Securing IoT devices using Blockchain

Siddesh Sharma[#1], Sudhanshu Singh[#2], Sakshi Rathod[*3], Piyush Kasar[*4]

Department of Computer Engineering,
Shri Vile Parle Kelavani Mandal's Institute of Technology, Dhule, India

***Abstract*:** Communication security between IoT devices is a major concern, and the blockchain has raised hopes that this concern will be addressed. The majority, if not all, of network nodes in the blockchain concept, examine the quality and integrity of transferred data before accepting and recording it, whether this data is related to financial transactions or measurements of a sensor or an authentication message. In evaluating the validity of an exchanged data, nodes must reach a consensus in order to perform a special action, in which case the opportunity to enter and record transactions and unreliable interactions with the system is significantly reduced. The validity of exchanged data can be guaranteed by validating the device it is coming from in the first place.This proposed work system provides security to the IoT devices through smart contracts which enhance security and privacy concerns.

Keywords: IoT, HL Fabric

I. INTRODUCTION

Due to the revolution of digital technology such as the Internet of Things, various areas such as industries, health sector, and governance use IoT. This IoT device makes the availability of data in real time scenarios. Besides this IoT also helps to automate the devices based upon certain triggering conditions. To do so various researchers started work in this domain. They came up with various solutions such as the way of connections of devices, protocols and speed of connectivity of devices. By the verge of development in the networking domain the connectivity of the internet transforms from 2G to 4G and in some of the developed countries it has shifted to 5G. IoT uses the connectivity media to transfer data which is sensed in the perception layer through the sensor. These sensors are input to the system and after sensing this data system processes the data, takes some decisions which are provided to the various actuators. Generally this discussed scenario appears in the automation sector. Automation is the most demanded. This automation is adopted in various domains such as public health, smart grids, smart transportation, waste management, smart homes, smart cities, agriculture, energy management, etc.

By leveraging the benefits of Iot it is easy to bring automation in Industries in particular, IoT an abbreviation of Industrial Internet of Things, an application of Iot where the focus is heavily on interconnectivity, automation, machine learning and real-time data. While every company and organization operating today is different, they all face a common challenge—the need for connectedness and access to real-time insights across processes, partners, products, and people.

To address the security challenges that persist currently in the perception layer and to establish trust in the IoT environment, To enhance integrity and credibility of data collected an auditable platform comes into picture that inherits tamper-resistant properties. The emerging blockchain technology provides a mechanism for establishing trust among various parties. As a result such a platform could assist in assuring the security of such parties, All information shared among IoT entities would be based on trust. The immutable property of blockchain could be a mechanism for establishing information provenance that is resistant to manipulation. Through "smart contract" it can be used to enforce access controls and adopt actionable strategies.

Limitations of "things" raise a number of challenges in connectivity as well as security aspects. This paper comprises brief analysis on current traditional design of IoT security components and how they function and flaws associated with them. And how to overcome those flaws in the current scenario with respect to IoT using blockchain approach by evolving smart contracts at perception layer.

II. Security issues in IoT and CPS

The security issues associated with IoT can be life threatening as well as costly when used in an industrial environment. These things can be used for automation and remote equipment management, Predictive maintenance, faster implementation of improvements, Pinpoint inventories, Quality control, and Supply chain optimization.

The main Iot security concerns are authentication, authorization, integrity, confidentiality, availability, Non-repudiation and privacy.

Security issues in different layers.

IoT Layers	Security Issues	Security Requirements
Perception	Tampering, Malicious code injection, Sybil Attack, Fake Node, Replay Attack, Routing Threats	Lightweight Encryption, Authentication, Key Agreement
Network	MITM, DoS, Eavesdropping/sniffing, Routing Attacks,	Communication Security, Routing Security, Intrusion Detection, Key Management
Application	Data Accessibility and Authentication	Authentication, Privacy protection, Information Security management

The perception layer (or) the physical layer of IoT and CPS share attacks with common intention and procedure. These attacks can be launched when an attacker is close to our interconnected system. Some of them are discussed below.

- **Tampering:**
- **Malicious Code Injection**
- **Fake Node Injection**
- **Sybil Attack**
- **Routing Threats**

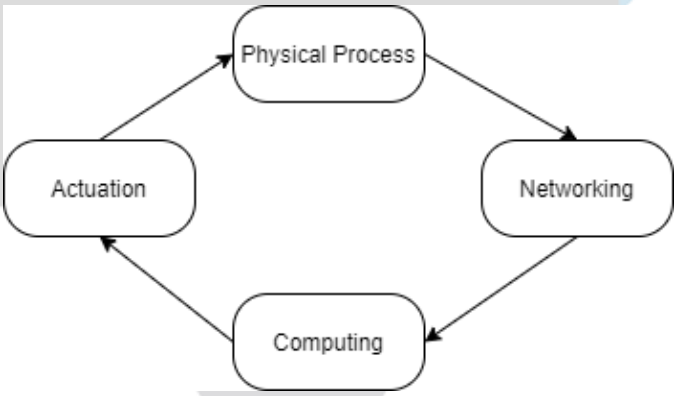
Now, as we all know that the IoT network is just a wide interconnection among *Cyber Physical System*(CPS) we will further discuss how CPS functions in the industrial environment and security issues associated with it.

A. Cyber Physical Systems

CPS refers to a new generation of systems with physical and computational capabilities that can interact with humans. CPS technology seeks to develop the process, networking and technology needed for the seamless integration of cyber and physical systems.

Workflow of CPS can be categorized into the following:

Monitoring, Networking, Computing, Actuation,



.

III. Blockchain solution for IoT

In this section, we will discuss proposed solutions from various authors sharing a common goal of addressing security challenges in the Internet of Things powered devices by leveraging the benefits of Blockchain technology.

Bluetooth Low Energy (BLE) enabled IoT devices connected to the gateway and required to maintain security as well as privacy concerns hence the researchers proposed by introducing consent to access the gateway. Based upon this approach untrusted or malevolent as well as dishonest clients cannot access the gateway[3].

In one of the works [3], Bluetooth Low Energy (BLE) enabled IoT devices to have Blockchain connected gateway to maintain secure and adaptive user privacy preferences. Users' data privacy is maintained by this gateway as it requires users' consent for accessing it. Untrustworthy or malevolent service providers and dishonest clients may purposefully withhold service provisions to profit themselves.

The work [5] proposes a blockchain-based non-repudiation network computing service method, which is especially useful in industrial IoT applications, to prevent such harmful repudiation operations. The required service programme is separated into two

non-executable portions, and blockchain is used as a service publication proxy as well as an evidence recorder in this scheme. Each of these pieces is transmitted individually via on-chain and off-chain channels, coupled with mandated evidence submissions, to enforce non-repudiation.

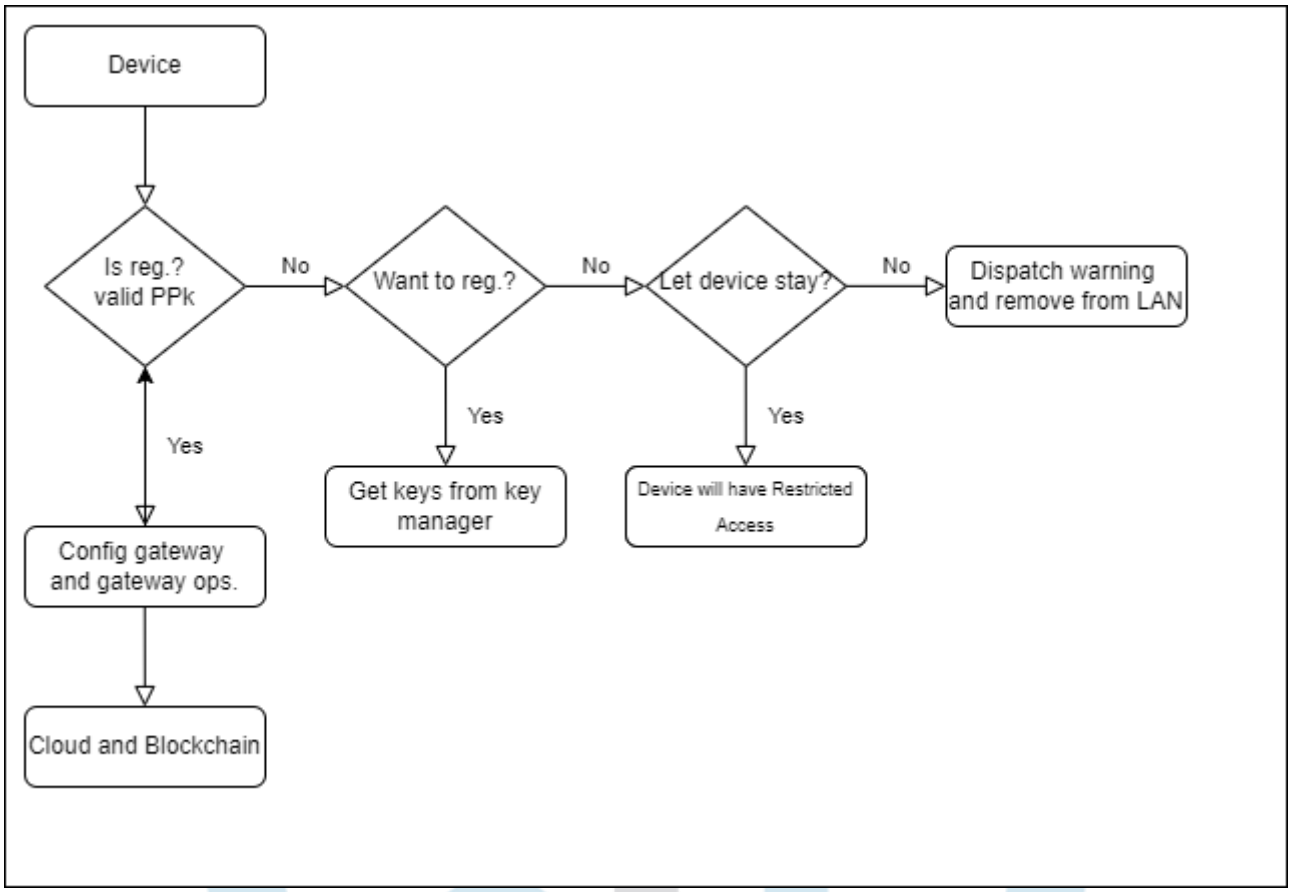
Lin et al. [6] have also proposed BSeIn for Industry 4.0, a blockchain-based system that enforces secure mutual authentication remotely with fine-grained access management. The suggested approach uses attribute signatures and blockchain to anonymously authenticate end-user terminals. The Message Authentication Code (MAC) is used to verify gateway authentication. Furthermore, BSeIn employs the multi-receivers encryption [7] approach to ensure that authorised participants remain anonymous. Finally, in order to assure scalability, Smart Contracts are used to process requests.

Apart from the ones mentioned above, two of the primary problems of industrial IoT are attaining high-quality data gathering with a restricted sensing range of energy-constrained Mobile Terminals (MTs). The other issue is ensuring secure data sharing and interchange among MTs. To solve this issue, the work [8] proposes an Ethereum blockchain-enabled method, as well as Deep Reinforcement Learning (DRL), to fulfil the stated goal and establish a reliable IoT ecosystem. The distributed DRL-based strategy assists MTs in moving to the best site for data collecting based on geographic fairness. An MT can encrypt data with its private key and send it to the blockchain as a signature for storage after data gathering. Ethereum offers data security and reliability since it is a tamper-proof ledger. Huang et al. [9] have developed a credit-based proof-of-work (PoW) mechanism for IoT devices to provide transaction efficiency and system security at the same time. The proposed methodology is built on blockchains with a DAG structure, which will be used to create a data authority management technique. This method controls who has access to sensor data, ensuring the secrecy and privacy of sensitive data. Apart from the plethora of options (mentioned above), Blockchain technology also enables various IoT applications to improve their security, and transparency, and add new capabilities to their pre-existing systems. As a result, we'll look at how two of the most important IoT applications have embraced blockchain to improve their system's decentralisation, scalability, and other features.

Let us discuss the solution in which we can couple IoT devices capable of making remote HTTPS calls with a Permissioned Blockchain network. Creation of suitable iot device, a suitable iot device is the one which can make http request to endpoints as Hyperledger network may sit in remote or local server. First course of action is to identify a device identification of a device can be done based on chip id which is immutable and is only limited to the chip. Chip id is enforced by device manufacturer at the time of manufacturing. Next, once we get access to original chip id we let IoT device to self-enrol themselves. Once the self-enrol process is initiated by the device it finds itself to be categorized into a pending pool. Pending pool is a record maintained by the network that represents devices which are not recognized by an authorized user.

The overview of implementation can be divided into three different part IoT device, Hyperledger fabric blockchain network, DAuth a frontend application to manage devices. IoT Device, ESP32 is a series of low-cost, low-power system on a chip microcontrollers with integrated Wi-Fi and dual-mode Bluetooth. The ESP32 series employs either a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations, Xtensa LX7 dual-core microprocessor or a single-core RISC-V microprocessor and includes built-in antenna switches, RF balun, power amplifier, low-noise receive amplifier, filters, and power-management modules.We later upload code to perform invoke task. Hyperledger Fabric Blockchain Network, The policies in the fabric network are defined in the way of a hierarchy. Each policy has its own dedicated section. The top-level hierarchy in policies is "/Channel". It is exceptionally restrictive because any change in the channel level policy affect the whole network. The next level is "/Channel/Orderer", "/Channel/Application", and "/Channel/Application/Organization". The policies have such names as "/Channel/Application/Organization / Policy Name ". The standard policy names are "Readers", "Writers", "Admins" and "Endorsers". For example, "/Channel/Application/Org1 /Readers" governs who can read the channel. Figure 5 shows our policies for Org1 (Org2 and IoT also have the same policies). The policy name is Readers, and the policy type is Signature. The rule for the Readers policy is "OR" which means that anyone from Org1MSP.admin, Org1MSP.peer, or Org1MSP.client can read the channel. DAuth, It is a frontend application written in reactJs. task with out Hyperledger newtork's REST API to perform task.

Once a device makes it to the pending pool it is the matter of time when an authorized user enrolls it to the authorized device pool that develops a middleware mechanism that sits between the IoT device and end application's (eg: server) communication link. This mechanism gives more control on devices and real time updates on activity performed by the network. A device can be added to enrolled devices when asymmetric enrollment takes place between verified user and a device.



IV. Conclusion

Nowadays, blockchain and Internet of Things (IoT) technologies are bonding. Blockchain first attracted attention as part of a wave of crypto currencies, especially Bitcoin, which challenged the normal course of financial transactions. But it was not the blockchain financial transactions that caught the attention of IoT activists, but rather the data exchanges. Blockchain is essentially an anti-hacking, distributed, and event logging mechanism that appears to be very useful for solving key issues related to networks where connected devices automatically interact with each otherwise. IoT. Because of the importance of security in IoT, many schemes have been proposed in this subject. In this report we saw how and where we can accommodate blockchain framework to strengthen the security and maintain integrity of our IoT network. We also discussed on elements that will make up our network and how will they communicate with each other. Further we will be making our own blockchain framework and setup cloud services and complete our network.

V. References

1. S. Cha, J. Chen, C. Su, K. Yeh, A blockchain connected gateway for ble-based devices in the internet of things, IEEE, Access 6 (2018) 24639–24649.
2. U.-M. H. J.-H. Kim, S.-K.; Kim, A study on improvement of blockchain application to overcome vulnerability of iot multi platform security, Energies 12 (402).
3. Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based non-repudiation network computing service scheme for industrial iot, IEEE Transactions on Industrial Informatics.
4. C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications 116 (2018) 42 – 52.
5. S. H. Islam, M. K. Khan, A. M. Al-Khouri, Anonymous and provably secure certificateless multi receiver encryption without bilinear pairing, Security and Communication Networks 8 (13) (2015) 2214–2231.
6. C. H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement 1405 learning, IEEE Transactions on Industrial Informatics.
7. J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, P. Zeng, Towards secure industrial iot: Blockchain system with credit-based consensus mechanism, IEEE Transactions on Industrial Info