A Synopsis on

Monitoring Health of IIOT Devices using Blockchain

Submitted in partial fulfillment of the requirements
of the degree of

Bachelor of Engineering

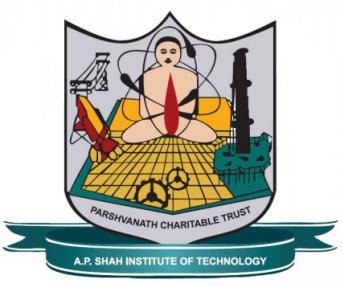
in

Information Technology

by

Rutuja Patole (17104011)
Rushika Ramane (17104064)
Soundarya Nevrekar (17104066)

Prof. Anagha Aher
Prof. Neha Deshmukh



Department of Information Technology
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI
2020-2021

CERTIFICATE

This is to certify that the Project Synopsis entitled ***"Monitoring Health of IIOT Devices using Blockchain"*** Submitted by ***"Rutuja Patole (17104011), Rushika Ramane (17104064), Soundarya Nevrekar (17104066)"*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology*** to the University of Mumbai, is a bonafide work carried out during academic year 2020-2021

(Prof. Neha Deshmukh)
Co-Guide

(Prof.Anagha Aher)
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane
Date:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

Rutuja Patole (17104011)
Rushika Ramane (17104064)
Soundarya Nevrekar (17104066)

Date:

Abstract

With the widespread applications of Internet of Things (IoT), e.g., smart city, business, healthcare, etc., the security of data and devices becomes a major concern. Although blockchain can effectively enhance the network security and achieve fault tolerance, the huge resource consumption and limited performance of data processing restrict its deployments in IoT scenarios.

IIoT devices are deployed in factories to help the manufacturing companies (e.g., automotive) gain in-depth insight into the various states of production, and thus improving production efficiency and achieving cost reductions. However, malicious code may compromise IIoT devices if either the devices are exposed to outside or unexposed inner devices are updated unauthentically. Due to their limited resources and features, it is challenging to implement strong security solutions for such embedded devices. In this article, we propose a blockchain-based software status monitoring system, called BoSMoS. The system is designed to monitor the software status of IIoT devices to detect and respond to identified malicious behaviors (e.g., intrusions).

BoSMoS takes a snapshot of the statue of monitored software and monitors its file system calls. In order to ensure the software integrity information, we use blockchain as the distributed ledger to store a snapshot of software status. The blockchain network of BoSMoS can employ different consensus algorithms. We also evaluate the performance of BoSMoS, in terms of exception response delay, resistance performance to various intrusions, and scalability. The experimental results justify that BoSMoS is practical and sound.

Introduction

In IoT scenarios, they mainly refer to the dependability of data and devices, and the capability of fault tolerance. Generally, IoT systems employ servers or clouds for storage, authorization, and certification. Such centralized strategies are highly vulnerable to denial of service, Sybil attacks or tampering. If certain vital facilities become malicious, the whole IoT network may crash. Moreover, the anonymity and heterogeneity of IoT devices cause difficulties for fault tolerance. With the field develops, the lack of security becomes a bottleneck restricting the further applications of IoT.

Fortunately, deploying blockchain in IoT to resolve such concerns receives widespread research interests. As an append-only database stored in a decentralized peer-to-peer (P2P) network, blockchain guarantees data integrity, traceability, and non tampering. Furthermore, through eliminating the reliance on certificate authorities (CA), security and fault tolerance are implemented in nontrusted environments. Although blockchain can effectively enable trustworthiness in IoT, such accomplishments require tremendous resources for support. Meanwhile, the performance of blockchain is limited due to distributed manners.

To address the above issues, various strategies are proposed, including computation offloading and authoritative entities. Nevertheless, these proposals cannot diminish all the constraints of blockchain in IoT.

Objectives

The main objective of the undertaking of this project is to create a sustainable system that boasts of

- accuracy
- monitoring
- soundness,
- security, and
- scalability.

The finished product should achieve the following goals:

- To make sure that other nodes communicating with the node are honest, they will respond to the node's request and send trusted block data it needs.
- To ensure the security of blockchain network, so as to prevent the system from being destroyed by attackers
- To ensure the accuracy of the monitoring module, false negatives and false positives can have bad impact on the system.
- To give access to multitude of nodes to join or leave the network, and their behavior will not have a bad impact on the network.

Literature Review

Almost a decade ago Satoshi Nakamoto, the unknown person/group behind Bitcoin, described how the blockchain technology, a distributed peer-to-peer linked-structure, could be used to solve the problem of maintaining the order of transactions and to avoid the double-spending problem (Nakamoto, 2008). Bitcoin orders transactions and groups them in a constrained-size structure named blocks sharing the same timestamp.

Blockchains introduced serious disruptions to the traditional business processes since the applications and transactions, which needed centralised architectures or trusted third parties to verify them, can now operate in a decentralised way with the same level of certainty. The inherent characteristics of blockchain architecture and design provide properties like transparency, robustness, auditability, and security. A blockchain can be considered a distributed database that is organised as a list of ordered blocks, where the committed blocks are immutable

In principle, a blockchain should be considered as a distributed append-only timestamped data structure. Blockchain allow us to have a distributed peer-to-peer network where non-trusting members can verifiably interact with each without the need for a trusted authority. To achieve this one can consider blockchain as a set of interconnected mechanisms which provide specific features to the infrastructure, as illustrated in Figure. At the lowest level of this infrastructure, we have the signed transactions between peers. These transactions denote an agreement between two participants, which may involve the transfer of physical or digital assets, the completion of a task, etc. At least one participant signs this transaction, and it is disseminated to its neighbours. Typically, any entity which connects to the blockchain is called a node. However, nodes that verify all the blockchain rules are called full nodes. These nodes group the transactions into blocks and they are responsible to determine whether the transactions are valid, and should be kept in the blockchain, and which are not.

This is actually the goal of the second Consensus layer. Depending on the blockchain type, different Consensus mechanisms exist. The most wellknown is the Proof-of-work (PoW). PoW requires solving a complicated computational process, like finding hashes with specific patterns, e.g. a leading number of zeroes, to ensure authentication and verifiability.

PoW requires solving a complicated computational process, like finding hashes with specific patterns, e.g. a leading number of zeroes , to ensure authentication and verifiability. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e., their mining power), Proof-of-Stake (PoS) protocols split stake blocks proportionally to the current wealth of miners. This way, the selection is fairer and prevents the wealthiest participant from dominating the network. Many blockchains, such as Ethereum are gradually shifting to PoS due to the significant decrease in power consumption and improved scalability.

Current literature categorises blockchain networks in several ways. These categories are formed according to the network's management and permissions as public, private and federated. In public blockchains (permissionless) anyone can join as a new user or node miner. Moreover, all participants can perform operations such as transactions or contracts. In private

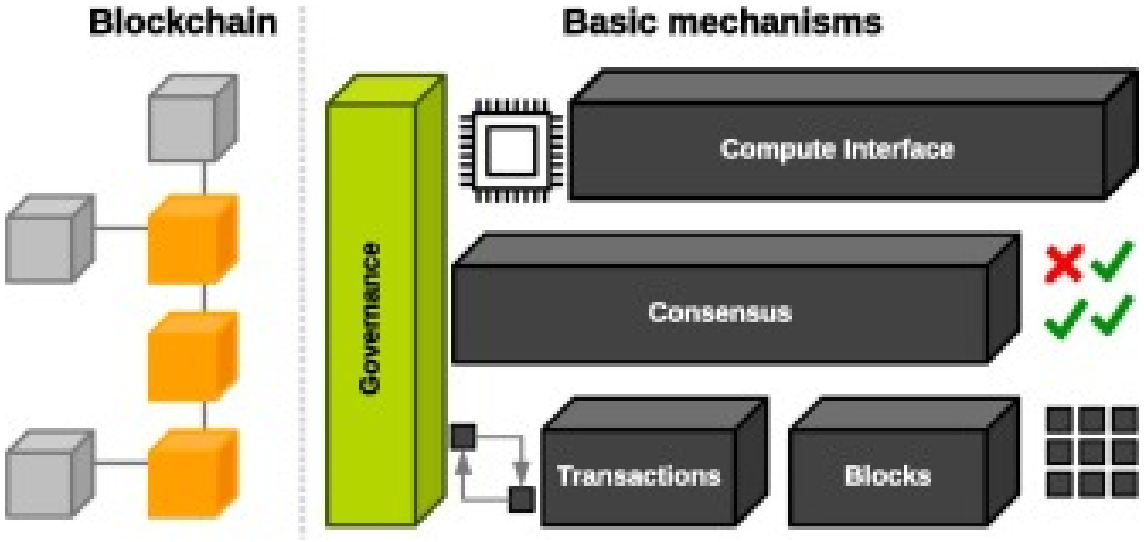


Figure 1: Blockchain Basic Mechanisms

blockchains; which along with the federated belong to the permissioned blockchain category, usually, a whitelist of allowed users is defined with particular characteristics and permissions over the network operations. Since the risk of Sybil attacks is almost negligible there private blockchain networks can avoid expensive PoW mechanisms. Instead, a wider range of consensus protocols based on disincentives could be adopted. A federated blockchain is a hybrid combination of public and private blockchains. Although it shares similar scalability and privacy protection level with private blockchain, their main difference is that a set of nodes, named leader nodes, is selected instead of a single entity to verify the transaction processes.

1) **BoSMoS: A Blockchain-based Status Monitoring System for Defending against Unauthorized Software Updating in Industrial Internet of Things.**

Author: Sen He, and Wei Ren, Tianqing Zhu, Kim-Kwang Raymond Choo

Approaches to consensus:

There are two main consensus algorithms, proof of work (PoW) and proof of stake (PoS). A proof of work consensus entails the validation of a block by nodes showing that they have done some work and come to an agreement of the results. The work is usually a set of complex calculations whereby nodes agree on the correct answer before appending a block to the Blockchain. This is done by miners and requires a lot of computation power. In the proof of stake consensus, nodes prove that they own stake on the Blockchain thus approve of the addition of the new block to the Blockchain. This is done by owners of a stake in the blockchain and is not necessarily resource-intensive in terms of computation power.

The practical byzantine fault tolerance algorithm (PBFT), which is used to establish consensus in blockchain systems, is only one of those potential solutions. Three examples of blockchains that rely on the PBFT for conses are Hyperledger, Stellar, and Ripple. Very

roughly and without explaining the whole algorithm (which would take a multiple page research paper), what the PBFT does is as follows: Each 'general' maintains an internal state (ongoing specific information or status). When a 'general' receives a message, they use the message in conjunction with their internal state to run a computation or operation. This computation in turn tells that individual 'general' what to think about the message in question. Then, after reaching his individual decision about the new message, that 'general' shares that decision with all the other 'generals' in the system. A consensus decision is determined based on the total decisions submitted by all generals.

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

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

2) **Tornado: Enabling Blockchain in Heterogeneous Internet of Things through A Space-Structured Approach**

Author: Yinqiu Liu, Kun Wang, Kai Qian, Miao Du, and Song Guo

A novel high-performance blockchain system with space-structured ledger architecture called Tornado to enable blockchain in IoT. Specifically, Tornado accommodates IoT devices of different configurations and improves the scalability in heterogeneous and resource-constrained IoT networks.

To overcome the heterogeneity, we design an anti-heterogeneity and high-performance consensus algorithm named collaborative proof of work (Co-PoW) based on the collaborations among IoT devices. CoPoW introduces parallel workflows, which support both wimpy and brawny devices and effectively improve the network throughput.

To exploit the resource efficiency, we present a novel space structured greedy heaviest-observed subtree(S2 GHOST) protocol. During S2 GHOST, the dynamic weight assignment (DWA) contributes to measure the trustworthiness of data and devices.

We also develop a prototype of Tornado. Experiments in a heterogeneous P2P network of 50 peers illustrate that Tornado can achieve a peak throughput of 3464.76 TPS.

Moreover, the performance of power efficiency, propagation latency, and scalability also gets significantly optimized.

Drawbacks: Differentiated mining difficulty, Parallel workflows.

Benefits: Enhanced connectivity with partners, customers, suppliers

3) **Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism**

Author: Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, Peng Zeng

We propose a credit-based proof-of-work (PoW) mechanism for IoT devices, which can guarantee system security and transaction efficiency simultaneously. In order to protect sensitive data confidentiality, we design a data authority management method to regulate the access to sensor data. In addition, our system is built based on directed acyclic graph (DAG)-structured blockchains, which is more efficient than the satoshi-style blockchain in performance. We implement the system on Raspberry Pi, and conduct a case study for the smart factory. Extensive evaluation and analysis results demonstrate that credit-based PoW mechanism and data access control are secure and efficient in IIoT.

They propose a credit-based proof-of-work (PoW) mechanism which can guarantee system security and transaction efficiency simultaneously. They also designed a data authority management method to regulate access to sensor data to protect the confidentiality of sensitive data.

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

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.

While blockchain applications are being widely deployed, many issues have yet to be addressed. By doing so, blockchains will become not only more scalable and efficient but more durable as well. The features they offer are not unique if judged individually, and the bulk of the mechanisms they are based on are well-known for years. However, the combination of all these features makes them ideal for many applications justifying the intense interest by several industries.

As blockchains become more mature, their applications are expected to penetrate more industries/domains than the ones covered in our survey. However, while many try to propose blockchains as a panacea and an alternative to databases, this is far from true. As already discussed, there are many scenarios where traditional databases should be used instead. Moreover, we identified the individual characteristics that are mostly required per each application domain. This facilitates the choice of the proper blockchain and the corresponding mechanisms to tailor the blockchain to the actual needs of the application.

Problem Definition

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, 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).

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.

With our project, we intend to do exactly that by creating a reliable product that makes use of Blockchain technology.

Proposed System Architecture/Working

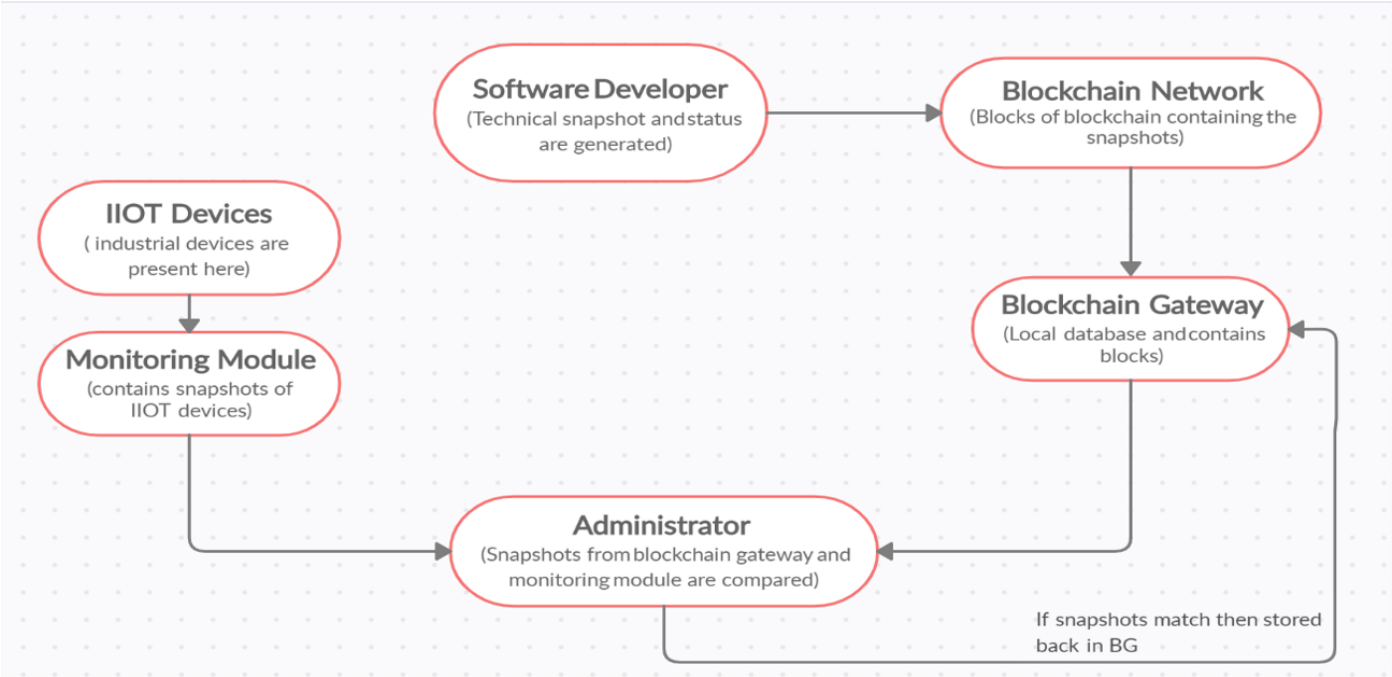


Figure 2: Proposed System Working

The product protects the integrity of the software by monitoring the status of it. The software's status information contains software integrity information and software related file information. By comparing trusted software status snapshots, the system can determine the software status and will alert the administrator if the status changes. The main elements of the product would be:

- Software Developer

  Trusted software technical status snapshots are generated by the software developers and each of them maintains a blockchain node. If a new version or update of the software is released, a snapshot of the status is to be taken. The snapshot is to be broadcasted in the blockchain network and signed with the private key of the developer, along with the package, and public key.

- Blockchain Network

  It is used as a trusted decentralized distributed database to store trusted software technical status snapshots. It contains full nodes and blockchain gateways. The full nodes maintain the network and communicate via P2P protocol. Snapshots in the blockchain network cannot be tampered with and are credible references for monitoring software.

- Blockchain Gateway

  They provide blockchain data for IIoT devices and respond to block requests. They help IIoT devices to obtain trusted data from the blockchain. They do not create new blocks but receive, verify, and store new blocks.

- IIoT Devices

  IIoT devices are main monitoring objects. All devices, including blockchain gateways and full nodes, run the same monitoring module. However, unlike other nodes, IIoT devices are not part of the blockchain network. They do not keep complete blockchain data but store only hash values of the same. They request block data from the blockchain gateways.

- Monitoring Module

  It determines the software status by comparing software snapshots and monitoring file system calls. The results are sent to the administrator terminal. It can interrupt abnormal software by itself if permitted by the rules set by the administrator.

- Administrator

  Administrator receives status information of all IIoT devices, blockchain gateways and full nodes maintained by the organization in real time.

Design and Implementation

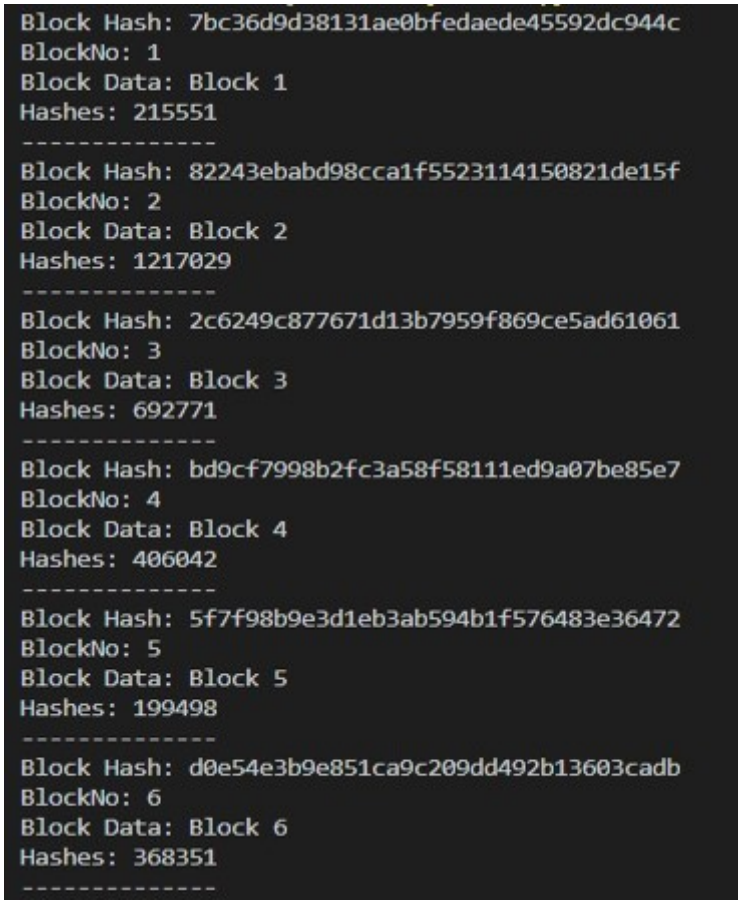


Figure 3: Blockchain Created

This snapshot demonstrates a chain of blocks which contain information. The first block in the chain is called the Genesis block. Each new block in the chain is linked to the previous block.A block also has a hash. It can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

Each Block has

- Data
- Hash
- Hash of the previous block

Summary

This project aims to create a method for Internet-of-Things-devices to achieve industrial grade reliability for information transfer from wireless sensor systems to production systems using blockchain technologies. An increased security and reliability of submitted data within the sensor network could be achieved on an application level. Therefore, a lightweight, high-level communication protocol based on blockchain principles was designed.

Blockchain has emerged as a key technology that will transform the way in which we share information. Building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IoT among them.

This paper focuses on this relationship, investigates challenges in blockchain IoT applications, and surveys the most relevant work in order to analyze how blockchain could potentially improve the IoT.

References

[1] "BoSMoS: A Blockchain-based Status Monitoring System for Defending against Unauthorized Software Updating in Industrial Internet of Things", https://ieeexplore.ieee.org/document/8869742

[2] "Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism", https://ieeexplore.ieee.org/document/8661654

[3] "Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach", https://ieeexplore.ieee.org/document/8906043

[4] "A systematic literature review of blockchain-based applications: Current status, classification and open issues", https://researchgate.net/publication/329136952

[5] "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", https://researchgate.net/publication/318131748

[6] "IoT Technological Development: Prospect and Implication for Cyberstability", https://www.researchgate.net/publication/331474208

[7] "Hackers are attacking power companies, stealing critical data: Here's how they are doing it", https://www.zdnet.com/article/hackers-are-attacking-power-companies-stealing-critical-data-heres-how-they-are-doing-it/

1 Publication

Paper entitled **"Monitoring Health of IIOT Devices using Blockchain"** is aimed to be presented at **"2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)"** by **"Rutuja Patole, Rushika Ramane, Soundarya Nevrekar".**