Monitoring Health of IIOT Devices using Blockchain

Rushika Ramane
Information Technology
A. P. Shah Institute of Technology
Thane, India
rushikaramane@apsit.edu.in

Rutuja Patole
Information Technology
A. P. Shah Institute of Technology
Thane, India
rutujapatole@apsit.edu.in

Soundarya Nevrekar
Information Technology
A. P. Shah Institute of Technology
Thane, India
soundaryanevrekar@apsit.edu.in

Prof. Anagha Aher
Information Technology
A. P. Shah Institute of Technology
Thane, India
anaher@apsit.edu.in

Prof. Neha Deshmukh
Information Technology
A. P. Shah Institute of Technology
Thane, India
npdeshmukh@apsit.edu.in

***Abstract*—Nowadays, we are encircled by countless IoT (Internet of Things) gadgets and sensors. These gadgets are intended to make life simpler and more agreeable. Blockchain innovation, particularly its mass application, is speedily developing into a profitable venture. A blockchain additionally called a circulated shared record, is a permanent information base of records by cryptography. It permits trade and capacity of computerized resources without the requirement for outsider oversight. Gadgets that download a setup record from an incorporated worker need to believe that power and in the event that it is undermined the gadget gets defenceless. With a blockchain, the requirement for focal authority is missing. Gadgets trade resources straightforwardly between one another. Reception of blockchain into big business networks actually has a couple of provokes that should be handled. Using blockchain can bring expanded security and proficiency of gadget upkeep. The vital component of the blockchain, immutability, carries protection from unapproved alterations. The entire history of gadget arrangement changes is put away in the blockchain, consequently recuperation after occurrences is exceptionally direct. Observing of gadget execution and traffic assumes working organization gadgets and their interconnection. Gadget and interface statuses should be followed for picking up an extensive review of organization conditions. This paper elaborates on monitoring the organization data and the idea is dependent on blockchain innovation. Organization heads control network gadgets by implicating by recording the change of gadget arrangement into the blockchain. The critical curiosity of our answer is a circulated executives of setup documents of IoT gadgets in big business networks using blockchain innovation. This is basically improving security and capacity alternatives for arrangements in the blockchain.**

***Index Terms*—Blockchain, Industrial Internet of Things, Security, Software Monitoring**

I. Introduction

Two of the foremost charming technologies these days are unit blockchain and Internet-of-Things (IoT). The alliance concerning blockchain and IoT has nice prospects and can explore new ways in which of developing different applications in varied domains. Blockchain technology maintains a distributed and consistent ledger at each node among the network with none trusty the third party.

IIoT tools remain stationed inside firms to support production organizations (e.g. automotive) to obtain in-depth acumen into the diverse phases of production, and hence enhancing product competence and attaining price rebates. The foremost draw of IIoT devices is that they will improve safety, dependability, and energy efficiency. These devices integrate sensors that collect real-time or consecutive data and hook up with data analytics and control methods. As the number of combined devices increases, so do conceivably devastating cyber threats. Cyber threats on crucial infrastructure can have much more damaging and extensive effects.

In this article, we recommend a blockchain-based scheme used to monitor the well-being of IIOT devices. This method is devised to observe the software situation of IIoT instruments to identify and acknowledge unidentified spiteful operations (e.g. invasions). The software catches the snap from the device and stocks it in the database and monitors their files and the system calls. To make sure the software probity data, we use a blockchain because the distributed record stocks a snap of software state. The evaluation of monitoring, scalability, security, and accessibility exhibits that the method can provide deployment of large-scale IIoT tools also assure validated software updating, to recognize unlawful malicious software status.

II. Literature Review

A. BoSMoS

The paper titled A Blockchain-based Status Monitoring System for Defending against Unauthorized Software Updating in Industrial Internet of Things (2020) [1] was published by Sen He, and Wei Ren, Tianqing Zhu, Kim-Kwang, Raymond Choo

Approaches to consensus: Each proof of work consensus necessitates the validation of a block through nodes unveiling that they expect some work and are public to an arbitration of the effects. The task is typically a combination of intricate calculations on how nodes consent to the appropriate answer before annexing a block to the blockchain. This is frequently executed by miners and demands tons of computation power within the proof of stake consensus, nodes prove that they retain a stake on the Blockchain consequently approving of the accretion of the new block to the Blockchain. The aforementioned is usually achieved by owners of a stake inside the blockchain and isn't inevitably resource-intensive in terms of computation power.

Benefits: Ledger will be the system of record for the business - Transactions (asset transfer) and Contracts (conditions for a transaction to occur).

Drawbacks: The entire system may be malfunctioning, communication can be faulty.

B. Tornado

The article titled Tornado Enabling Blockchain in Heterogeneous Internet of Things through A Space-Structured Approach (2020) [2] published by Yinqiu Liu, Kun Wang, Kai Qian, Miao Du, and Song Guo

Internet of things has made its way as an emerging technology in many well-known sectors such as healthcare, industrial manufacturing, etc. Generally, this technology is used in in-depth applications where there are issues related to security, authorization, and certification. The before-mentioned centralized approaches are profoundly exposed to Denial of Service, Sybil attacks, or tampering leading to the whole IoT network crashing. Deploying blockchain in such systems in an append-only database stored in a peer-to-peer (p2p) network, assuring data probity, non-tampering, and traceability. Even after stationing blockchain in IoT there still endures many concerns which can't be completely diminished. Thus to take care of the above problems the blockchain system with space-structured ledger architecture called Tornado to enable blockchain in IoT was developed. They have used the collaborative proof of work consensus algorithm and along with it is the protocol known as Space-Structured Greedy Heaviest-Observed SubTree (S2Ghost). This protocol secures the uprightness of data and devices.

Benefits: Enhanced connectivity with partners, customers, suppliers.

Drawbacks: Differentiated mining difficulty, Parallel workflows.

C. Towards Secure Industrial IoT

The paper titled Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism (2019) [3] was published by Junqin Huang, Ling Kong, Guihai Chen, Min-You Wu, Xue Liu, Peng Zeng

The integration of IoT and blockchain helps us achieve many factors such as data integration, authorization, and scalability. But still, there are many challenges to be addressed. Major issues include the trade-off between efficiency and security where the consensus algorithm comes into the picture to defend against malicious attacks but results in overloaded IoT devices.Then comes the issue related to privacy and transparency where the data collected is sensitive and needs to be only viewed by the authorized users. Lastly the concern with high concurrency and low throughput where the throughput of blockchain is limited by various mechanisms. To deal with all these matters a blockchain system with a credit-based consensus mechanism for IIoT was proposed. This paper deals with all the three major concerns mentioned above by proposing a general, scalable and secure blockchain system for IIoT, where we outline a moderate-cost credit-based PoW mechanism and a sufficient access control system for power-constrained IoT devices.

Benefits: It has immensely helped to further strengthen the industrial systems by offering benefits like secure data sharing, privacy preserving data aggregation, data confidentiality etc.

Drawbacks: Single point failure, Sybil attack and tampering of data.

While blockchain credentials continue being broadly extended, multiple concerns should still be discussed. Through this, blockchains will enhance not only extra scalable and skilled but more strong as well. The characteristics they contribute are exceptional if arbitrated independently, including the majority of the devices people imply are recognized for years. Despite, the combining of all these traits makes them perfect for many applications acquitting the intense interest of several industries.

III. Objectives

A. Accuracy

To ensure the precision of the monitoring module, wrong negative values and wrong positive values can have a severe influence on the whole network.

B. Monitoring

The monitoring module is supposed to identify the alteration of the current status of the target program and alert the admin terminal.

C. Security

To guarantee the elimination of any vulnerabilities of the blockchain network to avoid the framework from being damaged by attackers.

D. Soundness

To ensure that other nodes interacting with the node are genuine, the other nodes will acknowledge the node's request and direct the intended information to the trusted block.

E. Scalability

To grant access to a huge number of nodes to connect or exit the network and their presence and actions won't cause discrepancy within the network.

IV. Existing System

The existing security measures undertaken by corporations deploying IIoT are:

A. Risk assessment models

Before installing and operating IIoT systems, a risk assessment model should be employed to identify all the digital and physical components to be protected. Through vulnerability and risk assessments all risks should be discovered and classified as acceptable or unacceptable. Risk assessments should continue on an annual basis with periodic reviews.

B. Segmentation

IIoT systems should be divided into sub systems which have common security requirements, and then logically isolated from each other. Information flow and access is restricted and protected using firewalls, ACLs, etc.

C. Device integrity and availability

Using CIA models, devices and components that are classified as critical are protected with mechanisms that provide support to them.

D. Encryption

The IIoT systems must employ up to date cryptography protocols and support advanced forms of encryption. Many industrial protocols currently in use were not designed with security in mind and lack basic authorization and encryption features. Data is at risk at both rest and in transit.

E. Privacy

Encryption of confidential data needs to be ensured through widely used security protocols to ensure privacy in transit as well as storage.

V. Problem Statement

As more and more industries plan to incorporate IIoT devices to perform various services, the need to secure the data generated because of this arises with greater urgency. The requirement of the market is such that all parties involved in such an industry collaboration, which do not necessarily trust each other, can rely on a secure system to ensure their interests are being protected. Even minor mishaps could result in loss of sensitive data, or capital. The security measures currently being taken are not very effective due to the complexity of IIoT networks.

The threat of a cyber attack on IIoT networks isn't hypothetical, as hackers have already deployed malware to exploit inter connected sensors and gained access to private networks. Globally, industries face critical threats to their infrastructure because of unauthorised intrusions intending to disrupt, degrade, or destroy systems. Industrial operations were forced to close down in the Middle East due to use of a malware called Triton, a new type of Trojan. Power was also shut off in a region of Ukraine due to hackers. Numerous attacks have been observed to be the work of Russian, US, Iranian, North Korean, Chinese and Israeli organisations. Corporations from the sectors of energy, water, aviation, and manufacturing are at risk of having their data stolen, according to the FBI and US Department of Homeland Security (DHS). [3] [4]

Even so, companies like Cisco Systems, IBM Corporation, Intel Corporation, and many others in the market wish to connect millions of IIoT devices to analyse data and optimise business processes. By utilising IIoT devices, it would be possible to offer products as services. However, to bring this idea to fruition, it is essential to absolutely eliminate all present risks and vulnerabilities to create an airtight network that cannot be broken into.

We intend to do exactly that by creating a reliable product that makes use of blockchain technology. Our aim is to protect smaller scale industries from encountering disaster in their regularly scheduled operations by continuously monitoring activities and making sure that procedures are being carried out as intended.

VI. Proposed System

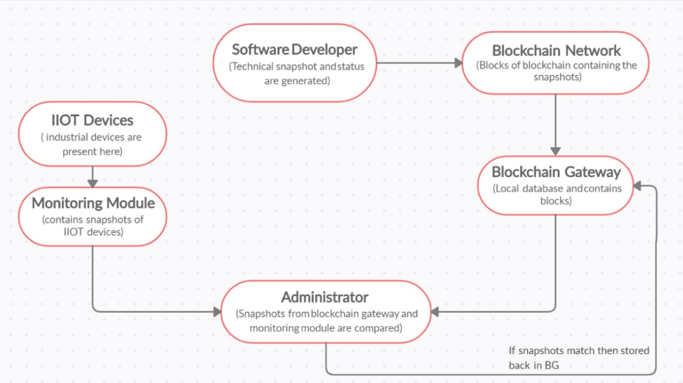
Software Developer
(Technical snapshot and status are generated)
Blockchain Network
(Blocks of blockchain containing the snapshots)
IIOT Devices
(industrial devices are present here)
Blockchain Gateway
(Local database and contains blocks)
Monitoring Module
(contains snapshots of IIOT devices)
Administrator
(Snapshots from blockchain gateway and monitoring module are compared)
If snapshots match then stored back in BG

Fig. 1. Proposed System Working

By observing the status of it, the product holds the trustworthiness of the app. The program's status data contains data on computer program judgment and record data that's critical to the program. By comparing reliable program status depictions, the gadget can decide program status and will alarm the chairman in the event that the status changes. The fundamental components of the item would be:

A. Software Developer

The software developers make dependable computer program mechanical status depictions and each keeps up a blockchain node. On the off chance that an unused form or computer program overhaul is discharged, a status depiction must be taken. The snapshot, along with the package and public key, is to be broadcast on the blockchain organize and marked with the developer's private key.

B. Blockchain Network

It is utilized to store trusted program specialized status depictions as a trusted, decentralized, distributed database. It incorporates total gateways and blockchain nodes. The network is overseen by the complete nodes and communicates through the P2P convention. Depictions would not be altered with within the blockchain organize and are dependable gadget following sources.

C. Blockchain Gateway

For IIoT gadgets, they give blockchain information and react to block requests. They support IIoT devices to get reliable information from the blockchain. They don't create new blocks, but new blocks are obtained, checked, and processed.

D. IIoT Devices

The key tracking modules are IIoT devices. The same observing module is run by all the gadgets, including blockchain portals and total nodes. In any case, IIoT devices do not contribute to the blockchain network like any other node. They don't hold attained blockchain records, but they store the same hash values. Block Information is sought from the blockchain gateways.

E. Monitoring Module

It chooses the program status by means of comparing gadget previews and recording record framework calls. The results will be submitted to the admin terminal. When permitted by the rules set by the admin, it'll hinder the anomalous program by itself.

F. Administrator

The Administrator gets status data that the company keeps up in genuine real-time for all IIoT gadgets, blockchain gateways, and total nodes.

VII. Conclusion and Future Work

This project intends to make a way for IoT devices to achieve industrial-grade accuracy for information transfer from remote sensing systems to AI systems using blockchain technologies. Consistently, updated security and reliability of acknowledged data inside the IoT network might be resolved on an application level. Therefore, a light-weight and effective communication protocol supporting blockchain principles was devised. This paper focuses on this relationship, examines challenges in blockchain IoT applications, and inspects the foremost appropriate work to research how blockchain could conceivably improve the IoT.

Future expansions incorporate planning a reasonable consensus algorithm for this scheme and deploying the amplified framework in reality. The sensor data quality control plans in blockchain-based frameworks can be investigated. Implementation of incentive mechanism will offer assistance proving the reliability of IIoT devices. With suitable incentives, IIoT devices, particularly power-sufficient machines, will contribute to computing power in maintaining the ledger. A world of large scale industrial collaborations where substantial amounts of data can be processed safely is envisioned.

References

[1] S. He, W. Ren, T. Zhu and K. R. Choo, "BoSMoS: A Blockchain-Based Status Monitoring System for Defending Against Unauthorized Software Updating in Industrial Internet of Things," in IEEE Internet of Things Journal, Feb 2020

[2] Y. Liu, K. Wang, K. Qian, M. Du and S. Guo, "Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach," in IEEE Internet of Things Journal, Feb. 2020

[3] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," in IEEE Transactions on Industrial Informatics, June 2019

[4] Hemsley, Kevin E., and E. Fisher, Dr. Ronald. History of Industrial Control System Cyber Incidents. United States: N. p., 2018.

[5] Anawar, Syarulnaziah and Zakaria, Nurul and Masud, Zaki and Zulkiflee, M. and Harum, Norharyati and Ahmad, Rabiah. (2019). IoT Technological Development: Prospect and Implication for Cyberstability. International Journal of Advanced Computer Science and Applications.

[6] Casino, Fran and Dasaklis, Thomas and Patsakis, Constantinos. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics.

[7] Zheng, Zibin and Xie, Shaoan and Dai, Hong-Ning and Chen, Xiangping and Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

[8] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. IEEE, 2011

[9] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead,"

[11] D. Arora, S. Ravi, A. Raghunathan, and N. K. Jha, "Hardware-assisted run-time monitoring for secure program execution on embedded processors," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2006

[12] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017

[13] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," Robotics and Computer-Integrated Manufacturing, 2018

[14] H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 International Conference on Web Information Systems and Mining (WISM), Sanya, 2010

[15] R.H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010)

[16] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks 57 (10) (2013)