This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2022.3182121

A Secure and Trusted Mechanism for Industrial IoT Network using Blockchain

Geetanjali Rathee, Farhan Ahmad, Naveen Jaglan, and Charalambos Konstantinou, *Senior Member, IEEE*

Abstract— Industrial Internet-of-Things (IIoT) is a powerful IoT application which remodels the growth of industries by ensuring transparent communication among various entities such as hubs, manufacturing places and packaging units. Introducing data science techniques within the IIoT improves the ability to analyze the collected data in a more efficient manner, which current IIoT architectures lack due to their distributed nature. From a security perspective, network anomalies/attackers pose high security risk in IIoT. In this paper, we have addressed this problem, where a coordinator IoT device is elected to compute the trust of IoT devices to prevent the malicious devices to be part of network. Further, the transparency of the data is ensured by integrating a blockchain-based data model. The performance of the proposed framework is validated extensively and rigorously via MATLAB against various security metrics such as attack strength, message alteration, and probability of false authentication. The simulation results suggest that the proposed solution increases IIoT network security by efficiently detecting malicious attacks in the network.

Keywords—Industrial Internet-of-Things (IIoT), Blockchain, Security, Secure IoT Devices, Trust Management.

1 Introduction

Today the performance and productivity of an organization entirely depends on the way it analyses and collects its business data. The onset of smart systems along with various other developments in the field of data science continue to provide new frontiers for the expansion of this technology. According to the recent statistics, the number of devices with online connectivity stand at 6 billion which collectively generate approximately 2.5 Quintilian bytes of data [1].

In conventional scenarios, collecting and analysing static data from devices in real-time was inefficient. Today, these devices communicate with each other, thanks to the novel Internet-of-Things (IoT) paradigm, resulting in generation of information without any human intervention [2]. Further, intelligent and smart objects/sensors working mutually are steadily becoming more expansive and venture to accomplish users' demands. In order to extract and address meaningful information from the data, a new field, namely, data science that uses scientific approaches, algorithms, procedures and systems for analysis and collection of huge data has been proposed recently. Data science in IoT (DS-IoT) is a technique that improves the online collection and analysis of information in a more scientific, realistic and efficient way [3]. DS-IoT integrates a diverse range of smart devices with commercial objects that export manufacturing information through sensors worn in the field of medicine, cyber physical systems and transportation and to retain the records [4].

Nowadays, DS-IoT is considered as an important technique within industries to increases their growth, effectiveness and overall efficiency [5], [6]. Further, a wide range of IoT-based applications such as smart cities, e-healthcare, intelligent transportation and Industrial IoT (IIoT) have been pioneer to aid intelligent verdict making by concerning a series of physical objects vital to the experimental escalation in an efficient and effective manner [7]. Amongst a variety of use cases offered by IoT technology, IIoT is considered as an important application of IoT that controls and traces every activity of the industry for its growth [8]. IIoT refers to the network where data is collected from numerous sensors, actuators, and machines within an industrial environment and is accessed through the Internet [9], [10].

1.1 Motivation

Despite of various advantages DS-IoT technique offers, organizations are still reluctant to use IoT devices due to several security concerns [11]. From the security perspective, a malicious device within the industry premises can degrade the network performance by limiting the legitimate IoT devices from sharing trusted and true information or alter the communication data. Even though a few open-source ciphers are still liable to bugs and exploits, they are persistently scrutinised by numerous users and turn less effective to malevolent modifications from centralised entities or third parties [12]. In conventional industrial applications, all the smart devices are often assumed to be cooperative and trusted. However, in practice and reality, IoT devices are prone to mischievous activities of the malicious devices (MD). Thus, the potential challenge is to distinguish the ideal

- *(Corresponding Authors: Geetanjali Rathee and Farhan Ahmad)*
- *G. Rathee is with the Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi, India. (e-mail: geetanjali.rathee123@gmail.com)*
- *F. Ahmad is with the Systems Security Group, Centre for Future Transport and Cities, Coventry University, Warwickshire CV1 5FB, United Kingdom (e-mail: ad5899@coventry.ac.uk)*
- *N. Jaglan is with the Department of Electronics and Communication Engineering, Jaypee University of Technology, Waknaghat-173234, India. (e-mail: naveenjaglan1@gmail.com)*
- *Charalambos Konstantinou is with the Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia. (e-mail: charalambos.konstantinou@kaust.edu.sa)*

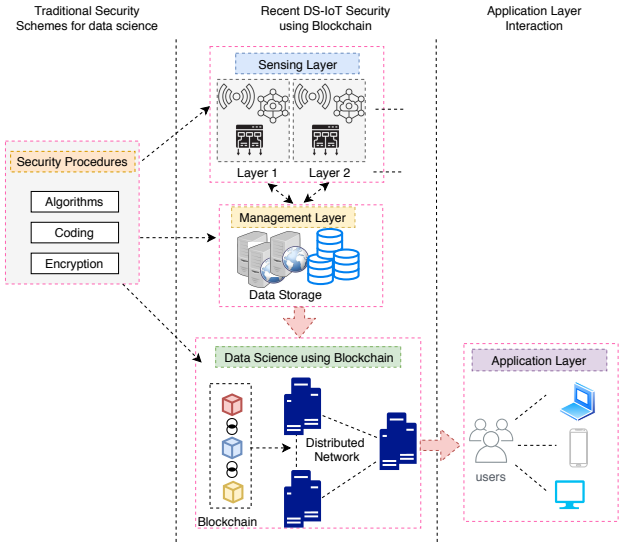


Fig. 1: DS-IoT Blockchain in Industrial IoT

DS-IoT devices from the malicious ones in order to establish a legitimate communication environment [13]. In addition, transparency plays an imperative role in increasing trust and security among the authorities so that any alteration in data can be immediately recognized by the owners [14]. Moreover, to prevent future modifications of data captured by smart devices, recently, blockchain has been proposed, where a network maintains a chain of blocks consisting of the data recorded by the IoT devices in IIoT environment while manufacturing and shipping the products as depicted in Fig. 1.

Blockchain provides an efficient and transparent mechanism for analyzing and controlling the data. Any alteration in the data by any user can be identified via Blockchain. In order for concurrent handling of events for brisk responses and secluded monitoring, the evolution of IIoT generates the possibility of connecting automated systems. Further, data science approaches also ensure effective data gathering and processing mechanisms and techniques for IIoTs. Although DS-IoT in industries has various benefits, many organisations and businesses are still reluctant to use it. The exploitation of this IoT scheme is still steep due to the high cost of allied centralized clouds and servers [15]–[17]. To the best of author's knowledge, the DS-IoT security through blockchain is unexploited for IIoT in the reported literature. IoT devices in the IIoT environment transmit very sensitive information, such as the temperature of the boiler, product manufacturing record, document or product shipping records etc. Therefore, it must be a paramount necessity that security by design is provided to the IIoT network. Further the presence of malicious nodes may have severe impact on the IIoT network as they have the ability to tamper the data generated by IoT devices. Therefore, this leads to the question about how to provide a secure networking paradigm for enabling the devices to share data in an attack-free environment.

1.2 Contributions of the paper

In order to analyze real-time data in IIoT while manufacturing and shipping the products, we have introduced an orchestration of security concerns with the aim to detect and resolve the threats caused by an intruder. To do so, we have computed the trust factor (TF) of all the devices using an elected Coordinator IoT Device (CID). The CID is the controlling unit of IoT environment that is responsible for verifying the legitimacy of the IoT devices present in the network. Further, in order to prevent future alteration of stored information in the local database, a private blockchain is introduced within IIoT environment to keep track of all the recorded information stored in the database. Therefore, the potential contributions of this paper are as follows:

- A novel security orchestration for IIoT using trust to gather and maintain huge amount of data generated by IoT devices has been proposed.
- A mathematical model has been derived to identify the probability of error generated in IIoT by exploiting the concept of probability of false IoT authentication and non-detection.
- A novel data security model using blockchain in IIoT to prevent the intruders from altering the stored information in a local database has been proposed.
- The performance of the proposed framework has been rigorously evaluated against probabilistic hypothetical scenarios for both small and large IIoT networks using a simulation model.

The rest of the paper is structured as follows. Section 2 is dedicated to the related work in IIoT and the use of blockchain in IIoT. Section 3 provides details of our proposed solution using blockchain to secure IIoT networks. Next, Section 4 provides the details of the simulation model and the results. Lastly, Section 5 concludes and directs the prospect of the paper.

2 Related Work

Various studies have been carried out to secure IIoT networks using data science and blockchain. For instance, Yan et al. [18] explored the issues of data processing for industrial big data by proposing novel structural multi source information for heterogeneous environments. This framework is validated by analyzing the heterogeneous data of industries. Even though the authors have discussed the use of smart devices for data driven mechanisms in industries by focusing on storage, processing and utilization schemes, they did not consider the ways through which stored data can be maintained and can further be compromised by various intruders. Further, Wang et al. [19] proposed a novel industrial data processing mechanism to apprehend various industrial functions including distributed access, storage, stream and batch data processing, and real time controlling. Compared to traditional data processing schemes, [19] have illustrated various features of analyzing, correlating and integrating huge amount of data in IIoT. However, the generation of such huge data may further lead to various complexity concerns such as data storage, communication through intermediate nodes and transmission cost. Therefore, secure data transmission through legitimate intermediate nodes is still a lingering question for researchers.

Recently, the most promising technique which adds decentralization, trust, privacy and security to diverse IIoT fields is blockchain. To ensure secure information delivery

via IoT devices, S. Yu et al. [20] proposed a blockchain-based mechanism to transmit the data with minimum cost and economic transfer value. Various techniques such as distributed network architecture, consent algorithm and mapping of intelligent devices were used to identify the decentralized autonomy of smart devices. Furthermore, Y. Yu et al. [21] addressed the issue of security and privacy concerns in IoT objects and proposed a blockchain-IoT framework. Authenticated scalability, decentralized schemes and assertion of data transfer for the payments are the several facilities offered with the blockchain facilitated IoT infrastructure. Further, the proposed phenomenon is validated by illustrating certain solutions using Ethereum by presenting the embedding of blockchain within IoT. However, the type of blockchain (public/private) through which intruders may further compromise intermediate IoT devices is not mentioned in this study.

Oh et al. [22] have proposed a data trading mechanism to ensure the privacy among business stakeholders for IoT markets. The authors have used Nash equilibrium to measure the feasibility and maximized the profits of market stakeholders. Hasan et al. [23] have proposed an interplanetary file system mechanism while streaming and storing the data generated by IoT devices. The authors have ensured the security of the proposed mechanism using blockchain by generating the smart contracts, algorithms and diagrams with their complete implementation process. The authors have showed the novelty and effectiveness of the proposed system as compare to traditional scheme. Lam et al. [24] have proposed a decentralized automatic orchestration and configuration mechanism based upon semantic policies. The proposed approach was deployed and verified while sending the information during planning and production in IIoT environment while transmitting over cloud.

Though various studies have proposed a wide range of techniques to ensure a decentralized, transparent and secure mechanism in IIoT networks, very few of them pointed the number of attacking strategies of the intruders aiming to disrupt or consume the network resources. Further, none of the authors relied on trust-based mechanisms to detect the nodes' legitimacy, data storage or processing techniques through blockchain specifically for IIoT networks.In summary, data science techniques within IoT were focused on various studies due to the advantages it offer as mentioned earlier. Further, few studies also focused on blockchain to provide security in IIoT. However, introducing both data science and blockchain within IIoT network can increase network efficiency in terms of efficient industrial data analytic in a secure environment. Therefore, this study provides a novel and secure framework for IIoT by integrating both data science and blockchain to identify possible threats within the network. In the next section, we provide details of our proposed framework.

3 Proposed Industrial Blockchain Framework

In order to describe our proposed solution, we considered an IIoT network, including both legitimate and malicious devices. Next, a system model is developed to validate the proposed framework. Further, a blockchain is integrated within the IIoT network to ensure secure data analysis in the proposed DS-IIoT environment. Finally, a mathematical model is derived to evaluate the performance of the network. The blockchain technique is able to build control systems and data sharing system for CU in order to address the challenges of decentralized information circulation, internal information controlling access and privacy while sharing the data among various entities. Figure 2 depicts the data sharing mechanism through blockchain where each record of every individual entity is stored on a blockchain that can be further traced and analyzed by all the users. The malicious data record or alteration in stored information can be immediately identified by all the entities though blockchain technique.

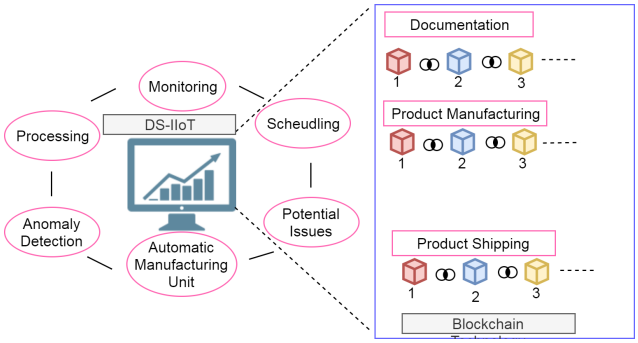


Fig. 2: Data Model of DS-IIoT using Blockchain

Further, Figure 2 highlights the blockchain-based data model in IIoT networks, suggesting that various phases such as generation, manufacturing, processing, monitoring, and anomaly detection in data can easily be resolved by maintaining separate blockchain of every phase. Moreover, by scheduling every transaction on blockchain further enhances the overall processing capabilities by maintaining a transparent relationship among the IoT devices.

3.1 System Model

Traditionally, the role of IoT devices in IIoT networks has been to monitor or control the product manufacturing, documentation, record and share it with the back-end server. In case of an attack, the intruders may breach the security of the network to steal confidential data such as industry records, employees' information and business statistical data which might affect the overall trade of the industry. Hence, in practice, IIoT networks are susceptible to attackers who tend to perform malicious activities in the IoT environment. Further, malicious devices behave intelligently in a random manner to remain undetected in order to bypass the monitoring phase of the network. Furthermore, the stored information about workers' location, activity processing, in-out time and product manufacturing record may also be stolen by the intruders for their personal usage. To tackle these sensitive issues, a novel framework has been introduced in this study, which integrates a trust-based solution and blockchain within IIoT.

The system model of the proposed framework consists of 'n' IoT devices which are assumed to be trusted initially. Among n IoT devices, the responsible to verify the legitimacy of the IoT devices is elected on the basis of two criteria, i.e., (1) energy level and (2) monitoring capability (MC). The energy

level indicates that the IoT device has sufficient energy to monitor and coordinate the activities and communication between neighbouring devices. The monitoring capability of the device, on the other hand, identifies the malicious behavior within the network. In this proposal, any IoT device with high energy level and monitoring capability is chosen as CID. Energy of the IoT devices and CID is calculated via Equation 1.

$$E_i = \sum_{p=1}^{n} \mid X_{(i,p)} \mid^2 = \begin{cases} E_i \geq \gamma \; presence \; of \; IoT \; device, \\ E_i \leq \gamma \; absence \; of \; IoT \; device. \end{cases} \tag{1}$$

Where $X_{(i,p)}$ is the p^{th} sample of the i^{th} IoT device, γ is a predefined threshold value to monitor and n is the total number of IoT devices. Further, MC of IoT devices is computed as Equation 2.

$$MC_i = NDG_i = \sum_{i=1}^{n} (PDR_i + E_i + Activeness_i) \tag{2}$$

Where MC_i is measured in terms of NDG_i (Network Development Goal) that detects the status and health of the network. The node's status and health is categorized into three colors, i.e., (1) *black* where nodes are identified as malevolent, (2) *green* for legitimate nodes, and (3) *grey* to indicate alert messages upon entry of a new node or extensive transmission of existing node in the network. DG is further dependent upon certain parameters. Packet Delivery Ratio (PDR_i) defines the number of packets forwarded by a particular node. E_i is the energy consumed by a node to transmit or forward the incoming packets and is calculated using Equation 1. Finally $Activeness_i$ shows how much time a node remains active in the network.

The MC of the CID further depends on the survival time (ST) of the device within the IIoT network. The device having sufficient energy level along with oldest survival time (OST) would be elected as the coordinator of radio environment consisting of table including CID identity, IoT device identity, CID address, ID address, TF and ST of each device. The oldest survival time of IoT device is defined as *the total time period of the IoT device to remain alive in the network*. The CID computes the trust factor of each IoT device by using various characteristics such as monitoring capability, communication among the users and actions of all the devices.

Depending on the nature of the IoT device, the potential response of CID falls into following two categories:

3.1.1 CASE 1: When existing IoT device is identified as MD

Whenever, the IoT device starts behaving maliciously, then two possibilities exist, i.e., either the IoT device is MD or it is disrupted. In both the cases, a random IoT device is forged and compromised by the intruders. In our proposed system, initial device is identified via Equation 3.

$$IoT \; Device = \begin{cases} LID: & ST_{ID} > ST_{MD} \text{ with transmission } T \\ MD: & ST_{ID} < ST_{MD} \text{ no transmission } T \end{cases} \tag{3}$$

Where, LID and MD are legitimate and malicious devices respectively. If the ST of the IoT device is higher than that of MD, then the device is identified as legitimate, otherwise, it is assumed to be compromised. Next, the TF of each IoT device is computed if the device is either compromised or transmits very large number of messages in the network. To achieve this, various parameters including previous history, MC and communication behavior (CB) are taken into account. CB is defined specially for malicious IoT devices which transmit huge number of false messages towards legitimate devices. MC and CB of any node satisfying predefined thresholds, TF is considered as 1. Otherwise, it is 0.

3.1.2 CASE 2: When new IoT device is identified as MD

In the case where a new IoT device (NID) is identified in the environment, the possibility of cases can be raised as either legitimate or malicious. In both scenarios, as the ST of NID is very less as compared to that of existing IoT devices, therefore, initially CID allows at least five communication transmissions to the NID. TF of a legitimate NID is 1, and for malicious NID, TF would always be below the predefined threshold range. Each node is assigned an initial trust value ranging from 0.7- 0.95 (as assumed) with 1 as the highest trust value. This trust is increased or decreased by checking the social rank of each node by using predefined threshold values. The main reason behind this value is that the threshold will be around 30% of the maximum value, so taking initial value range will help in the further calculation instead of taking every value as simply 1. There is a disadvantage of taking this scenario as few nodes tend to lose the trust early as compared to the other nodes. CID keeps all the records and information of the IoT devices in its table. After specified number of transmissions, TF of the NID would be checked by CID and corresponding action would be taken according to the Equation 4.

$$NID = \begin{cases} TF == 1, & \text{then legitimate ID,} \\ TF == 0, & \text{then malicious device.} \end{cases} \tag{4}$$

If TF of NID is 1, then ID is identified as trusted and allowed further transmissions, else all of its further transmissions would be blocked by considering it as an MD.

3.2 Alteration of stored information

The presence of the intruders with the intention to hack or compromise the network cannot be ignored as IIoT networks contain very sensitive information. Therefore, the proposed solution integrates blockchain in the back-end to ensure transparency in the network. The stored records are kept on blockchain so that any alteration or deletion of any information inside the IIoT network can be traced easily. The Algorithm 1 represents complete execution of the proposed framework. Further, Algorithms 2 and 3 show the high level algorithms to calculate the resulting functions TF() and MC() within the main algorithm.

3.3 Mathematical Model of the Proposed Approach

In order to validate the proposed framework, MDs are deployed randomly in the IIoT network with the following two aims: (1) to forge the identity of a legitimate device, and (2) to consume the network resources by generating false messages

Algorithm 1: Execution of Proposed IIoT Framework

Assumption: $Count_{threshold}$ = 50%
Input: (1) Network with 'n' IDs, (2) Among them one CID is elected, and (3) 'm' number of MD's
Output: ID identified as either legitimate or malicious
The CID selection is based on ST, energy level and MC.
CID maintains a table having ID id, ID address, routing information, CID id, ST and TF of each ID to identify MD. Upon the emergence, the NID is identified as MD else legitimate.
if *(ID is NID)* **then**
  CID allows first five assumptions and;
  Compute TF();
  Compute MC();
  Blockchain record ();
  The information of each record corresponding to ID is stored in the database with its current and previous hashes.
else
  ID is elected as MD
end

intentionally. This leads to a low value of the resulting TF computed by the CID. Moreover, every NID added to the network must prove its authenticity to CID. NID is only allowed to be a part of IIoT network, once it satisfies the CID by sending authentic messages. Further, if NID is malicious, then the MC would be significantly higher as it will transmit high number of messages and contact every neighbouring node to attract their attention. This results in the minimum values of DDR which affect the network throughput due to the fact that MD jeopardises and consumes most of the network resources.

Further, based on the computed TF, following four scenarios exist for both LID and MD within IIoT network. (1) H_{x0} signifies the absence of both LID and MD suggesting that neither LID nor MD approached CID to prove their legitimacy. (2) H_{x1} denotes the case when LID switches from active to the idle channel, hence requiring to prove its legitimacy to the CID. (3) H_{x2} represents a scenario, where MD tries to replicate LID in order to degrade the network performance, and finally (4) H_{x3} scenario exist, when both

Algorithm 2: Calculation of TF()

Input: The number of transactions/communications done by each IoT device are recorded to compute their TF
if *(ID's previous history and MC() satisfies predefined threshold value)* **then**
  Set TF=1 to ID;
  return 1;
else
  Set TF=0;
  Mark ID as MD;
  return 0;
end

Algorithm 3: Calculation of MC()

Input: The number of interactions or communications among IoT devices
if *(ID trace wrong information and store incorrect data)* **then**
  Set C = C+1 ;
  if *(Set C >* $C_{threshold}$*)* **then**
    ID is MD;
    return 0;
  else
    IoT device is legitimate and trusted
  end
else
  IoT device is malicious
end

LID and MD prove their legitimacy to the CID as depicted in the Equation 5.

$$\left.\begin{aligned} H_{x0} &= \text{neither LID nor MD,} \\ H_{x1} &= \text{LID only,} \\ H_{x2} &= \text{MD only,} \\ H_{x3} &= \text{LID and MD both.} \end{aligned}\right\} \tag{5}$$

The presence and absence of MD is indicated by M^{on} and M^{off} respectively. Therefore, the probability of each hypothesis 'H_{sk}' is denoted by 'μ_k' as shown in Equation 6.

$$\left.\begin{aligned} \mu_0 &= Pr(H_{x0}) = Pr(H_0), M^{off} = Pr(M^{off}/H_0)Pr_{H0,} \\ \mu_1 &= Pr(H_{x1}) = Pr(H_1), M^{off} = Pr(M^{off}/H_1)Pr_{H1,} \\ \mu_2 &= Pr(H_{x2}) = Pr(H_0), M^{on} = Pr(M^{on}/H_0)Pr_{H0,} \\ \mu_3 &= Pr(H_{x3}) = Pr(H_1), M^{on} = Pr(M^{on}/H_1)Pr_{H1} \end{aligned}\right\} \tag{6}$$

Furthermore, the attacking strategies are defined for the presence and absence of the IoT device using the attack parameters α and β which are determined as: α=Pr(M^{on}/H_1) and β=Pr(M^{on}/H_0). Therefore, previous equation can be extended to equation 7 in the following manner.

$$\left.\begin{aligned} \mu_0 &= (1-\beta)Pr(H_0), \\ \mu_1 &= (1-\alpha)Pr(H_1), \\ \mu_2 &= \beta Pr(H_0), \\ \mu_3 &= \alpha Pr(H_1). \end{aligned}\right\} \tag{7}$$

Now let W_{fa} and W_m denote the probability of false authentication and non-detection of MD at CID respectively, which are determined as: W_{fa}= $Pr(D_{on}/M^{off})$ and W_m= $Pr(D_{off}/M^{on})$, where D_{on} and D_{off} represents the CID's decision of MD's presence and absence respectively. The system will be in error if CID fails to decide correctly between the presence and absence of MD in the network. Therefore, we define the probability of error (W_e) to represent this behaviour, which is determined according to the equation 8:

$$\begin{aligned} W_e &= Pr(M^{on}, D^{off}) + Pr(M^{off}, D^{on}) \\ &= Pr(\frac{D^{off}}{M^{on}}) + Pr(\frac{D^{on}}{M^{off}})Pr(M^{off}) \\ &= W_m P(M^{on}) + W_{fa} Pr(M^{off}.) \end{aligned} \tag{8}$$

SNR_{LID} and SNR_{MD} are the the signal-to-noise ratio of LID and MD respectively. Further, to identify the impact of the MD, we have defined attack strength parameter as ρ=$SNR_{MD}/(1+SNR_{LID})$. To detect the compromised IoT devices within the network, we have considered the hypothesis that H_{x1} and H_{x3} will confirm the presence of NID with their respective probabilities μ_1 and μ_2. Therefore, the compromised IoT device (R_{NID}) can be identified according to equation 9.

$$R_{NID} = \mu_1.log_2(1+SNR_{LID}+ \mu_3.log_2(1+\frac{SNR_{LID}}{1+SNR_{MD}}) \quad (9)$$

4 Performance Analysis and Simulation Results

Till now, literature in the field has not projected a probabilistic hypothetical way to compute the trust of IoT devices for analyzing their legitimacy within IIoT networks. Probabilistic hypothetical is the probability to identify the legitimacy of IoT devices based on certain assumed hypothesis as in Equation 5. In this paper, we have formulated a mathematical model to identify the malicious IoT devices by assuming the probability of each hypothesis. Therefore, in order to evaluate our proposal, the system is validated initially on a small network by constructing a simulation area of 400m $\times$ 400m within MATLAB simulator and inserted 25 IoT devices initially. These devices are identified using unique numbers, which are assigned during the initialization phase in the system.

Whenever, a NID enters within the respective area, it is required to register and authenticate itself with the CID first. Based on the previous history and monitoring capability of the IoT device, CID either authenticates it or rejects it from the system by assigning different values of TF (either *accept* or *reject*).

We evaluated our proposed model using three distinct criteria: (1) probability of false authentication versus probability of error, (2) the compromised IoT device versus attack strength (α) whose probability is between 0-1, and (3) and the number of compromised IoT devices versus SNR caused by malicious IoT devices. Further, important simulation details are highlighted in Table 1.

TABLE 1: Simulation Parameters

Parameters	Details
Simulation Time	80 sec
Simulated Area	400m $\times$ 400m
Total IoT devices (small network)	(25, 45)
Total IoT devices (large network)	up to 100
IoT device Transmission Range	120m (Approx.)
Pr(M^{on})	0.8
Pr(M^{off})	0.2
β	0.8
α	0.2

4.1 Simulation Results

The effect of probability of false authentication (W_{fa}) on the probability of error (W_e) for the proposed system is illustrated in the Figure 3. It is apparent that W_e shows linearly increasing relationship with W_{fa}, where the probability of error increases when the authentication probability increases during the hand-off phase. In the ideal situation, the network only contains legitimate IoT devices, implying that (W_m)=1. This shows that the probability of the IoT devices to detect errors is high, as depicted in the Fig. 3. However, as soon as the network is polluted with MD, the ability of the nodes to detect error decreases. This is due to the fact that the proposed approach identifies the legitimacy of IoT devices by computing their TF. The devices with less TF are considered as MD that would not be involved during the communication process.

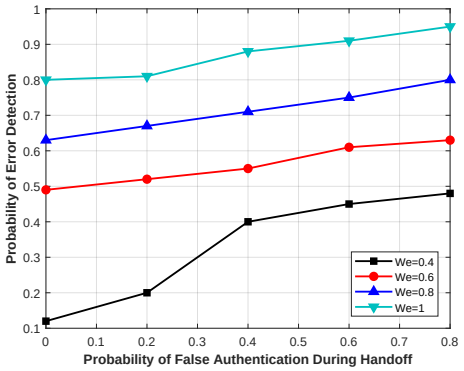


Fig. 3: Probability of false authentication (W_{fa}) on the probability of error (W_e)

Fig. 4 depicts the impact of the attack strength on the newly added IoT devices in the network. It can be seen that for a low attack strength, less number of IoT devices are affected. This compromise increases as soon as the attack strength of the MD increases. However, our proposed solution enables the network to detect MD with high impact due to the fact that the CID only allows a device to be part of the network, if it satisfies the required TF level. Moreover, the small values of α provide enhanced throughput which decreases with increase in the value of α.

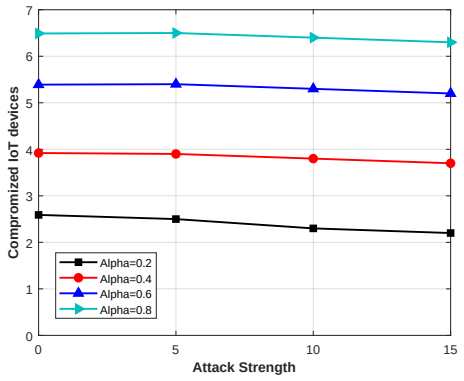


Fig. 4: Compromised IoT device affected by the attack strength

The relationship between the noise generation (R_{NID}) and SNR at compromised IoT receiver (SNR_{MD}) due to the addition of new IoT devices within the network is presented in Fig. 5. As the presence of the compromised devices increases in the network, the noise generation by intruders at

lower SNR is less as compared to higher SNR. The higher the SNR, the higher would be the probability of disruption caused by the intruders in the compromised network.

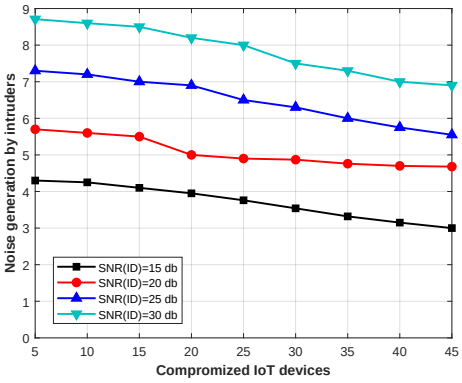


Fig. 5: SNR at compromised IoT receiver due to ID

As the proposed phenomenon analyzes each and every activity of the devices at each phase such as product manufacturing, storage recording and data delivery, the proposed approach computes the legitimacy of every node before its communication/transmission process.

4.2 Impact of Blockchain on the IIoT Network

This paper integrates a private blockchain mechanism [25], [26] at its back-end due to the fact that the data included in IIoT networks is mostly very sensitive. Further, this data must be kept private as the companies need to compete with rival industry. Therefore, the data within IIoT network must be kept private and secure, which can be achieved with the help of private blockchain. A private blockchain mechanism is the one where accessing and storing records is maintained at different levels in the network and hence it cannot be shared without the consent of administrator (CCU) permission. In this paper, separate blockchain is maintained for different process such as product manufacturing, storing records and delivering products, to name a few. All these blockchains are monitored by CCU and data is modified in the blockchain only with the consent of the administrator. Further, to encourage the cognitive users (CUs) of the network to provide positive data, CCU provides incentives in form of extra credits.

Further to analyze the integration of blockchain within IIoT networks, we relied on Java where different components (creation, validation and insertion) of blockchain is implemented. Further we validated the proposal against malevolent nodes from security aspects via MATLAB. Initially, 25 nodes are created that may further operate as IoT devices. The blockchain network contains blockchain creation module that is responsible to create blocks along with their previous and current hashes. Further, during the data insertion process of blockchain process, these devices have the ability to add various records in the blockchain. In this paper, we have inserted a single unit data (such as product manufacturing) to analyze it efficiently.

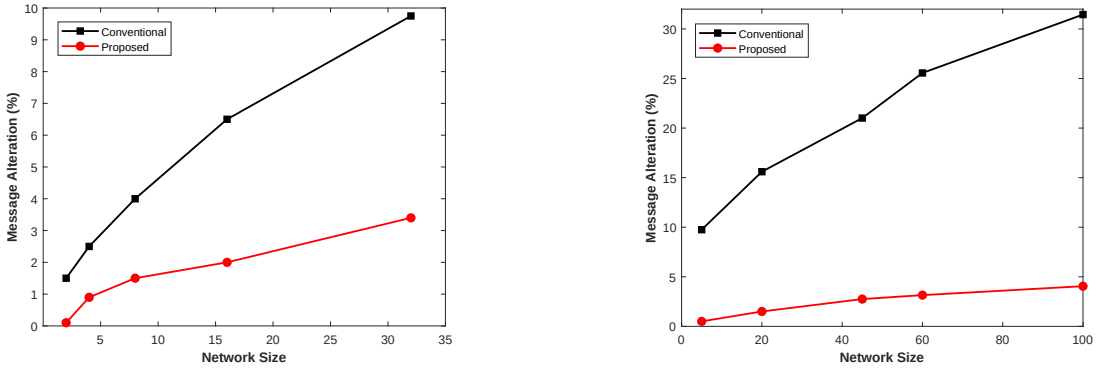
Finally, the newly added blocks by the miners need to be verified and validated. If the miners are successfully able to verify the block then they are considered as valid and stock is successfully added, otherwise block is rejected. We have evaluated our proposal in presence of intruders for both small and large IIoT networks. A blockchain network of initially 5 ledgers is implemented using Ethereum where each block contains the product information with its respective hash. This ledger grows further as soon as the devices generate data to be stored within the database. Further, we equipped malicious devices in the blockchain network with the ability to alter and delete the recorded data. Simulation results depicted that our proposed solution performs efficiently in presence of these malicious devices.

We have evaluated our proposal in presence of intruders for both small and large IIoT network as depicted in Fig. 6. A blockchain network of initially 5 ledgers is implemented using Ethereum where each block contains the product information with its respective hash. This ledger grows further as soon as the devices generate data to be stored within the database. Further, we equipped MDs in the blockchain network with the ability to alter and delete the recorded data as shown in Fig 7. We considered two scenarios, (1) *Conventional scenario*: where no blockchain is considered, and (2) *Proposed scenario* includes blockchain at the back-end. Fig. 6 shows that in the absence of blockchain in the conventional method, the network is affected more as the intruders can alter or delete the data. However, in our proposal, the impact of intrusion is limited as the devices will be unable to delete or alter the data. This is due to the fact that our proposed approach is based on blockchain in the back-end which provides transparency among all the IoT devices and users so that a single change would reflect in all others' database and would become easily traceable.

4.3 Impact of Trust on the IIoT Network

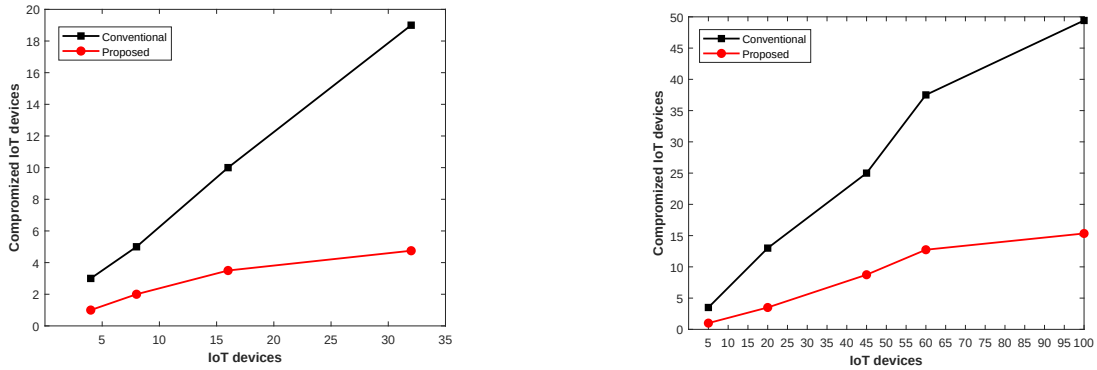
Fig. 7 depicts the impact of the compromised IoT devices on the legitimate devices in the network. Conventionally, without applying the trust based mechanism, it becomes very easy to compromise IoT devices by the intruders. However, the current proposal integrates a trust-based mechanism, which only allows the devices to be part of the network after they have been authenticated by the CID. This limits the impact caused by the compromised IoT devices.

However, the proposed phenomenon provides better results as CID computes TF based on their internal behaviour. Similarly, in Figure 7, the proposed phenomenon performs better in terms of compromised miners where during initial establishment of the network, intruders can easily alter the miners, however, miners are selected based on their TF which prevents this scenario. Further, the limitation of this paper is as follows 1) firstly, the proposed scheme is unable to provide a proper verification by comparing the security metrics against any existing method that uses the data sharing process using blockchain mechanism in IIoT networks. None of the authors to the best of our knowledge have worked on datascience mechanisms using blockchain in IIoT while manufacturing or shipping the information, and 2) secondly, the proposed scheme is unable to judge an accurate decision while transmitting the information in real time scenarios as the block verification process may further delay the validation and enhance the changes of other security threats inside the network.



(a) (b)

Fig. 6: Message Alteration for (a) Small Network (b) Large Network



(a) (b)

Fig. 7: Compromised IoT deivces for (a) Small Network (b) Large Network

5 Conclusion

This paper has proposed a secure framework based on trust management and blockchain to deal with the issues caused by MDs at various levels in IIoT networks. The proposed model identifies the legitimacy of each IoT device by computing its Trust Factor (TF) through an elected Coordinator IoT Device (CID). In order to prevent changes in the information of the local database, a data model based on blockchain is maintained at the back-end to keep track of all the transactions within the industry. The approach is validated extensively for different network sizes and evaluation criteria. Simulation results suggest that our proposed framework achieves 91% success rate against the network without a blockchain.

References

[1] A. Karpatne, G. Atluri, J. H. Faghmous, M. Steinbach, A. Banerjee, A. Ganguly, S. Shekhar, N. Samatova, and V. Kumar, "Theory-guided data science: A new paradigm for scientific discovery from data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 10, pp. 2318–2331, 2017. doi:10.1109/TKDE.2017.2720168.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017. doi: 10.1109/MCOM.2017.1600514.

[3] H. Oh, S. Park, G. M. Lee, H. Heo, and J. K. Choi, "Personal data trading scheme for data brokers in iot data marketplaces," *IEEE Access*, vol. 7, pp. 40120–40132, 2019. doi:10.1109/ACCESS.2019.2904248.

[4] P. A. Merolla, J. V. Arthur, R. Alvarez-Icaza, A. S. Cassidy, J. Sawada, F. Akopyan, B. L. Jackson, N. Imam, C. Guo, Y. Nakamura, *et al.*, "A million spiking-neuron integrated circuit with a scalable communication network and interface," *Science*, vol. 345, no. 6197, pp. 668–673, 2014. doi:10.1126/science.1254642.

[5] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," *IEEE communications magazine*, vol. 52, no. 2, pp. 122–130, 2014. doi:10.1109/MCOM.2014.6736752.

[6] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, no. 2, pp. 76–79, 2017. doi:10.1109/MC.2017.62.

[7] L. Zhou, D. Wu, J. Chen, and Z. Dong, "When computation hugs intelligence: Content-aware data processing for industrial iot," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1657–1666, 2017. doi:10.1109/JIOT.2017.2785624.

[8] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, 2019. doi:10.1109/TII.2019.2903342.

[9] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (iiot) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, 2018. doi:10.1109/TII.2018.2808190.

[10] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 3652–3660, June 2019. doi:10.1109/TII.2019.2894573.

[11] J. A. Shamsi and M. A. Khojaye, "Understanding privacy violations in big data systems," *IT Professional*, vol. 20, no. 3, pp. 73–81, 2018. doi:10.1109/MITP.2018.032501750.

[12] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based iot security through trustworthy cloud service: An integration of security and reputation approach," *IEEE Access*, vol. 7, pp. 9368–9383, 2019. doi:10.1109/ACCESS.2018.2890432.

[13] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1928–1939, 2016. doi:10.1109/TIFS.2016.2566446.

[14] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen, and J. Cao, "Collaborative network security in multi-tenant data center for cloud computing," *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 82–94, 2014. doi:10.1109/TST.2014.6733211.

[15] P. Danzi, A. E. Kalør, Č. Stefanović, and P. Popovski, "Delay and communication tradeoffs for blockchain systems with lightweight iot clients," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2354–2365, 2019. doi:10.1109/JIOT.2019.2906615.

[16] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, 2018. doi:10.1109/LWC.2018.2820009.

[17] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, 2019. doi:10.1109/JIOT.2019.2905743.

[18] J. Yan, Y. Meng, L. Lu, and L. Li, "Industrial big data in an industry 4.0 environment: Challenges, schemes, and applications for predictive maintenance," *IEEE Access*, vol. 5, pp. 23484–23491, 2017. doi:10.1109/ACCESS.2017.2765544.

[19] W. Wang, L. Fan, P. Huang, and H. Li, "A new data processing architecture for multi-scenario applications in aviation manufacturing," *IEEE Access*, vol. 7, pp. 83637–83650, 2019. doi:10.1109/ACCESS.2019.2925114.

[20] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, "A high performance blockchain platform for intelligent devices," in *2018 1st IEEE international conference on hot information-centric networking (HotICN)*, pp. 260–261, IEEE, 2018. doi:10.1109/HOTICN.2018.8606017.

[21] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018. doi:10.1109/MWC.2017.1800116.

[22] H. Oh, S. Park, G. M. Lee, J. K. Choi, and S. Noh, "Competitive data trading model with privacy valuation for multiple stakeholders in iot data markets," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3623–3639, 2020.

[23] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy iot data streaming using blockchain and ipfs," *IEEE Access*, vol. 10, pp. 17707–17721, 2022.

[24] A. N. Lam, Ø. Haugen, and J. Delsing, "Dynamical orchestration and configuration services in industrial iot systems: An autonomic approach," *IEEE Open Journal of the Industrial Electronics Society*, vol. 3, pp. 128–145, 2022.

[25] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial internet of things technology," *IEEE Transactions on Computational Social Systems*, vol. 6, pp. 1442–1453, Dec 2019. doi:10.1109/TCSS.2019.2924054.

[26] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 3527–3537, June 2019. doi:10.1109/TII.2019.2898900.

Geetanjali Rathee is currently working as an Assistant Professor in the Department of Computer Science and Engineering of Netaji Subhas University of Technology (NSUT), Dwarka, New Delhi, India. She has also worked as an Assistant Professor (Senior Grade) in Jaypee University of Information Technology (JUIT), Waknaghat, Himachal Pradesh for four years. She received her B.Tech, M.Tech and Ph.D., all in Computer Science & Engineering in 2011, 2014 and 2017 respectively. She has published around 06 national/international patents, around 10 IEEE transactions research papers with highest impact factor of 9.1, 20 SCI papers, around 40 Scopus indexed papers and more than 15 publications in national/international conferences and book chapters. She has also published one book titled "Large-Scale Data Streaming, Processing, and Blockchain Security". Her research interests include handoff security, cognitive networks, blockchain technology, resilience in wireless mesh networking, routing protocols, networking, and industry 4.0. She is a regular reviewer of various reputed journals like IEEE Transactions on Vehicular Technology, Wireless Networks, Cluster Computing, Ambience Computing, Transactions on Emerging Telecommunications Engineering, and International Journal of Communication Systems.

Farhan Ahmad is working as an Assistant Professor with the Systems Security Group at the Centre for Future Transport and Cities, Coventry University, United Kingdom. Dr. Ahmad received his Ph.D. in Computer Science from the University of Derby, the United Kingdom in 2019; M.Sc. in Communication and Information Technology from the University of Bremen, Germany, and B.Sc. in Electronics Engineering from COMSATS University Islamabad, Pakistan. Dr. Ahmed also holds ISO/SAE 21434 automotive standard certification (Certified Automotive Cyber Security Professional) from SGS, TUV SAAR Academy, Germany. His research is focused on the safety and security of Cyber Physical Systems, Threat Analysis and Risk Assessments of automotive networks and cyber security of vehicular Networks and Industrial IoT from trust management aspects.

Naveen Jaglan was born in 1989, obtained B.Tech (Hons.) and M.Tech (Hons.) degrees in Electronics and Communication Engineering from Kurukshetra University, India in 2009 and 2011, respectively. He obtained his Ph.D. on "Design and Development of Microstrip Antennas integrated with Electromagnetic Band Gap structures" from Jaypee Institute of Information Technology, Sec-62, Noida, U.P., India in June 2017. He has authored/co-authored several research papers in referred international journals and conferences. His research includes microwave communications, 5G antenna design, planar and conformal microstrip antennas including array mutual coupling, artificial materials (metamorphic, metamaterials), EBG, PBG, FSS, DGS, novel antennas, UWB antennas, MIMO systems, numerical methods in electromagnetic, Composite Right/Left Handed (CRLH) transmissions and High-k dielectrics. His skill includes modelling of antenna and RF circuits with Ansoft HFSS/CST Microwave Studio/ADS Momentum, measurements using Vector Network Analyzer and Anechoic Chamber.

Charalambos Konstantinou (S'11-M'18-SM'20) is an Assistant Professor of Computer Science (CS) and Electrical and Computer Engineering (ECE) at the Computer, Electrical and Mathematical Science and Engineering Division (CEMSE) of King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He is the Principal Investigator of the Secure Next Generation Resilient Systems Lab (sentry.kaust.edu.sa). His research interests are in secure, trustworthy, and resilient cyber-physical and embedded IoT systems. He is also interested in critical infrastructures security and resilience with special focus on smart grid technologies, renewable energy integration, and real-time simulation. He received a Ph.D. in EE from New York University (NYU), NY, in 2018, and a M.Eng. Degree in ECE from National Technical University of Athens (NTUA), Greece, in 2012. Before joining KAUST, he was an Assistant Professor at Florida State University. Konstantinou is currently the Chair of the IEEE Task Force on Resilient and Secure Large-Scale Energy Internet Systems and the co-Chair of the IEEE Task Force on Cyber-Physical Interdependence for Power System Operation and Control. He is a Senior Member of IEEE, a member of ACM, and an ACM Distinguished Speaker (2021-2024).