On the Design and Implementation of a Secure Blockchain-based Hybrid Framework for Industrial Internet-of-Things

Geetanjali Rathee[a], Farhan Ahmad[b,*], Rajinder Sandhu[a], Chaker Abdelaziz Kerrache[c], Muhammad Ajmal Azad[d]

[a] *Department of Computer Science and Engineering, Jaypee University of Information Technology, India*
[b] *Systems Security Group, Institute for Future Transport and Cities, Coventry University, Coventry, United Kingdom*
[c] *Laboratoire d'Informatique et de Mathématiques, Université de Laghouat, Laghouat, Algeria*
[d] *Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom*

Abstract

Industrial Internet-of-Things (IIoT) refers to the next stage in the evolution of organizations where collecting, analyzing, recording the data and controlling the entire activities of the various entities is achieved with connected machines in real time with enhanced quality and minimum production cost. Although, various phenomenal schemes for cross management activities exist in current systems, however there are still several concerns with such setups within the organizations. Further, the introduction of Internet-of-things (IoT) within the industries is increasing the scope of applications by connecting every device with the Internet. However, these IoT devices are prone to various attacks by the intruder, thus affecting the industry with lower production and high manufacturing cost, to name a few. To address these issues, Blockchain is considered as one of the best scheme which offers protection and secrecy of control systems in real time upto certain level. In this paper, we have proposed a hybrid Blockchain

*Corresponding author
Email addresses: geetanjali.rathee123@gmail.com (Geetanjali Rathee), ad5899@coventry.ac.uk (Farhan Ahmad), rajsandhu1989@gmail.com (Rajinder Sandhu), ch.kerrache@lagh-univ.dz (Chaker Abdelaziz Kerrache), m.azad@derby.ac.uk (Muhammad Ajmal Azad)

mechanism for providing security for a multi-national level IIoT with offices located in multiple countries. The proposed framework is validated rigorously against various security metrics over conventional mechanism. The simulation results suggest that our proposed solution leads to 94% efficiency in terms of DoS and DDoS threat, message alteration attack and authentication delay.
Keywords: Industrial IoT, blockchain, security, hybrid industry, malicious devices, smart city

1. Introduction

World wide network connectivity has pushed us into an era where suppliers, manufacturers and consumers are spread across the globe and are an inseparable part of a global market system. This new revolution has brought the diverse markets of the world closer and on a single platform where exchange of goods and services occurs freely [1, 2]. The accelerated pace of urbanization in the recent decades has endangered the environment and economic sustainability by raising several social, technical and economic concerns. In spite of providing a much needed push to developing economies by establishing the manufacturing units in these countries by Multinational Corporations (MNCs) and creating jobs for millions, management of entities spread across the globe has been a severe issue that has not been properly addressed [3, 4]. This, combined with the security issues has been an obstruction to the growth and spread of businesses of big firms. Imagine a situation where the headquarters of a company are located at a place X and its manufacturing units are located at Y or Z, the overseeing and management of these entities located thousands of kilometers away from each other has always been a tedious task and a major factor discouraging MNCs in expanding their business oversees.

Traditionally, monitoring and controlling systems in industries such as product manufacturing details, records of product (selling or consuming information), workers' information that acts on the value chain, is usually time consuming, inefficient and apparently slow. The facilities manager has to physically

attend to the entire control system that often leads to delay in action, mainly in food or agriculture industry, the food and water quality controls are managed manually by checking expiry or PH value of the products. The management of these products may involve various individuals and thus puts a lot of responsibility on the organizations. Moreover, it is extremely difficult to trace the products and workers location in real time within the organizations. Sometimes, the lack of communication transparency in real time drives into inefficiency and absence of knowledge about the performance, record of the products and workers' activity may lead to a great loss to an industry's growth. The basic mechanism of using blockchain in Internet-of-Things (IoT) and Industrial Internet-of-Things (IIoT) is the same since in both cases the sensors are collecting the information from the environment and then, transfer it to the blockchain as a new block where each and every information produced by sensors are validated by the miners [5]. In the case of IIoT where the sensors are used to collect the data about shipping information, manufacturing product, data storage etc, every information by the sensors will be maintained in the blockchain and will is again validated by the miners every time.

Industrial IoT (IIoT) refers to the coming phase in the evolution of organizations to trace and control actions of their individuals [6, 7, 8]. Its principle is to gather, analyze, store the information and control the entire actions of the various entities with computerized machines in real time with enhanced quality and abridged production cost. It is directly related to the generation of smart devices that are designed to manage their resources in a more flexible, efficient and fast way. Further, smart devices may over look the entire control systems (i.e. products selling/consuming costs, products manufacturing rate, workers location, malicious activity etc) without any intervention of man power [9]. To implement this scenario, we need a Cyber Physical System (CPS) and Internet of Things (IoT) as a necessity since they allow control and surveillance over the entire activities on real world objects [10, 11]. IoT has turned out to be a common tool adopted across various industries as it provides a considerable value in increased efficiency, cost diminution and superior visibility for all facets of the

business such as logistics [12], transportation [13] and healthcare [14], to name a few. The IoT permits real-time collection of data from the sensors. Further, the deployment of sensors may reduce the security risks regarding product stealing or any misbehavior in the companies. Numbers of organizations have adopted Industrial Internet of Things (IIoT) technology attracted by its security benefits and reduced deployment cost [15, 16, 17].

1.1. Research Objective

Presently, the majority of IoT benefits depend on a centralized client-server paradigm that is connected to cloud servers via Internet. The storage of user's data over the cloud may incorporate a number of security risks [18] such as man-in-middle attack, data falsification threat, cost overhead etc. Users may protect their data by buying their private cloud, however, it further increases the costs related issues for the users and their organizations. Besides the fact that this solution works accurately, the expected escalation recommends that new paradigms must be anticipated.

Nowadays, most of the corporations have a hybrid architecture that is the combination of both centralized and decentralized networking where companies assets are distributed across different countries and cities. The managers or the owners need to communicate and maintain the transparency of all the records between these entities. IIoT refers to a scenario where data is collected from different actuators, sensors and machines within a manufacturing environment, and the objects producing and sharing this information is connected to a decentralized network via Internet [19, 20, 21]. IIoT is intrinsically a decentralized or hybrid system as presented in Figure 1. The figure also depict that a company is located in three different locations in different countries communicating via Internet. All the companies are connected with IoT devices that can be easily manageable and trackable by the owners. Lets suppose that the headquarter of the company is located in location *'X'*, and has all the permissions to keep data, overlook or examine the entire actions of all the branches located at various locations (such as location Y and location Z). IIoT gives the advantage by

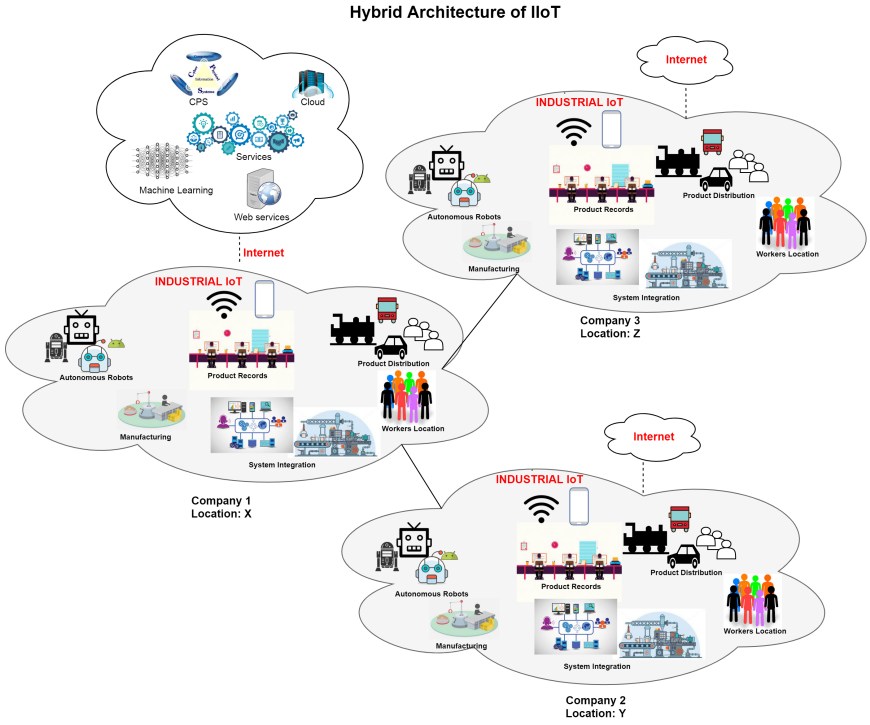

Figure 1: Hybrid Architecture of Industrial Internet-of-Things

monitoring or controlling all the illegal or legal actions occurring at any of its branch from a single place. Despite alot of IIoT benefits, smart control systems or devices may further lead to various security and privacy issues. Security violation in IIoT can occur in variety of ways, such as:

1. A worker may violate the company secrecy by hacking the communication devices to steal important information.
2. Tracing the workers' location, delivery of supplies, product manufacturing, shipment and products documentation were supervised separately that further enhance the issue of information stealing or alteration.
3. It is difficult to look over the actions of all the branches located at various places.

Although, various phenomenal schemes for cross management activities present

in the literature, however there are still several security and privacy concerns that needs to be considered. In order to ensure the security of products manufacturing and delivery, manufacturers need to request some third party agents to receive their materials from the suppliers. Although they may look over the entire manufacturing of the products and delivery details by using different strategies including the CCTV cameras to know the locations of their workers, product shipping action or any type of illegal behavior done by the co-workers. However, these techniques may further enhance the communication cost and other security and privacy concerns.

To ensure a secure and transparent communication mechanism, blockchain is considered as a relevant technology which can coordinate, trace, and keep record of huge amount of objects. It not only provides security during data transmission, but, also ensures a transparent communication between the devices to trace each and every activity of different branches located at different places [22, 23, 24, 25].

1.2. Major contributions

To address the above issues, we proposed a novel technique which can provide security within the context of IIoT networks using blockchain. Therefore, the major contributions of this paper are:

1. Providing a novel architecture ensuring the security of all the records of the products located in different zones.
2. Providing a transparent interaction among communicating entities via blockchain, and
3. Providing an efficient security mechanism using private blockchain framework to reduce the data storage and communication overhead.

1.3. Outline

The remaining structure of the paper is organized as follow. The related works of IIoT and blockchain are discussed in Section 2. The hybrid blockchain scheme in IIoT is detailed in Section 3. In addition, Section 4 elaborates the

simulation results against various network metrics. Finally, Section 5 concludes the work by defining the future directions of the paper.

2. Background and related work

This section presents the recent advancements in Blockchain technology then discusses the existing efforts towards the implementation of Blockchain for Industrial Internet-of-Things (IIoT)

2.1. Recent works on Blockchain technology

Baniata et al. [26] have proposed an ant colony optimization and Blockchain Scheduling System in which the algorithm allowed the fog system to manage, process and perform several latency reduction tasks. The proposed mechanism is validated against more accuracy parameter by improving the network load and execution time. Chen et al. [27] have proposed preservation method using blockchain solutions where in order to recognize the fake news, the approach used the concept of weighting rank and incentive scheme. The proposed approach is further implemented over digital contents to show the benefits. In addition, Berdik et al. [28] have illustrated a literature review on blockchain services where the authors discussed various blockchain studies instances across several applications. The author's have discussed the long term directions of blockchain in various fields. Putz et al. [29] have proposed an Owner-centric decentralized model through a sharing model for ensuring the confidentiality and integrity of the digital components. The proposed scheme is validated over semi-structured industry use case. Oham et al. [30] have proposed a smart blockchain vehicular system in which the author's have used a permissioned blockchain to monitor the vehicles state during communication process. The author's have demonstrated the mechanism that ensured an efficient storage size and response time. Further, Xu et al. [31] have proposed theoretical model for computing the transactional latency that analyzed the block interval and block size for computing the latency. The proposed approach is validated against

experimental and analytical results by identifying various bottlenecks in performance measurement. Zhao et al. [32] have proposed a privacy preserving data integrity model using bilinear pairing, cryptosystem and blockchain mechanism that ensured the data privacy and security to the IoT systems. The simulated results validated the efficiency of proposed scheme. Li et al. [33] have proposed public auditing method using blockchain mechanisms in which the author's have generated a Merkle Hash Tree to improve the integrity and computation overhead reduction using lightweight verification method. The proposed approach is experimented that defend approximate 51% threats with improved communication and computation process. Further, Esposito et al. [34] have proposed distributed identity management policy where the author's have used blockchain scheme that improved the integrity and security policies in a global view The proposed scheme is validated against various existing schemes. Hardin et al. [35] have proposed an Amanuensis trusted and blockchain enabled system for mhealth where the proposed scheme improved the trust using shared verification and accessing policy method while storing the data. The proposed approach is validated and trusted over mhealth data having dollar 0.07 per data source per day. Furthermore, Hu et al. [36] have proposed data slicing scheme in which the authors have used over 10,000 smart contract and LSTM data to test and train the datasets. The proposed approach is simulated over various contractual approaches by detecting the f1-score and precision metrics.

2.2. Related work

IoT is the essential technology to provide intercommunication between different objects, since it addresses various critical issues. Several studies have been conducted on the usage of blockchain within different applications of IoT [37, 38, 39, 40]. In this section, the detailed discussion of the blockchain use cases and role of blockchain in IIoT has been illustrated. For improving the suppliers experience and efficiency, the IIoT is revolutionizing industries for suppliers, manufacturers and retailers. In order to build confidence among customers and establish the trust between various entities, reputation mechanism plays

a significant role. Liu et al. [41], have proposed a reputation based approach in retailer-consumer channel by accumulating the reputations from consumers' feedback. Further, to isolate the feedback posts by consumers, the authors have proposed an anonymous system which preserves identity and feedback of the individuals. Further, in order to increase the reliability and reputation, the authors have exploited the consensus and distributed tamper proof nature of blockchain mechanism. The efficiency of the proposed mechanism is enhanced by designing proof of stakes and cryptographic mechanisms as compared to traditional approaches. Further, the authors have highlighted the challenges of implementing proof of stake and blockchain architecture using Ethereum. Finally, the approach is demonstrated against off/on scalability performance to check the feasibility of method. Industrial IoT came into existence to improve scalability, security and transparency between individuals. Though, existing industrial IoT mechanisms are still vulnerable to several security threats, the above discussed issues can be easily resolved using blockchain mechanism that ensures a secure communication about each and every activity of industries. Huang et al. [42]have pointed the low throughput and less power intensive nature of blockchain that is not suitable for high power IoT nodes. The authors in this paper have proposed a credit based censuses system for industrial IoT that ensures the efficiency and security during transaction for IoT devices. Further, to preserve data confidentiality, the authors have designed authority management for regulating the accessed data from sensors. The performance of the proposed mechanism is enhanced by using directed acyclic structured graphs that are implemented through Raspberry Pi. The proposed mechanism results are simulated and demonstrated with an efficient and secure data access control. Liu et al. [43] have raised the issue of computing difference between blockchain network and data processing servers. The processing difference during offloading computation is a major issue in blockchain networks. The authors have proposed a multi-hop distributed and cooperative offloading algorithm which considers both mining tasks and processing tasks to minimize the economic cost.

Further, the authors have formulated the offloading issue as a potential game where devices make autonomous decisions by proving the existence of ash equilibrium. Finally, they have proposed a distributed algorithm for message exchange for reducing the computational complexity. The authors' approach is validated through experimental results over minimum cost upon increasing the number of IoT devices as compare to existing schemes. In order to modernize the industrial sector using various new technologies such as big data and robotics, blockchain has stood apart as a technique that ensures the security, trust and decentralization in various industrial sectors. Carames et al. [44] have focused on analyzing the challenges and benefits of using blockhain mechanism and smart consensus to develop industrial IoT use cases. The authors have presented a review on various blockchain mechanisms for industrial sectors by providing detailed guidelines for future developers. Finally, the authors have determined how blockchain based approaches may enhance the cyber security applications in industrial sectors. Khan et al.[45], Li et al. [46] and Guan et al. [47] have proposed number of blockchain based security mechanisms using various cryptograhic, energy trading and encryption mechanism to further ensure the secure in IIoT environments.

Blockchain technology has been raised to provide an optimized system performance by ensuring a flexible, secure and scalable communication environment. Business process management involves various performance concerns to improve the business growth. Viriyasitavat et al. [48], the authors have demonstrated the emerging research fields, promising use cases and challenges by integrating the blockchain technique with business process management. Further, Mohamed et al. [49] have proposed a middle ware scheme for utilizing the blockchain capabilities and services to enable trust, security, autonomy and traceability in smart manufacturing use cases. The proposed approach has offered various advantages to establish security using trust among communicating entities during product manufacturing and shipping processes. Further, the authors have realized that the proposed mechanism may enable a promising new technique for establishing the security and benefits for smart manufacturing.

Karamacoski et al. [50], have proposed a novel mechanism of communication through named distributed channel that shows a transaction between two or more entities during data exchange through multiple physical channels. Further, the authors have proposed an enhanced security development through blockchain mechanism. The blockchain technique is used to bypass the transformation matrix and encryption keys exchange between sender and receiver. The entire process used the spatial spreading approach to transfer the information between independent channels. Further, the proposed mechanism is more secure and reliable than basic approach through distributed storage algorithms.

To date, existing works have projected various applications of blockchain mechanism. However, very few of them have described the concept of blockchain mechanism in industries. The goal of this paper is to describe a framework of blockchain industrial IoT by evaluating the results in respect of message alteration, Dos and DDoS attacks, and authentication delay.

3. Proposed Framework

Figure 2 represents the traditional documentation, product shipping, location tracing for workers and tracing schemes for products in IIoT.

As depicted in the Figure 2, the individual managers or some trusted authority or party is appointed for recording the independent actions such as delivery of supplies and raw materials, product manufactures, shipment and documentation record, product supplier's information and products receivers' or customer record. Even though, the actions are captured through devices, however, it is very difficult to trace each activity. Some of the devices may be hacked by a number of attackers where it becomes very complicated to detect the fault. Although, the fault may come under consideration after some time, however, till then the attackers would have fulfilled their intent.

3.1. System Model

This section discussed the system model of the proposed framework. The hypothetical situation as depicted in Figure 3 consists of a company whose head-

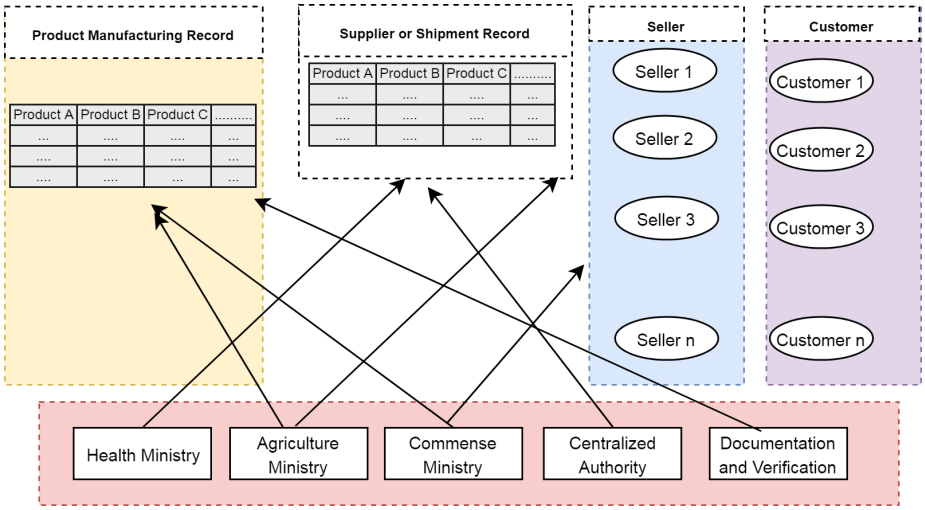

Figure 2: Traditional method of data manufacturing and handling

quarters are located in a country 'A' and the raw material supplying units and factories are situated in a country 'B'. Further, their corresponding consumer stores can be assumed to be located at various places across the world keeping in mind the international business associated with the firm. In the proposed frame work, the blockchain is implemented as level wise. In order to reduce the blockchain size, storage and complexity of validating or verifying the real time data, each level is separated with a distinct blockchain that further the implementation and efficiency of the system.

Now, in order to keep track of every activity of all the entities, headquarters and different branches of the company have used blockchain technology. As depicted in Figure 3, the initial implementation of blockchain is started by the headquarter which has all the rights to look over each and every activity of different branches of their company. Further, the suppliers, factories and stores have independent blockchain in order to trace each and every activity within and among the entities. The below text describes the working of the blockchain by dividing it into certain levels.

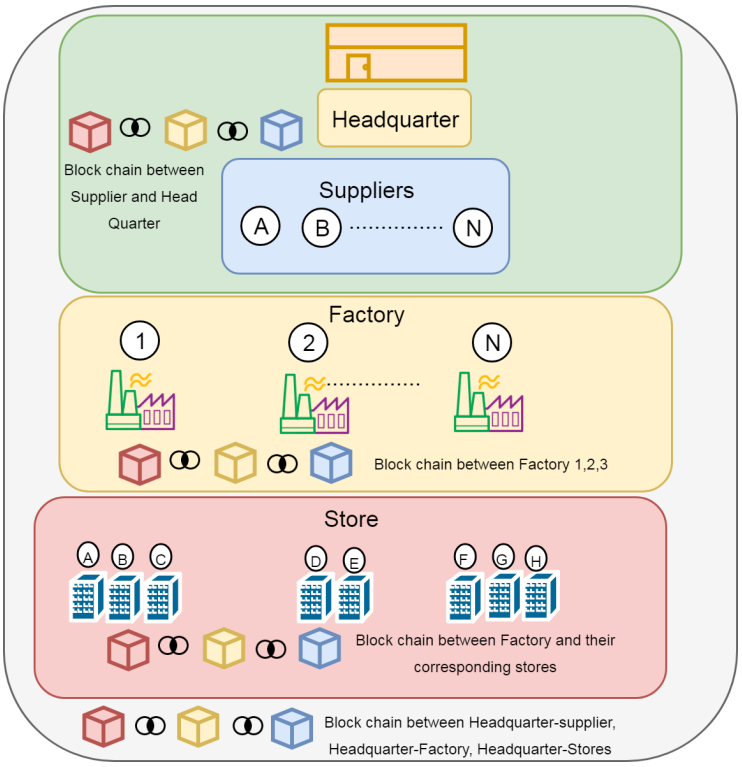

Figure 3: System model of the proposed framework

3.2. Working of proposed framework

In order to understand and organize the management systems, the Blockchain shall be implemented in three different levels. Headquarter and suppliers contribute to become a single blockchain at Level 1 while headquarter, supplier and factory may combine to form another blockchain. Further, level 3 includes the blockchain among the factories, stores and the headquarters. The depicted Figure 4 presents all the three levels of the blockchain architecture.

1. **Level 1:** In case one, a blockchain is setup between the Headquarters and the unprocessed material suppliers whenever an order is placed by the former. Upon receiving the request, the suppliers ship the stuff to the factories in accordance with the number of finished products required and a notification is sent to the headquarters. For transparency, the orders of

all the suppliers are stored on the same system and are viewable by all. The depicted figure 4 represents the level 1 blockchain where headquarters located in country 'A' start implementing the blockchain and add all the suppliers' entries in that chain.

2. **Level 2:** In case 2, the extended blockchain is setup at another level between the headquarters, suppliers and factories as depicted in Figure 5. When goods are supplied to the factories, a notification by each one of them is automatically sent to the headquarters such as supplier sent notification 'a' to the headquarter as the acceptance and departure of the material to the corresponding factories. Further, factories 1, 2 and 3 sent the notification 'b' to the headquarter upon receiving the raw materials. The factories manufacture products according to the orders and the no. of products are reflected on the blockchain.
3. **Level 3:** In case 3, the blockchain also includes the stores to which the factories are liable for supplying finished goods. Whenever the products are delivered to the stores, the headquarters are notified as depicted in Figure 4, all the stores will send notification 'c' upon receiving of products from their corresponding factories. Further, the count of products delivered by each factory is seen on the network.

Now, how the blockchain addresses the various associates is explained as follows. Suppose, we have 4 different entities as depicted in Figure 4 which are headquarters, known as the first entity that initiates and looks over the entire associates, suppliers R1 and R2 denote the second entity which supply the raw materials to the corresponding factories upon receiving the order from the headquarters.

Further, third entity are the factories 1, 2 and 3 that accept raw materials, produce the products and deliver them to the corresponding stores while the fourth entity are the stores that receive the products and ship to corresponding receivers. The tabular representation of the blockchain with the entries that occurred at each level of the firm is presented in figure 6. Let us take an example

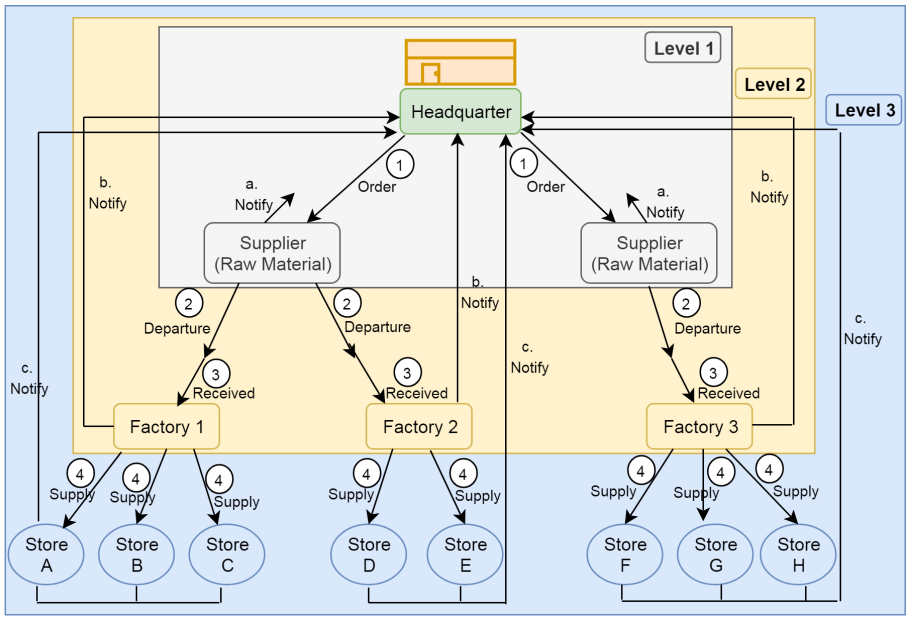

Figure 4: The process of the Blockchain-based architecture in the three different levels

where the headquarters place an order with the suppliers for raw provisions for manufacture of 10 smart phones. Immediately a blockchain is set up between the Headquarters and suppliers R1 and R2. Now, suppose that factory 1 has to manufacture 6 smart phones and supply them to Stores P, Q and R with three for each. Factory 2 has to manufacture and ship four products to store 3. The chances of cheating are very low as all the data associated with a particular factory is visible on the blockchain and the stores directly send a notification to the Headquarter as delivery is done according to their consumer demands.

1. Initially, the headquarter 'HQ' that initiates the blockchain will initiate the transaction of first chain H-R1 and H-R2 with a hash by broadcasting the request to available ledgers. headquarter will contain the details of all associates' entries such as suppliers, factories and corresponding stores.
2. In the second step, the suppliers R1 and R2 will accept 'HQ' request and add another blockchain into the existing one with its current and previous

hash. As depicted in Figure 5 suppliers R1 and R2 include factories into their blockchain where in order to maintain the transparency; both the suppliers are able to see their material entries ordered by the HQ.

3. In the third step, factories will include their corresponding stores by appending another block with new and previous hash. As depicted in Figure 6, the blockchain includes all the factories and stores where factories are able to see each other's details.
4. Further, the stores P,Q,R will receive the products from their corresponding factories with a current hash and previous hash function where the final blockchain will finish. Here, all the stores will able to see each other's details and their corresponding factories' details.

While implementing the blockchain certain restrictions have been assumed to achieve higher efficiency. In level 2 (Headquarter-Supplier-Factory), whenever the manufactured products are shipped by the factories, headquarter is free to put restriction on the data visibility for raw material suppliers regarding the no. of products shipped to the stores by the factories. Also, in level 3 (Headquarter-factories-stores) the restrictions shall be put on the factories regarding the visibility of delivered products on the blockchain so that a direct seller and headquarter connection is setup and any middleman attack can be avoided. Further, the illegal activities of the workers operating at a particular location or the shipping of products from the stores to the corresponding receivers may involve the blockchain. The text below considers both the cases and elaborates them briefly. Further, algorithms 1,2,3 and 4 presents the pseudo code of proposed blockchain mechanism.

3.3. Traceability of the illegal activities by the workers at different places

In order to manage the illegal actions of company's workers, blockchain plays a vital role. Even if all the actions including data entry, product shipping or any other significant documentation are handled and stored by IoT devices, a company worker or even any higher authority person may steal significant

Algorithm 1 Blockchain Creation

Input: current hash ($Hash_{current}$), previous block hash ($Hash_{previous}$), timestamp (t) and data (d)
Output: The blockchain is validated successfully or not
Create Blockchain
Blockchain1()
Blockchain2()
Blockchain3()
Blockchain
Compute hash() of each block 'B'
Generate hash value for a block SHA-256
Initialize getters and setters of each block 'B'
Create an array list Li to maintain chain.
Create first block() known as genesis by passing parameters
Genesis Block=data + $Hash_{current}$
New block=genesis block $Hash_{previous}$+ data+ $Hash_{current}$

Algorithm 2 Blockchain Validation

Input: A network 'n' consist of 'd' number of IoT devices
Output: The IoT devices are either legitimate or malicious
Step: Create a getLatestBlock() // validate the newly added block
Alter $Hash_{previous}$ of a block 'B'
Create validate method() // validate hash value of block
if (Bi($Hash_{previous}$)==Bj($Hash_{previous}$) **then**
    Block valid
else
    Block Invalid
end if

Algorithm 3 Data Validation

Input: A network 'n' consist of 'd' number of IoT devices

Output: The IoT devices are either legitimate or malicious

Step: Alter the data of any block 'B'

Miner nodes will verify the block 'B'

if (Bi(blockdata$_i$(Hash$_{previous}$))== blockdata$_j$(Hash$_{previous}$) **then**

    Data valid

else

    Data invalid

end if

Algorithm 4 Blockchain1(), 2() and 3()

Input: A network 'n' consist of 'd' number of IoT devices

Output: The IoT devices are either legitimate or malicious

Step: Blockchain 1() //maintained among headquarters and supplier's'

headquarter will keep track of supplier Si_{data}

Blockchain 2() //maintained among headquarters, suppliers and factory

headquarter will keep the record of supplier Si_{data} + factory (shipping and manufacturing)

Blockchain 3() //maintained among headquarters, suppliers, factory and stores

headquarter will keep record of supplier Si_{data} + factory (shipping and manufacturing)+ $store_{record}$

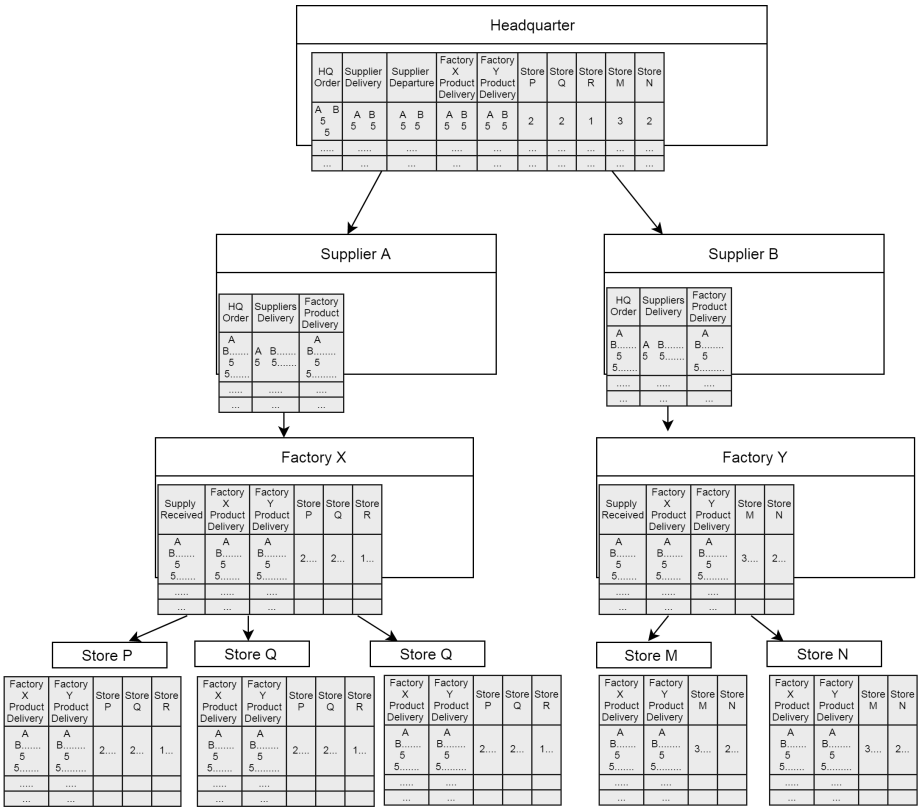

Figure 5: Blockchain at each entity

documents, products or enter into restricted areas by hacking the devices. The malevolent actions of these devices may be unrecognizable where benefiters may harm the economical growth of the company. If each and every action/activity of the company is stored by smart devices associated with a blockchain then it becomes very critical for the attackers to apply illegal actions. Further, it would be very easy for the owners to look over each and every activity of their entities efficiently from a single place.

3.4. When a store ships a product

Traditionally, if an individual 'A' desires to deliver any product to an individual 'B' let's say from X to Y, then, this practice is typically done by using any trusted third authority. However, this process occurs to addition of some cost, needs some time and threats the privacy of the end users 'A' and 'B'. However, with blockchain techniques, all these concerns can be easily resolved. Now, how the blockchain addresses the product shipment is described as follows. Let's say we have a network of 4 entities that actually desire to move the product from one place to another place. 'A' is considered as sender or product provider while 'B' is the dealer liable to accept the delivery order. However, person 'C' is liable for managing the product delivery consignments among the sender and the receiver and 'D' is the final receiver that recognize the product.

1. Initially, the sender 'A' that commences the product shipment practice will be going to insert a transaction of first chain A leads to B with a hash and transmit the request messages to accessible dealers.
2. Further, the dealer i.e. 'B' will consider the request of 'A' and add another block into the present chain with its new and previous hash.
3. The third person that is 'C' will validate the acceptance of both 'A' and 'B' and insert a new block as handler with its new hash and previous hash.
4. Further, the dealer 'B' will relocate the product to the person 'D' i.e. receiver with a new and previous hash function where the final blockchain will finish.
5. Blockchain is a chain of product transactions which public to others that leads all the blockchain entities have entire copy of the chain. It offers transparency between the devices where everyone in the network is capable to trace, how much time and where the product is to take further to be shipped.

3.5. Synchronization among the nodes

Here, we understand how the users or nodes synchronize their transactions or ledgers. Let us suppose there are 'A' number of organizations , 'B' number of

dealers, ‘C’ number of handlers ’D’ number receivers. Now if ‘B’ desires to place some product to ‘D’ then initially dealer ‘B’ will broadcast and publicize the intended transaction request in the network. Everyone present in the network will quickly check that ‘B’ desires to ship a product x to receiver ‘D’ and is considered as a valid transaction till now. Therefore, to get this deal into the existing blockchain, the network need ‘miner’. Here, ’C’ is considered as Miner, it is a significant authenticating device that has the capability to stop the ledger. These miner nodes are liable to do following major tasks in the network.

Miner node are liable to contend among each other to become first one to take the every new transaction by analyzing, verifying and putting it into the ledger. The first node that will do may get a financial reward. Validation or verification refers to the cross checking of new transaction.

Furthermore, it is also the responsibility of the miner node to search the special key equivalent to the generated hash that will facilitate with the previous transactions by locking the new transaction with the old one and publish it further to the entire network.

4. Performance Analysis

have proposed a secure blockchain mechanism for IIoT that not only provides valid management of product manufacturing and shipping records but also ensure transparency among different entities. Table 1 depicts IIoT milieu of 500m $\times$ 500m having several number of nodes. We have generated a local blockchain network where all the devices are communicated among each other in a same system. The size of each block is 5000 bytes having previous hash, data size and current hash. We have created 10 blocks using SHA256 hash where the generation time of each block is nearly 3 seconds [51]. Further, along with blockchain creation and validation, the proposed phenomenon is inspected over various malevolent nodes.

The blockchain creation, validation and insertion process is done through java while the validity and security against malevolent nodes are verified through

Table 1: Simulation environment of smart E-voting

Parameters	**Values**
Simulation time	60s
Grid Area	500m × 500m
Number of nodes	200
Range of transmission	120m (approx)
Size of data	256 bytes
Physical layer	PHY 802.11

MATLAB. Initially, fifty nodes are created that operates as IoT devices. In addition, a synthesized data is generated to provide normal pattern distribution where the proposed mechanism is validated against several security threats such as authentication mechanism, denial of service (DoS) and distributed denial of service (DDoS) attacks and message alteration. The authentication parameters are used to verify or validate the legitimacy of communicating nodes. It validates whether the communicating device is the one that it claims to be or not. Further, DoS attack is the one that interrupts or slows down the communication process in the network. Moreover, message alteration validates how proposed phenomenon behaves in case of altering or changing the communicated or stored data in the network. To analyze the authenticity of the proposed scheme, 10% of legitimate nodes are altered to malicious. Initially, the proposed phenomenon presents the creation, validation and insertion of blocks in de-centralized environment. Further, the scheme is analyzed against various security measures over existing method.

Figure 6 presents the creation of blockchain where numbers of blocks are created along with their previous and current hashes. The depicted Figure 6 shows the valid creation of blockchain where each block is verified and validated by miner nodes. Similarly, Figure 7 depicts data insertion process where numbers of entities are adding various records in the blockchain. In this Figure 7, we have inserted a single unit data (such as product manufacturing) to analyze

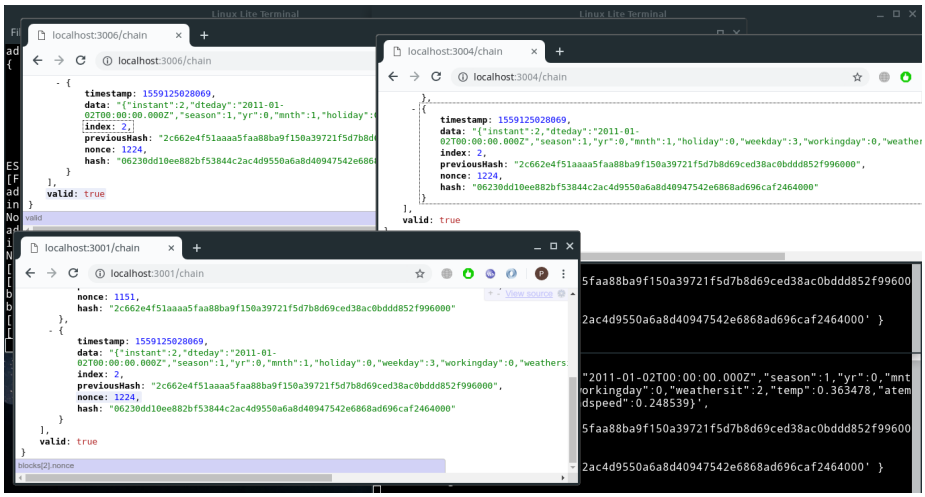

Figure 6: Block creation

it efficiently.

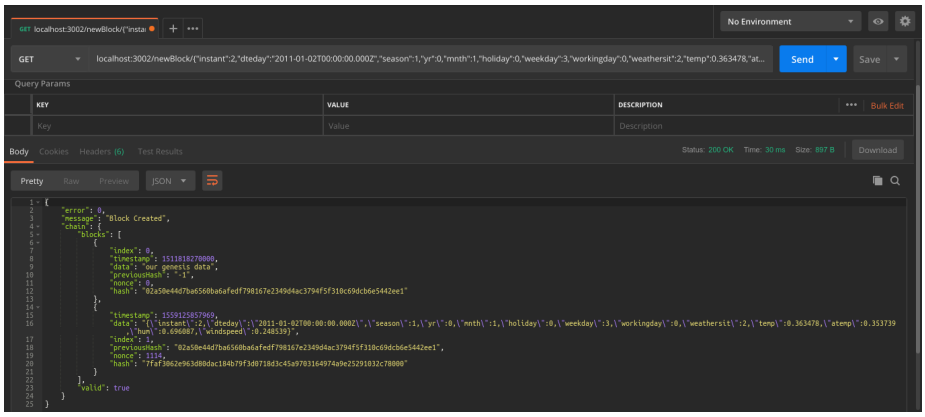

Figure 7: Data insertion

Moreover, Figure 8 presents the validation and verification process where before adding any information into the blockchain, the miners first verify or validate the newly added block. If the miners are successfully able to verify the block then they are considered as valid and stock is successfully added else block

is rejected and not verified by the network. In this mechanism, the blockchain framework is justified by defining proof-of-miners as proposed phenomenon is validating the data insertion and validation against several security concerns. After completing the initial verification and creation of blockchain mechanism, the proposed approach is analyzed over various security concerns such as DoS attack, message alteration and authentication verification. The proposed framework architecture consists of headquarters that are liable for verifying the legitimacy of the nodes and are able to trace each and every activity of their entities presented at different levels.

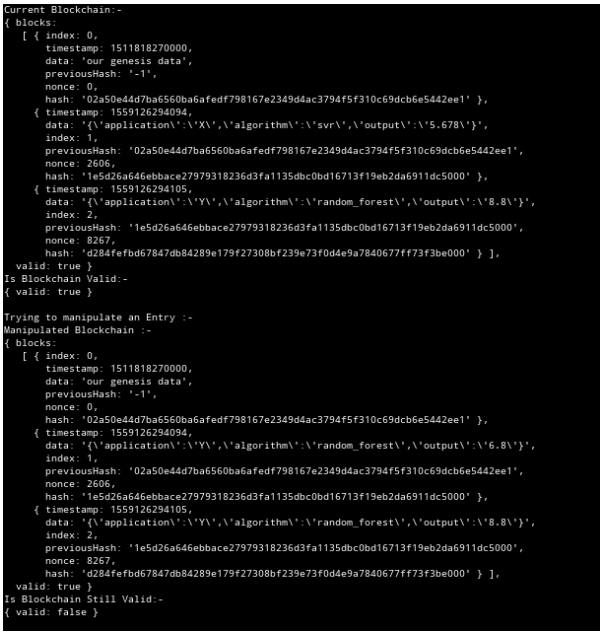

Figure 8: Miners validation

4.1. Evaluation Metrics

1. Authentication Delay (AD): It is defined as the maximum and average amount of time required to validate the participating and communicating nodes. It is the request delay which indicates the difference between time

taken to authenticate and time taken by requesting node.

$$AD = \sum_{i=1}^{N} \frac{Time_{Rqst} - Time_{auth}}{Total\ number\ of\ requesting\ nodes} \tag{1}$$

2. Message Alteration (MA): it is defined as a change in small or large information of data to perform malicious activities in the network.

$$MA = \sum_{i=1}^{N} \frac{Alteration\ of\ hash\ and\ data}{Total\ size\ of\ data} \tag{2}$$

3. Brute force and cryptographic attack: it is defined where attacker tries every possible way to obtain the information or message communication between nodes without any knowledge of key or hash.

4. DoS and DDoS threat: They are defined as the total number of resources utilized by node's during communication.

$$Attack = \sum_{i=1}^{N} \frac{Resource\ utilized\ by\ node}{Total\ number\ of\ resources\ present\ in\ network} \tag{3}$$

4.2. Results and discussion

We have considered several parameters to compare our proposed phenomenon against existing (baseline) method. In traditional mechanism mentioned as ex-

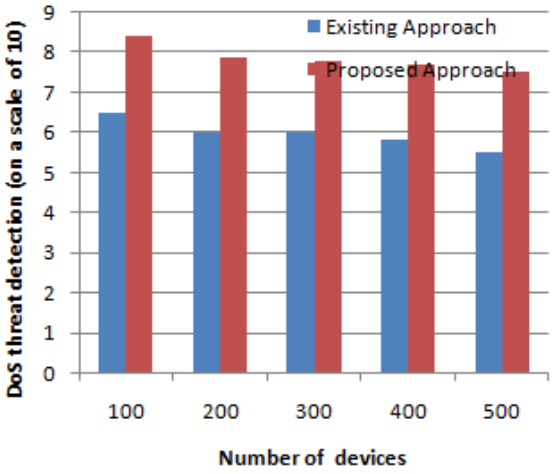

Figure 9: Case of DoS attack

isting (baseline) method, malevolent nodes are measured using some cryptographic mechanisms that include the overall complexities and computational overhead of managing and storing of cryptographic keys. In addition, the management of cryptographic keys may further leads to storage overhead and scalability issues where upon increasing of nodes, the keys needs to be created and distributed to maintain the security. Further, the complexity of proposed mechanism is better as compare to existing mechanism as the additional involvement of cryptographic techniques may lead to increase the computational complexity of the communication mechanism[17]. However, in our proposed phenomenon, message alteration, DoS attack and authentication process performs better as upon identification malicious nodes are immediately removed from the network. In order to measure legitimacy or misbehaviour of nodes, we have analyzed the traceability and permission of data access through blockchain mechanism. All the mentioned simulation results suggest that the proposed solution leads to 94% efficiency in terms of DoS and DDoS threat, message alteration attack and authentication delay. Figure 9 and 10 illustrates the DoS and DDoS threats that are specific to blockchain framework. In depicted Figure 9, proposed mechanism performs better because of blockchain mechanism where a node performing any malicious behaviour or activity can be identified and eliminated immediately from the communicating environment.

Similarly, Figure 10 represents DDoS attack where the permission and distributed nature of blockchain mechanism ensures security against message alteration such as election administrator is liable to allow accessing and permission to remaining levels and is able to trace and look over every individual's malicious activity done by any entities. However, in comparison of existing method, it becomes very difficult to detect, trace and prevent any malicious activity at such an early stage. Further, the distributed and permissioned environment reduces the overload on remaining number of levels to store and manage huge database of information.

Figure 11 represents message alteration attack where attackers try to alter or access information communicating in the network. Now, in this case, proposed

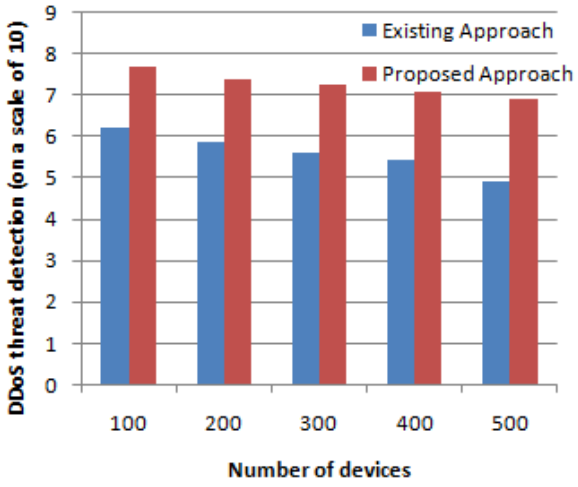

Figure 10: Case of DDoS attack

mechanism performs better because election administrator has the permission to look over the entire environment and allows the remaining levels to access the information.

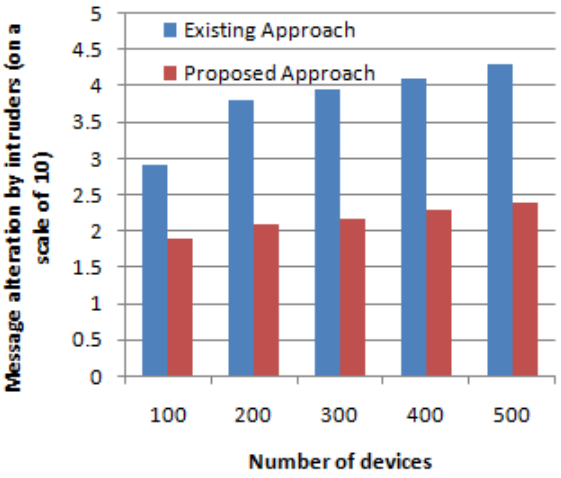

Figure 11: Case of messages alteration attack

525 Finally, Figure 12 presents authentication delay of existing and proposed IIoT mechanism over several numbers of devices. The proposed phenomenon

outperforms against existing scheme because of its permission environment. The headquarter have all the rights to trace and access activity of every individual entity. However, the accessing restrictions are increased with the increasing level to further overcome the storage and communication overhead.

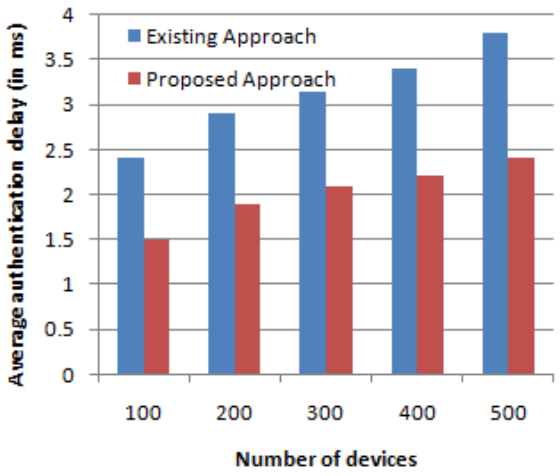

Figure 12: Authentication delay

Though proposed mechanism is efficiently able to ensure the security in the network, however, sometimes it may critical for the miners to validate the data or information (block) where number of blocks are requested to be added at the same time in the network.

5. Conclusion

The paper have proposed a secure Blockchain technique in the context of IIoT. The proposed mechanism use IoT devices to control the entire industry's task automatically such as data collection, analysis, distribution of products and traceability of workers' location. The proposed mechanism detects various security threats in order to reduce production cost. Further, Blockchain technology is used to trace each and every activity of industries that ensures the protection and secrecy of control system in real time scenarios. The Blockchain

technology stores the previous information of records including workers' location. The proposed phenomenon is validated through blockchain creation, data validation and miner's validation. Further, the proposed framework significantly performs better in terms of authentication delay, message alteration, DoS and DDoS attack.

On the other hand, the storage of user's data over cloud may incorporate a number of security risks including: man-in-middle attack, data falsification threat, cost overhead which we will be targeting in the future work. In addition, the user may protect its data by buying its private cloud. However, this further increase the costs-related issues for the user or the organization that are also among the remaining open challenges to be addressed.

References

[1] W. M. Halton, S. Rahman, The Top Ten Cloud-Security Practices in Next-Generation Networking, Intern Journal of Communication Networks and-Distributed Systems 8 (1) (2012) 70.

[2] Z. L. Berge, L. Muilenburg, Seamless Learning: An International Perspective on Next-Generation technology-enhanced learning, in: Handbook of mobile learning, Routledge, 2013, pp. 133–146.

[3] P. Lombardi, S. Giordano, H. Farouh, W. Yousef, Modelling the Smart City Performance, Innovation: The European Journal of Social Science Research 25 (2) (2012) 137–149.

[4] O. Bouachir, M. Aloqaily, L. Tesng, A. Boukerche, Blockchain and fog computing for cyber-physical systems: Case of smart industry, arXiv preprint arXiv:2005.12834.

[5] F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, A. Adnane, E. Barka, Blockchain in Internet-of-Things: Architecture, Applications and Research Directions, in: International Conference on Computer and Information

Sciences (ICCIS), IEEE, 2019, pp. 1–6. doi:10.1109/ICCISci.2019.8716450.

[6] F. S. Ali, M. Aloqaily, O. Alfandi, O. Ozkasap, Cyberphysical blockchain-enabled peer-to-peer energy trading, Computer 53 (9) (2020) 56–65.

[7] G. Rathee, F. Ahmad, R. Iqbal, M. Mukherjee, Cognitive automation for smart decision making in industrial internet of things, IEEE Transactions on Industrial Informatics (2020) 1–1Early Access, doi:10.1109/TII.2020.3013618.

[8] G. Rathee, A. Sharma, R. Kumar, R. Iqbal, A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology, Ad Hoc Networks (2019) 101933.

[9] J. Wan, J. Li, M. Imran, D. Li, A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3652–3660, doi:10.1109/TII.2019.2894573.

[10] I. Lee, K. Lee, The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises, Business Horizons 58 (4) (2015) 431–440.

[11] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and Other Botnets, Computer 50 (7) (2017) 80–84.

[12] G. Perboli, S. Musso, M. Rosano, Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases, IEEE Access 6 (2018) 62018–62028. doi:10.1109/ACCESS.2018.2875782.

[13] F. Ahmad, A. Adnane, F. Kurugollu, R. Hussain, A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks, in: 11th IEEE Wireless Days (WD), 2019, pp. 1–8.

[14] H. Wu, C. Tsai, Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy

in Data Sharing, IEEE Consumer Electronics Magazine 7 (4) (2018) 65–71. doi:10.1109/MCE.2018.2816306.

[15] G. Rathee, F. Ahmad, C. A. Kerrache, M. A. Azad, A Trust Framework to Detect Malicious Nodes in Cognitive Radio Networks, Electronics 8 (11) (2019) 1–19.

[16] F. Al-Turjman, S. Alturjman, Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2736–2744.

[17] A. Karati, S. H. Islam, M. Karuppiah, Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3701–3711.

[18] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, M. Guizani, The Rise of Ransomware and Emerging Security Challenges in the Internet of Things, Computer Networks 129 (2017) 444–458.

[19] Y. Liu, H.-H. Chen, L. Wang, Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges, IEEE Communications Surveys & Tutorials 19 (1) (2016) 347–376.

[20] C. Sankaran, Network Access Security in Next-Generation 3GPP Systems: A Tutorial, IEEE Communications Magazine 47 (2) (2009) 84–91.

[21] W. Khan, M. Rehman, H. Zangoti, M. Afzal, N. Armi, K. Salah, Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges, Computers & Electrical Engineering 81 (2020) 106522.

[22] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Business & Information Systems Engineering 59 (3) (2017) 183–187.

[23] M. A. Khan, K. Salah, IoT Security: Review, Blockchain solutions, and Open Challenges, Future Generation Computer Systems 82 (2018) 395–411.

[24] R. Krishnamurthy, G. Rathee, N. Jaglan, An Enhanced Security Mechanism Through Blockchain for E-Polling/Counting Process using IoT Devices, Wireless Networks (2019) 1–12.

[25] P. K. Sharma, J. H. Park, Blockchain based Hybrid Network Architecture for the Smart City, Future Generation Computer Systems 86 (2018) 650–655.

[26] H. Baniata, A. Anaqreh, A. Kertesz, Pf-bts: A privacy-aware fog-enhanced blockchain-assisted task scheduling, Information Processing & Management 58 (1) (2021) 102393.

[27] Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, I. Al Ridhawi, An incentive-aware blockchain-based solution for internet of fake media things, Information Processing & Management 57 (6) (2020) 102370.

[28] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A survey on blockchain for information systems management and security, Information Processing & Management 58 (1) (2012) 102397.

[29] B. Putz, M. Dietz, P. Empl, G. Pernul, Ethertwin: Blockchain-based secure digital twin information management, Information Processing & Management 58 (1) 102425.

[30] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, S. Jha, B-ferl: Blockchain based framework for securing smart vehicles, Information Processing & Management 58 (1) (2020) 102426.

[31] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, A. V. Vasilakos, Latency performance modeling and analysis for hyperledger fabric blockchain network, Information Processing & Management 58 (1) 102436.

[32] Q. Zhao, S. Chen, Z. Liu, T. Baker, Y. Zhang, Blockchain-based privacy-preserving remote data integrity checking scheme for iot information systems, Information Processing & Management 57 (6) (2020) 102355.

[33] J. Li, J. Wu, G. Jiang, T. Srikanthan, Blockchain-based public auditing for big data in cloud storage, Information Processing & Management 57 (6) (2020) 102382.

[34] C. Esposito, M. Ficco, B. B. Gupta, Blockchain-based authentication and authorization for smart city applications, Information Processing & Management 58 (2) 102468.

[35] T. Hardin, D. Kotz, Amanuensis: Information provenance for health-data systems, Information Processing & Management 58 (2) (2020) 102460.

[36] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, Y. Liu, Transaction-based classification and detection approach for ethereum smart contract, Information Processing & Management 58 (2) 102462.

[37] A. Rabbachin, T. Q. Quek, H. Shin, M. Z. Win, Cognitive Network Interference, IEEE Journal on Selected Areas in Communications 29 (2) (2011) 480–493.

[38] D. Hlavacek, J. M. Chang, A Layered Approach to Cognitive Radio Network Security: A Survey, Computer Networks 75 (2014) 414–436.

[39] F. Ahmad, C. A. Kerrache, F. Kurugollu, R. Hussain, Realization of Blockchain in Named Data Networking-Based Internet-of-Vehicles, IT Professional 21 (4) (2019) 41–47.

[40] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, A. Nallanathan, On the Security of Cognitive Radio Networks, IEEE Transactions on Vehicular Technology 64 (8) (2014) 3790–3795.

[41] D. Liu, A. Alahmadi, J. Ni, X. Lin, X. Shen, Anonymous Reputation System for IIoT-Enabled Retail Marketing a Top Pos Blockchain, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3527–3537.

[42] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards Secure Industrial IoT: Blockchain System with Credit-based Consensus Mechanism, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3680–3689.

[43] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, Y. Zhang, Cooperative and Distributed Computation Offloading for Blockchain-Empowered Industrial Internet of Things, IEEE Internet of Things Journal 6 (5) (2019) 8433–8446.

[44] T. M. Fernández-Caramés, P. Fraga-Lamas, A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories, IEEE Access 7 (2019) 45201–45218.

[45] P. W. Khan, Y. Byun, A blockchain-based secure image encryption scheme for the industrial internet of things, Entropy 22 (2) (2020) 175.

[46] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, IEEE transactions on industrial informatics 14 (8) (2017) 3690–3700.

[47] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, M. Guizani, Towards secure and efficient energy trading in iiot-enabled energy internet: A blockchain approach, Future Generation Computer Systems 110 (2020) 686–695.

[48] W. Viriyasitavat, L. Da Xu, Z. Bi, V. Pungpapong, Blockchain and Internet of Things for Modern Business Process in Digital Economy—the State of the Art, IEEE Transactions on Computational Social Systems 6 (6) (2019) 1420–1432.

[49] N. Mohamed, J. Al-Jaroodi, Applying Blockchain in Industry 4.0 Applications, in: IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2019, pp. 0852–0858.

[50] J. Karamačoski, N. Paunkoska, N. Marina, M. Punčeva, Blockchain for Reliable and Secure Distributed Communication Channel, in: 2019 IEEE

International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), IEEE, 2019, pp. 91–97.

[51] E. Barka, C. A. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, F. Kurugollu, Towards a Trusted Unmanned Aerial System using Blockchain for the Protection of Critical Infrastructure, Transactions on Emerging Telecommunications Technologies (2019) e3706Doi:10.1002/ett.3706.