_exist == true)
5         Deny transaction
6         return error ()
7       else
8         Execute PoAh.
9         Register user ID in blockchain
10        return user ID certificate
11  end
```

4.1.2. Device registration

In the proposed architecture, the physical layer contains sensor and actuator devices. After the necessary preprocessing is performed on the sensor's or actuator's data, the STM32-based microcomputer sends the information to a lightweight node in the blockchain service layer. The lightweight node processes the device registration request to the blockchain node as a new transaction proposal. A smart contract verifies the device ID and executes the transaction in the blockchain network. After the PoAh process is completed, a new block is generated and distributed among all the blockchain nodes. All the sensors and actuators are registered in the blockchain network with a unique ID and each registration follows the same process, as shown in Figure 5. The execution of device registration process is further elaborated in Algorithm 3.

Algorithm 3: Device Registration

```
1   begin
2     IoT device generates a unique ID.
3     Device ID: PRESSURE587.
4     Microcomputer sends the information to light
      nodes.
5     Light nodes process the registration request.
6       if (Device_ID_exist == true)
7         Deny transaction.
8         return error ( )
9       else
10        Execute PoAh
11        Register device ID in blockchain
12        Issue the notification of successful registra-
      tion.
13  end
```

4.2. Data storage

All the sensors and actuators are successfully registered in the blockchain network during the first phase. The next important part of operation management is to store data in the blockchain network from the registered devices. Figure 6 shows the data storage process from the IoT device to the blockchain network. Here, STM32 performs the necessary preprocessing on a sensor's data and sends it to a lightweight node of the blockchain service layer. First, the ARM Cortex-M4-based lightweight node verifies the device by using its registration ID. If the blockchain authenticates the device, then the processor executes ECDSA in real time. This process encrypts the data and generates public and private keys. All the information is copied to all the lightweight nodes, which provides a backup facility in case a single node crashes. After the encryption process, the lightweight node interacts with a smart contract to execute the transaction. The smart contract allows the transaction and stores the encrypted data in the blockchain network. Here, the public key is used to verify the integrity of the data, and the private key is shared only with authorized users who can decrypt the data after accessing it from the blockchain network. All the devices in the physical layer follow this same process. The data storage process is further elaborated in Algorithm 4.

4.3. Operation management

The proposed architecture facilitates the utilization of the services of a smart industrial environment by using the blockchain network. These services include access to stored sensor data and actuators operation based on their requirements.

Journal Pre-proof

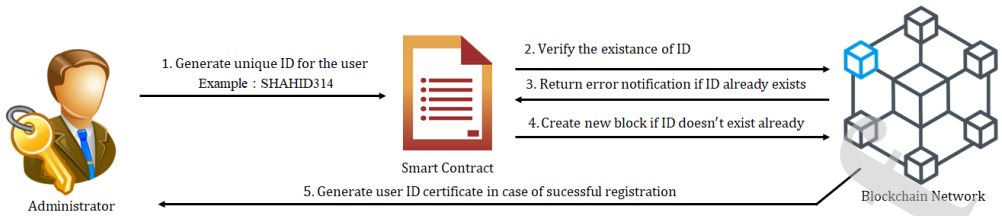

Figure 4: User registration process.

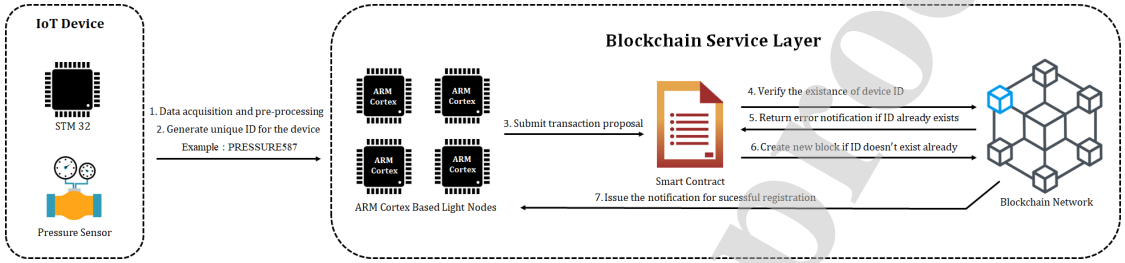

Figure 5: Device registration process.

4.3.1. Data acquisition

To gain access to the sensor data stored in the blockchain, a user submits a transaction proposal to a smart contract along with the appropriate device information. The first smart contract verifies the user's ID; when verification is successful, it then asks the user for their public key. The user provides their public key, and after verification, the blockchain will grant access to the user. Now, that user can access data from the corresponding device and decrypt it using their private key. The data access process is presented in Figure 7 and further elaborated in Algorithm 5.

4.3.2. Actuation task

To operate actuators such as a motor, solenoid valve, or robotic arm, a user submits a transaction proposal along with the appropriate device information. After verification of the user's ID and device ID, a smart contract will allow the transaction to execute. After successful PoAh, the blockchain will then allow the user to operate the corresponding actuator. After completing the actuating process, the actuator sends the latest information to the blockchain service layer along with the actuation task results. The lightweight nodes again update the blockchain record. The actuation process

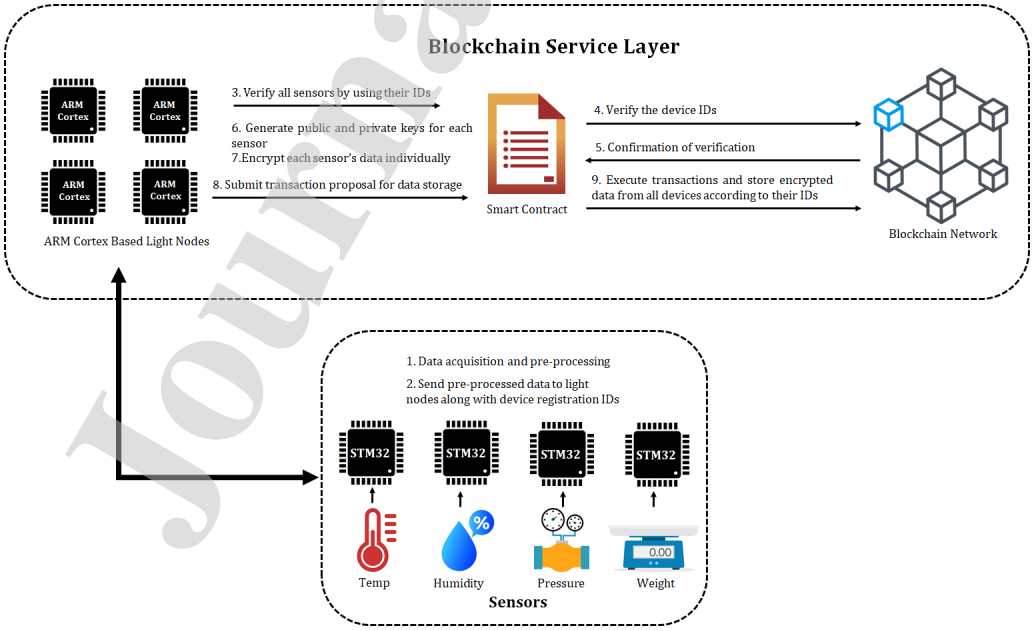

Figure 6: The sensor data storage process.

Journal Pre-proof

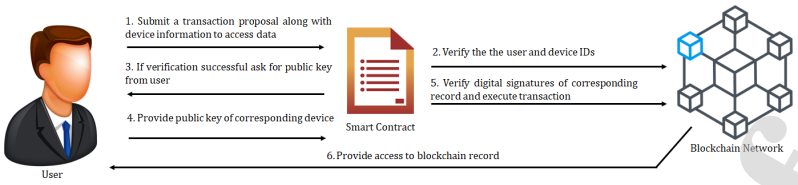

Figure 7: Data acquisition process.

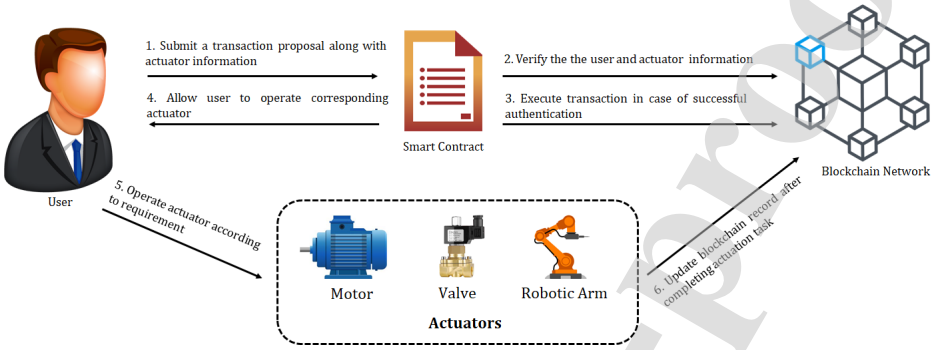

Figure 8: The process to operate actuators.

Algorithm 4: Data Storage

```
1  begin
2    STM32 microcomputer pre-process sensor's data.
3    Send information to ARM Cortex light nodes.
4    ARM cortex verifies the device using its registration ID.
6      if (device authentication == true)
7        Execute ECDSA
8        Generate public and private keys.
9        Submit transaction proposal to blockchain for data storage.
10         if (PoAh == true)
11           Store encrypted data in the blockchain network.
12         else
13           return error ( )
14       else
15         Deny transaction
16         return error ( )
17 end
```

Algorithm 5: Data Acquisition

```
1  begin
2    The user submits a transaction proposal along with device information.
3    Blockchain nodes verify the user and device IDs.
6      if (verification == true)
7        Ask public key from the user.
8      else
9        return error ( )
10   The user provides the public key of the corresponding device.
11   Blockchain network verifies digital signatures of corresponding record.
12     if (verification == true)
13       Execute transaction.
14       Provide access to the blockchain record.
15     else
16       Deny transaction.
17       return error ( )
18 end
```

is presented in Figure 8 and further elaborated in Algorithm 6.

5. Performance analysis

In this section, we evaluate the performance of the proposed framework in the context of cryptography, consensus algorithms, and different operations.

5.1. Performance of ARM Cortex-M processors for asymmetric cryptography

The most significant feature of this research is that we introduced an implementation of the cryptographic algorithm at the device level for the blockchain network. Here, we evaluate the performance of the four M series processors in the context of asymmetric cryptography. In our research, we implemented ECDSA using the X-CUBE-CRYPTOLIB library, which has been certified for industrial use by the NIST Cryptographic Algorithm Validation Program. To determine the statistical error of the obtained results (X_i) over the number of executions (N), the mean ($\bar{X}$), standard deviation (σ_X) and standard error ($\sigma_{\bar{X}}$) can be calculated using

Journal Pre-proof

Algorithm 6: Operation of Actuators

```
begin
    The user submits a transaction proposal along with actuator information.
    Blockchain nodes verify the user and actuator information.
        if ((user_ID&&actuator_ID == true)
          Execute transaction.
          Allow the user to operate the corresponding actuator.
        else
          return error ( )
    The user performs desired actuation operation,
    After task completion, actuator send the latest information to light nodes.
    Light nodes update blockchain record with the latest information
end
```

equations (1) to (3).

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \tag{1}$$

$$\sigma_X = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})^2} \tag{2}$$

$$\sigma_{\bar{X}} = \frac{1}{\sqrt{N}}\sigma_X \tag{3}$$

To evaluate the performance of ARM Cortex-M series processors, we consider three performance metrics.

5.1.1. Execution time

This is the total time required for key generation, encryption, and decryption using ECDSA. To determine the best execution time of ECDSA, we consider the records of 15 executions for each processor. The execution time of each processor for ECDSA is graphically presented in Figure 9. For in-depth analysis, the execution time is calculated in terms of mean, standard deviation, and standard error for each processor. These results are presented in Table 1. The estimated execution time of ECDSA for each processor is mentioned in the following.

$$M0 : 17.253\ s\ \pm 0.001\ s$$

$$M3 : 26.352\ s\ \pm 0.002\ s$$

$$M4 : 1.462\ s\ \pm 0.000\ s$$

$$M7 : 1.156\ s\ \pm 0.000\ s$$

According to the obtained results, the average execution times of processors M0 and M3 are quite high: 17.253 s and 26.352 s, respectively, while the execution times for processors M4 and M7 were 1.462 s and 1.156 s, respectively. The

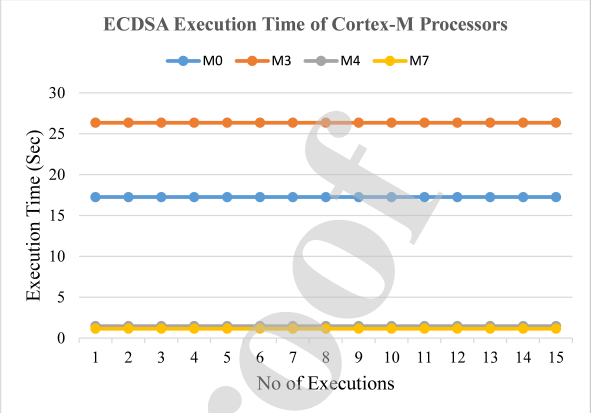

Figure 9: Comparative representation of execution time by each processor.

Table 1
Detailed comparison of execution time for ECDSA.

Processor	$\bar{X}(sec)$	$\sigma_X(sec)$	$\sigma_{\bar{X}}(sec)$
M0	17.253	0.002	0.001
M3	26.352	0.006	0.002
M4	1.462	0.000	0.000
M7	1.156	0.000	0.000

results indicate that the M4 and M7 processors have the best ability to execute ECDSA. These time measurements enable easy planning and adjustments to determine the delay tolerance in an IIoT network.

5.1.2. Power consumption

This metric describes the power consumption by the microprocessor (MP) during cryptographic algorithm execution. The consumed power was calculated by measuring the voltage V_{MP} across a shunt resistance R. The current consumption of the processor I_{MP} was calculated by using Ohm's Law.

$$I_{\mathrm{MP}} = \frac{V_{\mathrm{MP}}}{R} \tag{4}$$

Here R is the shunt resistance of 1.0 ohms.

The power consumption of the processor can be calculated by using equation (5).

$$P_{\mathrm{MP}} = V_S \times I_{\mathrm{MP}} \tag{5}$$

Here V_S is the supply voltage, $V_S = 5V$

The mean, standard deviation, and standard error of power consumption are calculated by using equations (1) to (3). To determine the average power consumption, ECDSA was executed for 15 runs. The comparison of power consumption by MPs is presented in Figure 10.

Detailed mathematical results of power consumption are presented in Table 2. The estimated power consumption of

Journal Pre-proof

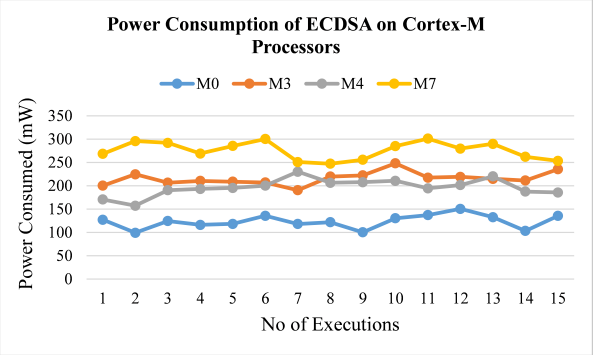

Figure 10: Comparative representation of power consumption by each processor for ECDSA.

each processor for ECDSA is mentioned in the following.

$$M0 : 123.383\ mW \pm 7.989\ mW$$

$$M3 : 215.793\ mW \pm 2.726\ mW$$

$$M4 : 196.802\ mW \pm 6.442\ mW$$

$$M7 : 275.791\ mW \pm 3.078\ mW$$

Table 2
Detailed comparison of power consumption for ECDSA.

Processor	$\bar{X}(mW)$	$\sigma_X(mW)$	$\sigma_{\bar{X}}(mW)$
M0	123.383	30.941	7.989
M3	215.793	10.558	2.726
M4	196.802	24.949	6.442
M7	275.791	11.921	3.078

The obtained results show that the average power consumption by the M0, M3, M4, and M7 processors were 123.383 mW, 215.793 mW, 196.802 mW, and 275.791 mW respectively. This comparison shows that the power consumption of all the processors is low. Therefore, the implementation of ECDSA on the ARM Cortex-M processors is an energy-efficient solution.

5.1.3. Memory utilization

Memory utilization includes the utilization of both RAM and flash memory for the implementation of the cryptographic algorithm. We used the memory analyzer tool Atollic TrueSTUDIO, which provides a detailed analysis of RAM and flash memory utilization. The RAM and flash memory utilization of ECDSA is described below.

RAM: Each processor in the ARM Cortex-M series has a different RAM configuration. The detailed results of the RAM occupation analysis conducted for ECDSA are summarized in Table 3. A graphical representation of the percentage of RAM used by each processor for the ECDSA is also presented in Figure 11. According to the obtained results, M0 and M3 possess relatively large amounts of RAM considering their total capacities. M4 and M7 are both

Table 3
RAM occupation of ECDSA for ARM Cortex-M series processors.

ARM Cortex Processor	Memory Utilization (RAM)		
	Total	Utilized	Percentage (%)
M0	8 kB	1.59 kB	19.88
M3	8 kB	1.57 kB	19.63
M4	128 kB	3.52 kB	2.75
M7	512 kB	1.65 kB	0.32

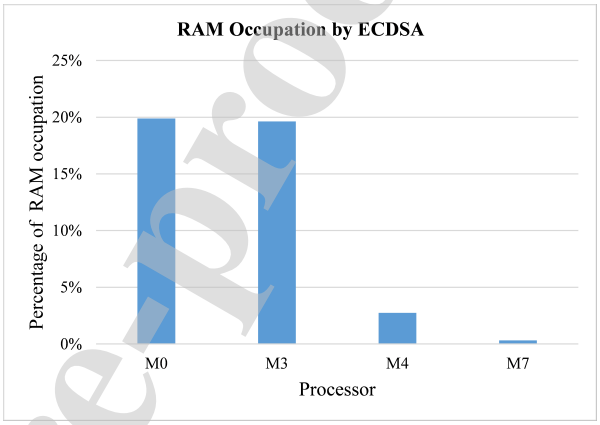

Figure 11: RAM occupation by each Cortex-M processor for ECDSA.

equipped with even larger amounts of RAM, so the overall memory utilization in the two processors constitutes a smaller percentage of their total capacity.

Flash: This memory holds the main code. The detailed results of the Flash occupation analysis conducted for ECDSA are summarized in Table 4. A graphical representation of the percentage of Flash used by each processor for the ECDSA is presented in Figure 12. According to memory analyzer tools, ECDSA occupies 40.42% and 18.73% of the available flash memory for M0 and M3, respectively, while for the M4 and M7 processors, the values were only 3.15% and 1.19%, respectively.

Table 4
Flash occupation of ECDSA for ARM Cortex-M series processors.

ARM Cortex Processor	Memory Utilization (Flash)		
	Total	Utilized	Percentage (%)
M0	64 kB	25.87 kB	40.42
M3	128 kB	23.97 kB	18.73
M4	1024 kB	33.28 kB	3.15
M7	2048 kB	30.57 kB	1.49

Based on the above discussion, ECDSA is a lightweight cryptographic algorithm. We do not recommend the M0 and M3 processors for ECDSA cryptographic operations because of their longer execution times and higher memory utilization rates; however, implementing ECDSA on the ARM Cortex-M4 and M7 processors is highly suitable for real-time cryptography applications in IIoT. More precisely, the

Journal Pre-proof

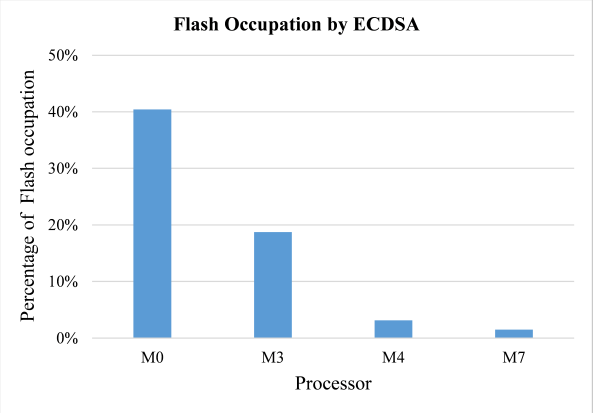

Figure 12: Flash occupation of ECDSA for ARM Cortex-M series processors.

low-power ARM Cortex-M4 is an ideal choice for this purpose.

5.2. Analysis of the PoAh consensus algorithm

The PoAh algorithm implements an authentication mechanism that uses fewer resources and less energy. It can be highly advantageous for the resource-constrained IIoT architectures. In the following, we present an overview of the most significant characteristics of the PoAh consensus algorithm.

5.2.1. Resource utilization

PoW is a traditional consensus algorithm in which individual nodes generate the data blocks and miners validate them before being added to the blockchain. The mining process is a computation of the reverse hash function that consumes a lot of energy [30]. Too much energy utilization is not feasible for resource-constrained IIoT networks. PoAh addresses this issue by utilizing minimal energy. It introduces an authentication mechanism that utilizes cryptography and digital signatures. In the context of cryptography, digital signature verification and hash computation is a fast and energy-efficient process. Therefore, PoAh is an energy-efficient solution for resource-constrained IIoT systems.

5.2.2. Execution time

PoAh requires less execution time as compared to traditional PoW without compromising security threats. PoW approximately takes 10 minutes to validate a single block [30]. It is not feasible for any kind of IoT application. PoAh resolves this issue by utilizing cryptographic authentication for block validation. Cryptographic authentication is a very fast process that significantly reduces the execution time. Therefore, PoAh can be an ideal choice for resource-constrained IIoT networks.

5.2.3. Security

The integration of PoAh as a consensus algorithm in blockchain-based IoT frameworks provides a sustainable security solution for IoT frameworks. IoT systems don't require the same level of security as required for cryptocurrencies [31]. IoT applications require real-time security with proper authentication of data. PoAh integrates with the existing cryptographic concept of PoW excluding the reverse hash computation for block validation. Therefore, PoAh provides a sufficient level of security with ECDSA in decentralized IIoT networks. Furthermore, the PoAh addresses two major weaknesses of current blockchain consensus, namely unstable network connectivity, and the 51% attack in the network. In PoAh, all the network devices are eligible to generate blocks, whereas only trusted nodes are authenticating them. In any unfavorable situation arising from these weaknesses, are not broadcast to all peers. Only trusted peers can authenticate and add blocks to the chain. As a result, the 51% attack weakness of PoW is addressed due to the dynamic nature of trust values.

5.3. Performance evaluation of industrial operations

This section presents the performance analysis of the proposed blockchain architecture. Several experiments were performed to evaluate the service execution time for different industrial operations. The execution time or CPU time of a given task is defined as the time spent by the system executing that task, including the time spent executing run-time or system services on its behalf. The proposed system performs five different industrial operations that include user registration, device registration, sensor data recording, data acquisition, and actuation. In this study, we divided the users, devices, records, and actuators into different groups and record the service execution time by performing extensive simulations in a python environment using Dell Alienware Aurora R11 Core i7 desktop computer. In the following, we discuss the service execution time of each operation.

First, we analyze the user registration process in the blockchain-enabled smart industrial network. Users are divided into five groups which contain, 10, 20, 30, 40, and 50 members. The registration process of a single user required three main steps that include, submission of transaction proposal, authentication of the transaction, and update the blockchain after successful authentication. For the first group, the minimum and maximum execution time are recorded as 1012 ms and 1471 ms respectively. The average execution time for the first group is recorded as 1263 ms. Comparative analysis of service execution time for the different groups of users is presented in the bar graph as shown in Figure 13. This comparison indicates, that the increase in the number of users required more execution time. The 5th group is considered as the largest group that contains 50 users. The average time for this group is recorded as 1900 ms. The overall response of the user registration process is fast.

In the second phase, the device registration process is analyzed. Same as previous sections devices are categorized into five groups that contain 10, 25, 50, 75, and 100 devices. Most of these devices are sensors equipped with mini computing devices and few actuators. The device reg-

Journal Pre-proof

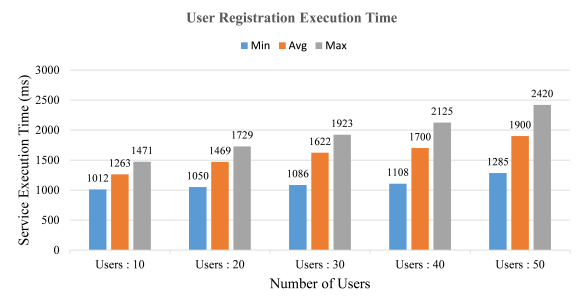

Figure 13: Comparative analysis of service execution time for the user registration process.

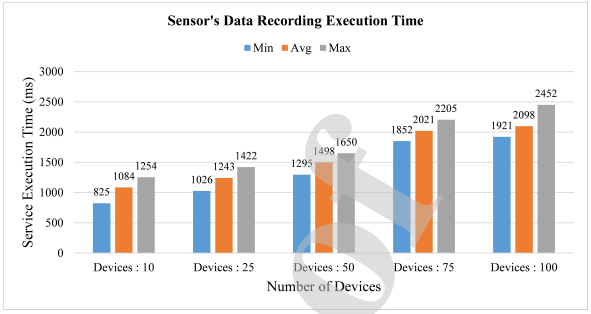

Figure 15: Comparative analysis of service execution time for the sensor's data storage process.

istration process contains 4 step that includes the generation of unique ID for each device, submission of transaction proposal, validation of transaction, and registration of device in blockchain network after a successful transaction. Comparative analysis of service execution time for the different groups of devices is presented in the bar graph as shown in Figure 14. The average execution time for the smallest group is recorded as 1175 ms. The minimum and maximum time for this group are recorded as 1025 ms and 1308 ms respectively. Same as user registration the execution time is gradually increasing with the increase in the number of devices.

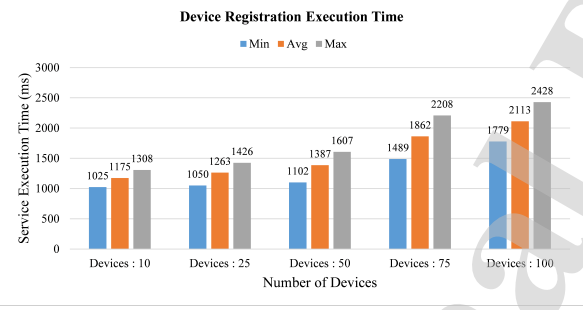

Figure 14: Comparative analysis of service execution time for the device registration process.

In the third phase, the sensor's data recording process is analyzed. Data recording in immutable manners is one of the most significant characteristics of blockchain-enabled systems. For the proposed solution the sensors are categorized into five groups which contain 10, 25, 50, 75, and 100 devices. Data storage in the blockchain network is a four-stage process that includes sensor authentication, data encryption, transaction execution, and storage of the sensor's data storage according to the device ID. Comparative analysis of service execution time for the different groups of sensors for data recording is presented in a bar graph as shown in Figure 15. According to the graph, the average execution time for the largest group of devices is recorded as 2098 ms. It indicates the satisfactory performance of the proposed architecture in terms of the sensor's data recording.

The fourth important operation is to access the sensor's data by authorized users. This is a three steps process that includes submission of transaction proposal along with user and device information, user and device authentication, and provide them access to stored information after successful authentication. To evaluate the execution time the sensor's record is categorized into five groups that contain the numerical data of environmental parameters such as temperature, pressure, weight, and humidity, etc. Comparative analysis of service execution time for the different groups of records is presented in a bar graph as shown in Figure 16. According to the graph, the overall execution time is less than 1000 ms which indicates the faster performance for this operation. The average execution time for the largest group of sensor's records is recorded as 578 ms. It indicates the satisfactory performance of the proposed architecture in terms of the sensor's data recording.

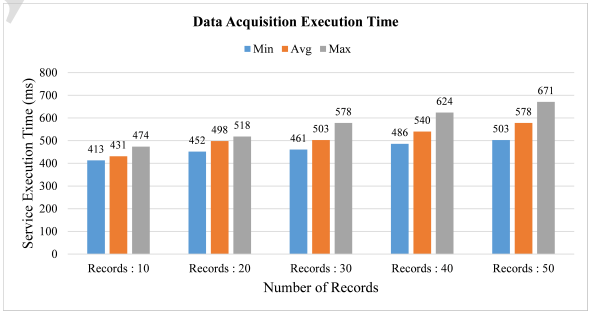

Figure 16: Comparative analysis of service execution time for the data acquisition process.

The final task of the proposed platform is to operate industrial actuators and record the process variables during operation. This is the heaviest process in terms of processing time and energy consumption. It contains five stages that include submission of transaction proposal along with user and actuator's information, verification of user and actuator's ID, permission to operate actuator after successful authentication, actuators operation, and update the records of blockchain after task completion. To evaluate the service execution time, we categorized the actuators into five groups that include 1, 2, 3, 4, and 5 actuators. Comparative analysis of service execution time for the different groups of actuators is presented in a bar graph as shown in Figure 17. Accord-

Journal Pre-proof

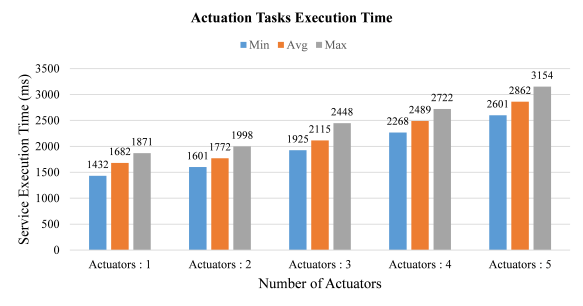

Figure 17: Comparative analysis of service execution time for the data acquisition process.

ing to the graph, an average execution time for the single actuator is recorded as 1682 ms. For the largest group, the average execution time is recorded as 2862 ms. In summary, the overall results of service execution time indicate the satisfactory performance of the proposed blockchain platform for each operation.

5.4. Performance comparison with state-of-the-art blockchain-based architectures

Most of the recent studies mainly focused on the sensor's data storage using blockchain technology. These studies don't concentrate on other operations in a smart industrial environment. Another shortcoming of the aforementioned researches is that they didn't present the security measures to protect industrial data at the device level. The first significant contribution of our study is that we introduced lightweight cryptography and authentication at the device level that also ensures data protection outside the blockchain network. Another distinction of this work is to build a trust mechanism among all the elements and operations of the network that ensures security and transparency at all levels of the smart industry. In this section, we compare the proposed blockchain architecture with other state-of-the-art schemes. This comparison is organized on the basis of the different cryptography schemes, consensus mechanisms, blockchain platforms, energy efficiency, hardware dependency, speed and processing fee. The detailed comparison is presented in Table 5. Cryptography is an integral part of blockchain technology that is used to protect user identities, to ensure transactions, and to secure all kinds of information. In the blockchain context, asymmetric key cryptography is preferred over symmetric key cryptography. Different researchers have utilized various commonly available cryptographic schemes in their studies. These schemes include the Advanced Encryption Standard (AES), the 256-bit Secure Hash Algorithm (SHA-256), ECDSA, identity-based signature (IBS) schemes, and elliptic-curve Diffie-Hellman key exchange (ECDHE). All these schemes have their own advantages and disadvantages. We selected ECDSA for our architecture for several reasons. First, ECDSA has been certified by the NIST Cryptographic Algorithm Validation Program for industrial applications [26]. Second, this algorithm has low computational complexity and low memory requirements. The implementation of ECDSA on a low-power ARM Cortex-M4 proves that this scheme is the ideal, lightweight choice.

In blockchain technology, the consensus process allows new transactions to be added to the network. In related work, a few researchers have proposed lightweight consensus mechanisms by considering the resource-constrained nature of devices and the issue of scalability. Some of them have utilized conventional consensus algorithms such as PoW, PoS, PoC, and PoA algorithms. However, the energy requirements of the PoW approach are very high; thus, it is not recommended for any kind of low-power computation device. The computational complexities and energy requirements of the PoS, PoC, and PoA approaches are lower than those of the PoW approach but still not much more feasible for many low-performance devices. Therefore, in the proposed architecture, we use the PoAh approach, which requires less energy resource consumption for block validation. The PoAh mechanism uses cryptographic authentication for block validation, which makes it faster than other consensus algorithms. The third point of comparison is the blockchain platform used. Most researchers have used open-source platforms for their architectures. Although these platforms provide good-quality services for specific applications, the use of third-party services can sometimes create savior problems. To address this challenge, we have introduced a private blockchain network for the smart industry.

Energy efficiency is another important parameter that usually depends upon the selected consensus algorithm. Traditional PoW is not feasible for any kind of energy-efficient applications. PoC and PBT have fair energy efficiency for particular some specific IoT devices. Experimental results proved that PoAh as a consensus mechanism is energy efficient. As most of the researchers used open-source platforms, few of them provide support for specific hardware platforms. Therefore, hardware dependency is another issue that is addressed in this work. Extensive experiments indicate the faster performance of the proposed framework. The last factor of comparisons is the transaction processing fee. Different blockchain platforms charge some processing fees for their services which can be sometimes costly. The prosed framework utilizes fewer resources so there is no processing fee involved.

In summary, the proposed architecture is an advantageous combination of the ECDSA encryption algorithm, the PoAh consensus mechanism, and a private network, that makes it an ideal and secure, fast, and energy-efficient blockchain platform for a smart industrial environment.

6. Experiment: A blockchain-based fruit processing plant

IIoT has become a staple of modern research trends for industry and academia. Several researchers have proposed intelligent systems to enhance the capabilities and performance of industrial environments. Along with other modern industry characteristics, security and privacy are important

Journal Pre-proof

Table 5
Performance comparison with state-of-the-art.

Author	Cryptographic Scheme	Consensus Mechanism	Blockchain Platform	Energy Efficiency	Hardware Dependency	Speed	Processing Fee
Cao et al. [17]	SHA-256	PoC	Hyperledger	Fair	Yes	Slow	No
Huang et al. [19]	AES, SHA-256	Credit-base PoW	DAG-Structured Blockchain	Yes	No	Fair	Yes
He et al.[20]	Local Public-Key	PBFT	BigchainDB	Fair	No	Slow	Yes
Liang et al.[21]	Local Public-Key	PoW	Hyperledger Fabric	No	Yes	Slow	No
Umair et al.[22]	ECDSA	PoC	Ethereum Blockchain	Fair	Yes	Fair	Yes
Shen et al. [23]	IBS, ECDHE	PoW	Consortium Blockchain	No	Yes	Slow	No
Our Study	ECDSA	PoAh	Private Blockchain	Yes	No	Fast	No

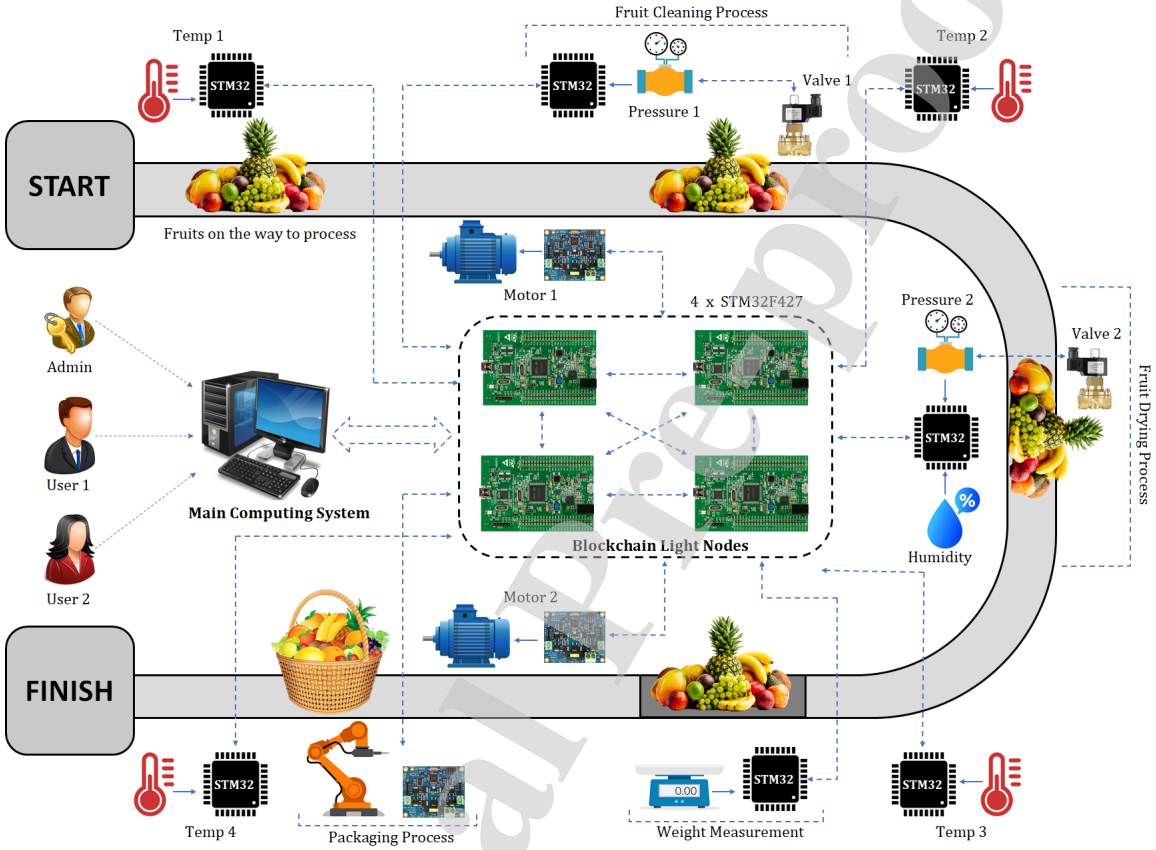

Figure 18: A blockchain-based fruit processing plant.

factors. In this context, we introduced and implemented a blockchain-based architecture for fruit processing plants.

A brief blockchain-based architecture for fruit processing is presented in Figure 18. In this plant, from start to finish, all the processes are performed as the fruit passes along a specially designed conveyor belt. The belt movement is controlled by 2 high-torque DC gear motors. Intelligent motor driver modules are also deployed to control these motors efficiently. In the fruit processing environment, room temperature is also highly important. To maintain room temperature efficiently, 4 high precision temperature sensors are deployed along with STM32 microcomputers. The next stage is the fruit cleaning process, which is performed by low-pressure steam. At this stage, a pressure sensor and an STM32 are interfaced with a solenoid valve. This combination effectively maintains the steam pressure. In the second stage, the fruit drying process is conducted by forced air. Here, pressure and humidity sensors are used with STM32 to maintain a suitable air pressure and humidity. A solenoid valve controls the air flow by interacting with the pressure sensor. The third stage involves preparing the fruits according to user requirements. Here, a weight sensor is used with an STM32 to sort the fruit according to a desired weight range. In the final stage, a robotic manipulator is used to pack the fruits into a basket or box; then, the conveyor belt forwards the packed fruit to another section for further processing.

To record the sensing data and states of actuators efficiently, these modules are interfaced with the lightweight nodes of the blockchain service layer. This section consists of four STM32F427 development boards. Each module has a copy of the record. If a single node fails, another node acts as a backup. The lightweight nodes execute the real-time encryption processes on the collated data and send these data

Journal Pre-proof

to the main computing system where the private blockchain is designed. Finally, the data are stored in secure and well-organized manner in the blockchain network. Administrators and authorized users are also connected to the system and access the services according to requirements.

In a traditional IIoT system, the security and privacy aspects of industrial modules are not generally deeply considered. Blockchain technology provides the best form of security in an industrial environment and makes it very difficult for an attacker to insert a device into a system or obtain access to sensitive industry records. In conclusion, blockchain is a very promising technique that can ensure security, confidentiality, and verification in a smart industrial environment.

7. Conclusion

The industrial IoT modernizes smart industries by introducing the latest technologies, and blockchain is an emerging technology that has received substantial attention from both academia and industry. Integrating blockchain technology into a smart industry adds several advanced features, including security, immutability, trust, decentralization, and a greater degree of automation. In this paper, we propose a blockchain-based architecture for a smart industrial environment. The proposed scheme enables a secure, lightweight, and decentralized private blockchain-based IIoT network that performs several critical operations, such as user and device enrollment, data storage, and machine operation in a trusted manner. In particular, we introduce an implementation of asymmetric cryptography at device level that reduces the computational complexity and enhance the security of the industrial platform. The performance of the proposed architecture is evaluated by considering several performance parameters. Experimental results proved the superior performance of the proposed architecture as compared to other state-of-the-art schemes. Finally, we transformed a traditional fruit processing plant based on the proposed architecture to achieve the great potential of blockchain technology for a smart industry.

References

[1] Martin Wollschlaeger, Thilo Sauter, and Juergen Jasperneite. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE industrial electronics magazine*, 11(1):17–27, 2017.

[2] Jiafu Wan, Jiapeng Li, Muhammad Imran, and Di Li. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, 15(6):3652–3660, 2019.

[3] Daniel Kiel, Christian Arnold, and Kai-Ingo Voigt. The influence of the industrial internet of things on business models of established manufacturing companies–a business level perspective. *Technovation*, 68:4–19, 2017.

[4] Charith Perera, Dumidu S Talagala, Chi Harold Liu, and Julio C Estrella. Energy-efficient location and activity-aware on-demand mobile distributed sensing platform for sensing as a service in iot clouds. *IEEE Transactions on Computational Social Systems*, 2(4):171–181, 2015.

[5] Shahid Latif, Zhuo Zou, Zeba Idrees, and Jawad Ahmad. A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE Access*, 8:89337–89350, 2020.

[6] Shanshan Zhao, Shancang Li, and Yufeng Yao. Blockchain enabled industrial internet of things technology. *IEEE Transactions on Computational Social Systems*, 6(6):1442–1453, 2019.

[7] Yong Chen. Industrial information integration—a literature review 2006–2015. *Journal of Industrial Information Integration*, 2:30–64, 2016.

[8] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.

[9] Yong Chen. A survey on industrial information integration 2016–2019. *Journal of Industrial Integration and Management*, 5(01):33–163, 2020.

[10] Lei Hang and Do-Hyeun Kim. Reliable task management based on a smart contract for runtime verification of sensing and actuating tasks in iot environments. *Sensors*, 20(4):1207, 2020.

[11] Elisa Bertino and Nayeem Islam. Botnets and internet of things security. *Computer*, 50(2):76–79, 2017.

[12] Zhiwei Zhao, Geyong Min, Weifeng Gao, Yulei Wu, Hancong Duan, and Qiang Ni. Deploying edge computing nodes for large-scale iot: A diversity aware approach. *IEEE Internet of Things Journal*, 5(5):3606–3614, 2018.

[13] Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018.

[14] William J Gordon and Christian Catalini. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, 16:224–230, 2018.

[15] Fei-Yue Wang, Yong Yuan, Jun Zhang, Rui Qin, and Michael H Smith. Blockchainized internet of minds: A new opportunity for cyber–physical–social systems. *IEEE Transactions on Computational Social Systems*, 5(4):897–906, 2018.

[16] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 2008.

[17] Yan Cao, Feng Jia, and Gunasekaran Manogaran. Efficient traceability systems of steel products using blockchain-based industrial internet of things. *IEEE Transactions on Industrial Informatics*, 2019.

[18] Mengting Liu, F Richard Yu, Yinglei Teng, Victor CM Leung, and Mei Song. Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach. *IEEE Transactions on Industrial Informatics*, 15(6):3559–3570, 2019.

[19] Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, 15(6):3680–3689, 2019.

[20] Sen He, Wei Ren, Tianqing Zhu, and Kim-Kwang Raymond Choo. Bosmos: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial internet of things. *IEEE Internet of Things Journal*, 7(2):948–959, 2019.

[21] Wei Liang, Mingdong Tang, Jing Long, Xin Peng, Jianlong Xu, and Kuan-Ching Li. A secure fabric blockchain-based data transmission technique for industrial internet-of-things. *IEEE Transactions on Industrial Informatics*, 15(6):3582–3592, 2019.

[22] Umair Khalid, Muhammad Asim, Thar Baker, Patrick CK Hung, Muhammad Adnan Tariq, and Laura Rafferty. A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Cluster Computing*, pages 1–21, 2020.

[23] Meng Shen, Huisen Liu, Liehuang Zhu, Ke Xu, Hongbo Yu, Xiaojiang Du, and Mohsen Guizani. Blockchain-assisted secure device authentication for cross-domain industrial iot. *IEEE Journal on Selected Areas in Communications*, 38(5):942–954, 2020.

[24] Avrohom Gottheil. Iiot world: Can blockchain address the industrial iot security?, 2018. http://iiot-world.com/cybersecurity/can-blockchain-address-the-industrial-iot-security/.

Journal Pre-proof

[25] Arm Ltd. Microprocessor cores and technology, 2020. https://www.arm.com/products/silicon-ip-cpu.

[26] STMicroelectronics. X-cube-cryptolib: Stm32 cryptographic firmware library software expansion for stm32cube (um1924), 2020. https://www.st.com/en/embedded-software/x-cube-cryptolib.html.

[27] Nikolay Teslya and Igor Ryabchikov. Blockchain platforms overview for industrial iot purposes. In *2018 22nd Conference of Open Innovations Association (FRUCT)*, pages 250–256. IEEE, 2018.

[28] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 254–269, 2016.

[29] Deepak Puthal and Saraju P Mohanty. Proof of authentication: Iot-friendly blockchains. *IEEE Potentials*, 38(1):26–29, 2018.

[30] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.

[31] Deepak Puthal, Nisha Malik, Saraju P Mohanty, Elias Kougianos, and Chi Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, 2018.

Journal Pre-proof

Journal Pre-proof

Credit Author Statement

Dear Editor,

We declared that **Shahid Latif** is the main contributor and author.

Shahid Latif (S.L)

Zeba Idrees (Z.I)

Jawad Ahmad (J.A)

Lirong Zheng (L.Z)

Zhuo Zou (Z.Z)

Authors Contributions: Conceptualization, (S.L, Z.I, J.A, Z.Z) and Methodology, (S.L); Software, (S.L); Validation, (S.L) and; Formal Analysis, (S.L, Z.I, J.A); Investigation, (S.L, Z.I); Resources, Z.Z and L.Z); Writing-Original Draft Preparation, (S.L, Z.I); Writing-Review & Editing, (S.L, Z.I. J.A. Z.Z); Visualization, (S.L, Z.I. J.A. Z.Z); Supervision, (Z.Z, L.Z); Project Administration, (Z.Z, L.Z); Funding Acquisition, (Z.Z, L.Z).

Best Regards

Shahid Latif et al.

Micro and Nano System Center

School of Information Science and Engineering

Fudan University, Shanghai, China

Journal Pre-proof





Journal Pre-proof

Journal Pre-proof

Conflicts of Interest Statement

The authors have no conflicts of interest to declare. All coauthors have seen and agree with the contents of the manuscript and there is no conflict of interest to report. We certify that the submission is original work and is not under review at any other publication.

Best Regards

Shahid Latif et al.

Micro and Nano System Center

School of Information Science and Engineering

Fudan University, Shanghai, China

Journal Pre-proof