A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory

Seoul National University of Science and Technology
Computer Science and Engineering

Young Hun Lee
2019-05-21

INDEX

Abstract

- Through IIoT, which is the use of Internet of Things technologies in manufacturing, smart factories are progressing, but the number of nodes and the size of networks are constantly increasing.

- To provide effective support for IIoT system, propose the distributed network with Blockchain architecture.

- First, Analyze the problems of the traditional IIoT architecture and summarize the improvements.

- Second, Introduce the security and privacy model to adopt block-chain based architectures.

- Finally, Design the data interaction process and the algorithms of the architecture and use an automatic production platform to discuss the specific implementation.

- Result of the experiment shows with compare traditional IIoT system.

1. Introduction

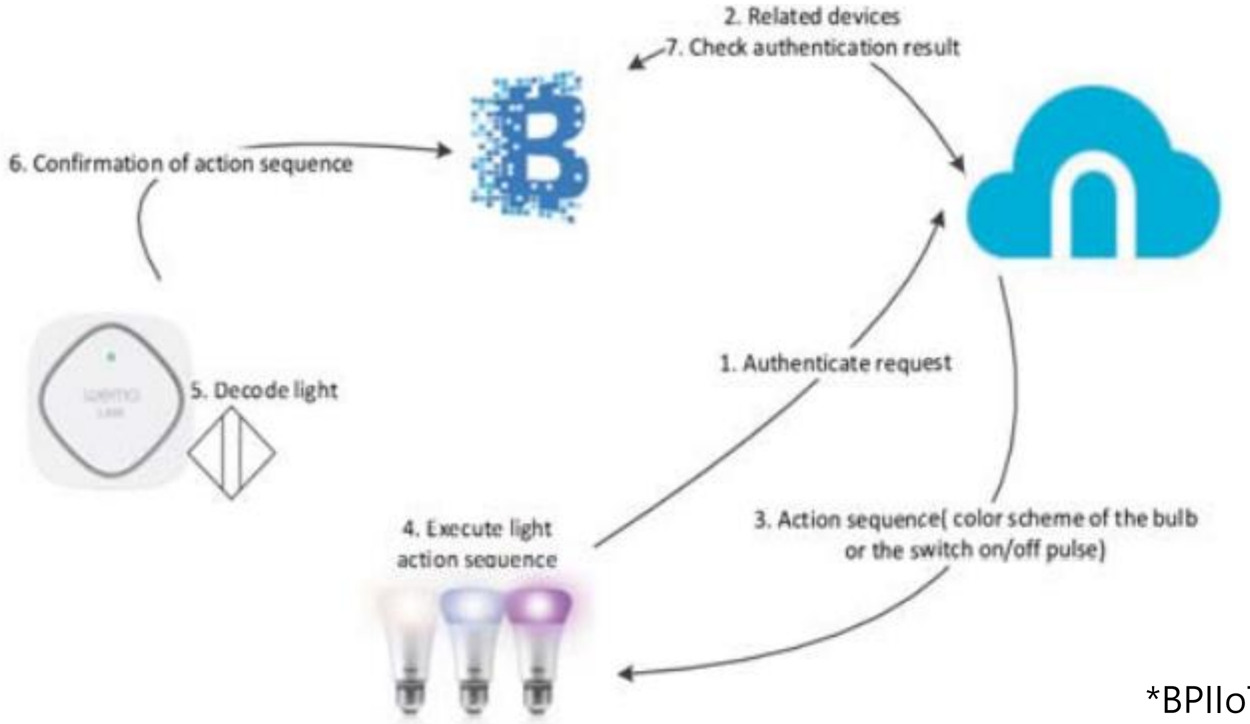
IIoT

- Forth industrial revolution technology(Big Data, Cloud Computing, Cyber Physical System) make promoted to industry to a new level.
- Industrial Internet of Things(IIoT) makes collision and fusion of the data and connect the unconnected things in the industry.
- IoT platforms serving the smart factories breaking the information isolated island problem of the equipment and realizing the integration of various equipment in a smart factory.
- However, due to the limitations of the IIoT architecture and vulnerabilities of the underlying equipment, a large amount of critical security and private data is very vulnerable to the attacks.
- The authors revealed that malware, malicious scripts, etc., could be easily sneaked into various equipment at the application level, which could violate users' private data without users' permission and causing many problems.

1. Introduction

Blockchain

- Nakamoto proposed a peer-to-peer digital currency system named the Bitcoin.
- There's Two-factor authentication scheme based on the Blockchain and with Smart Contract(*BPIIoT) technology to ensure data security.[10] (Pin code, Blockchain ➔ able to distinguish a home IoT device from the malicious device)
- These methods created to improve the security on the equipment level and realize data exchange without trusted intermediaries.



[Two-Factor authentication scheme]

*BPIIoT(Blockchian-Based Platform Architecture for Industrial IoT)

1. Introduction

Drawbacks of existing research

1) real-time capability not deep consideration in industrial environment
2) relative studies is small → real industry is not completely independent system
3) open source platforms → may cause unpredictable problems

Main contributions of this paper

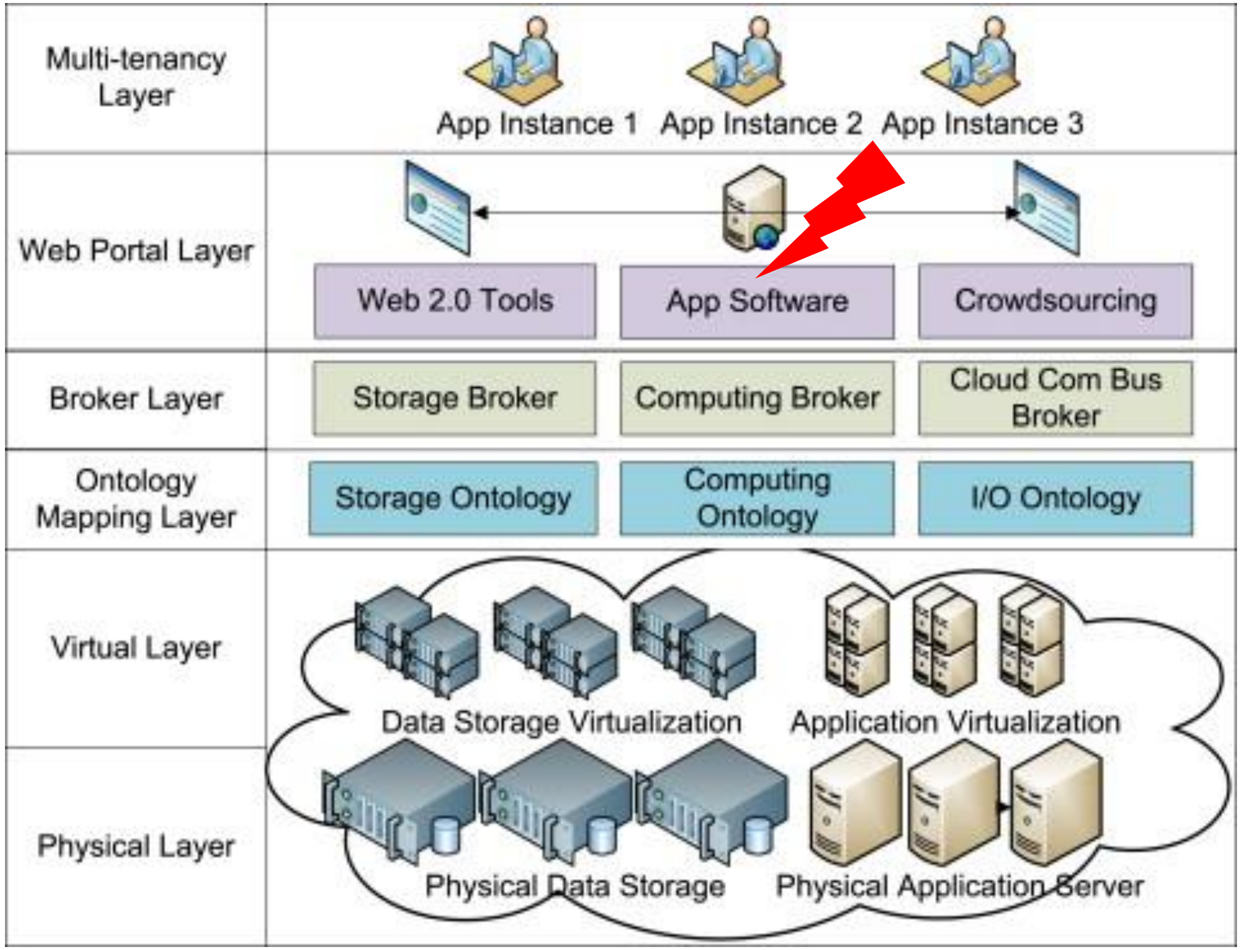
1) Combine the Blockchain technology and Bitcoin design ➔ privatized, lightweight, easily expanded..

2) A security and privacy model is introduced to help analyze the key aspects of the architecture

3) Whitelist mechanism and asymmetric encryption mechanism used ➔ improve the security and privacy,

2. Blockchain-Based IIoT Architecture For Smart Factory

Current Smart Factories



[Current Smart Factories scheme]

- **Cloud-Based Manufacturing(CBM)** [14]

- Users to access the shared pool of manufacturing resources anytime and anywhere using Cloud.
- Rapid configuration and management of resources can be realized with the minimal work.

- But, Centralized architecture is very fragile.
- If central node is damaged, all services will be suspended.

- Proposed decentralized system with nodes supervising each other mutually.

2. Blockchain-Based IIoT Architecture For Smart Factory

Proposed Blockchain-Based IIoT architecture

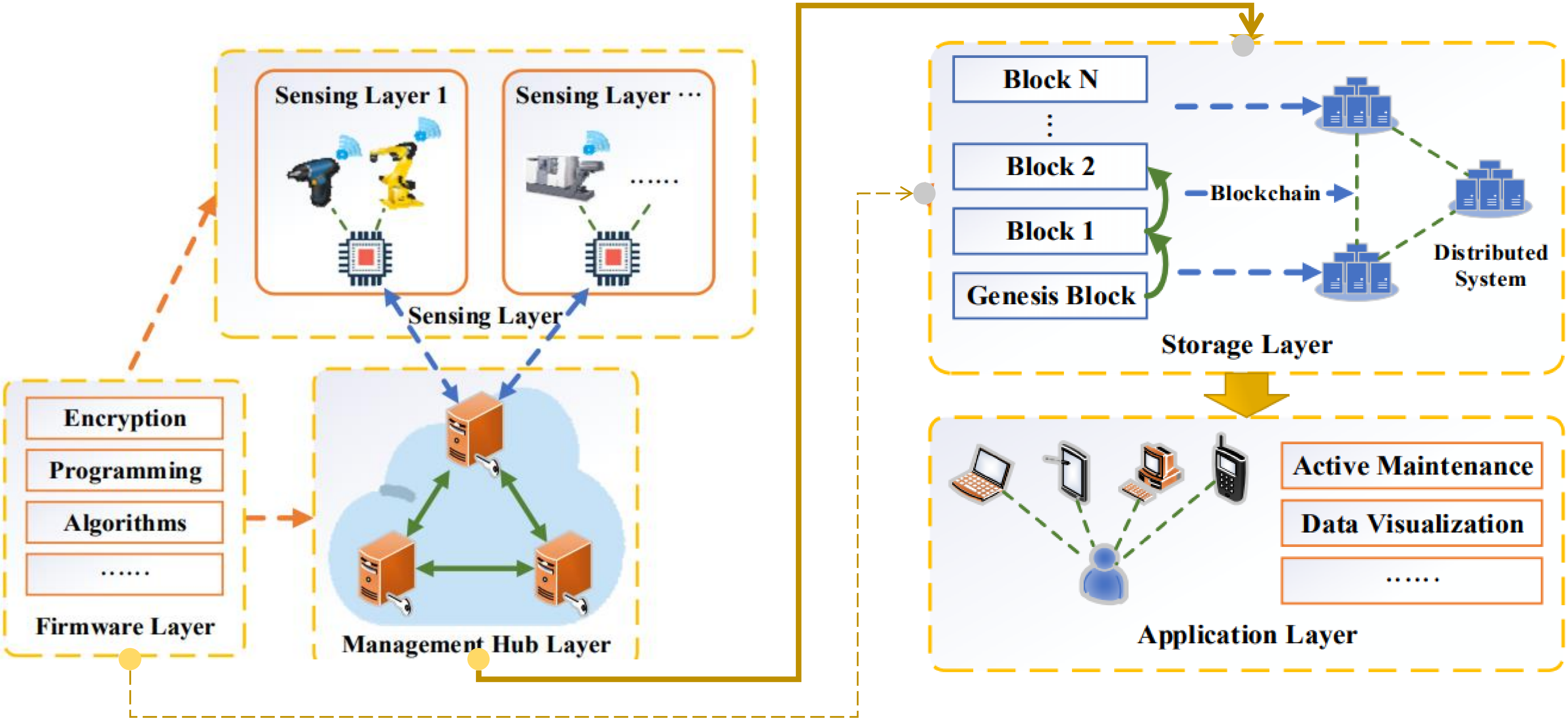
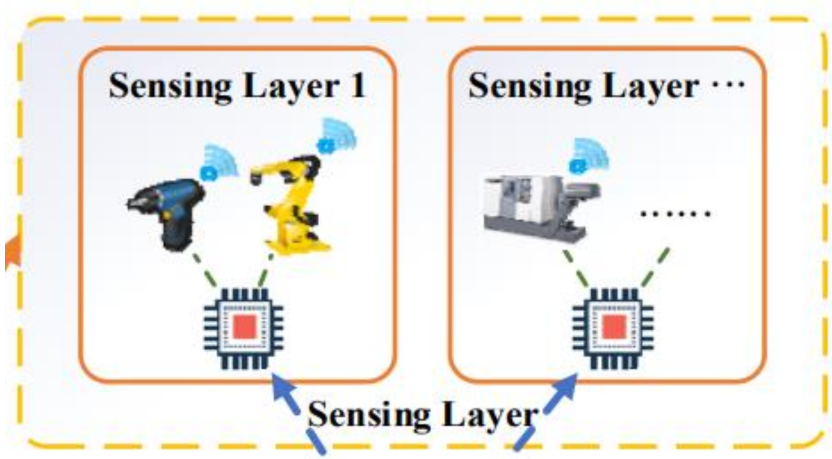


Fig. 1. The Blockchain-Based IIoT architecture for a smart factory.

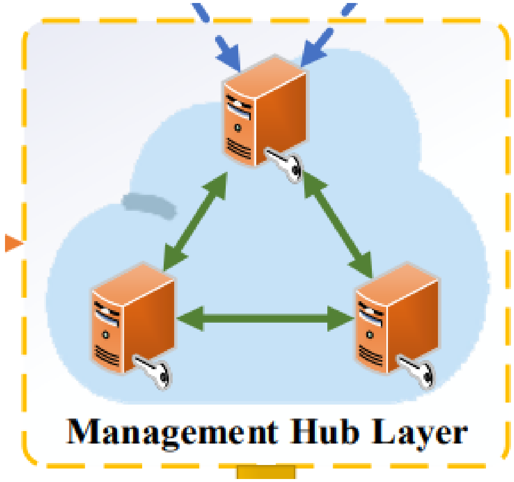
2. Blockchain-Based IIoT Architecture For Smart Factory

1) Sensing layer



- Various types of sensors and at least one microcomputer with a certain computing power.
- Obtain information on various equipment, and preprocesses the collected data

2) Management Hub layer

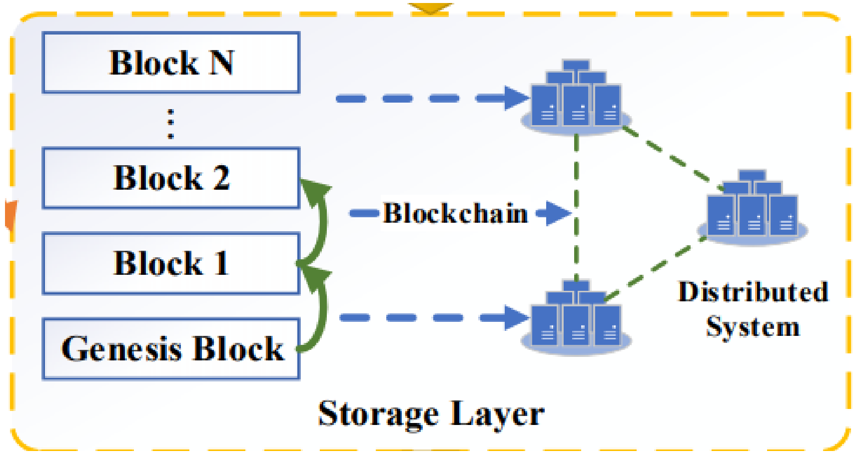


- parses the uploaded data
- encrypts the data
- packages the data to generate blocks
- stores it in the database

- Integrate and manipulate different equipment
- Respond to the users' requests in real time

2. Blockchain-Based IIoT Architecture For Smart Factory

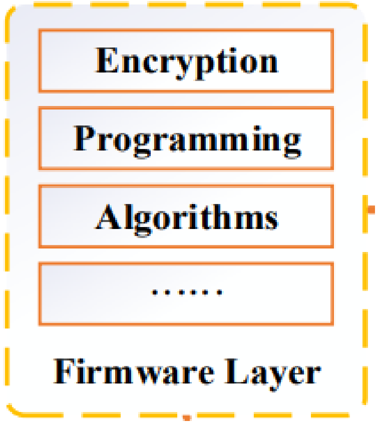
3) Storage layer



- A data center
- Keeping the encrypted
- Stored in a distributed form
- Synchronized at a certain interval

- Tamper-resistant data and blockchain records.

4) Firmware layer



- Implementation technologies

- data acquisition
- distributed algorithms
- data storage technology

- To make each layers effective

- Involves the underlying implementation technologies to connect each layer

2. Blockchain-Based IIoT Architecture For Smart Factory

5) Application layer

- Real-time monitoring
- Failure prediction, etc.

2. Blockchain-Based IIoT Architecture For Smart Factory

A. Division of the architecture

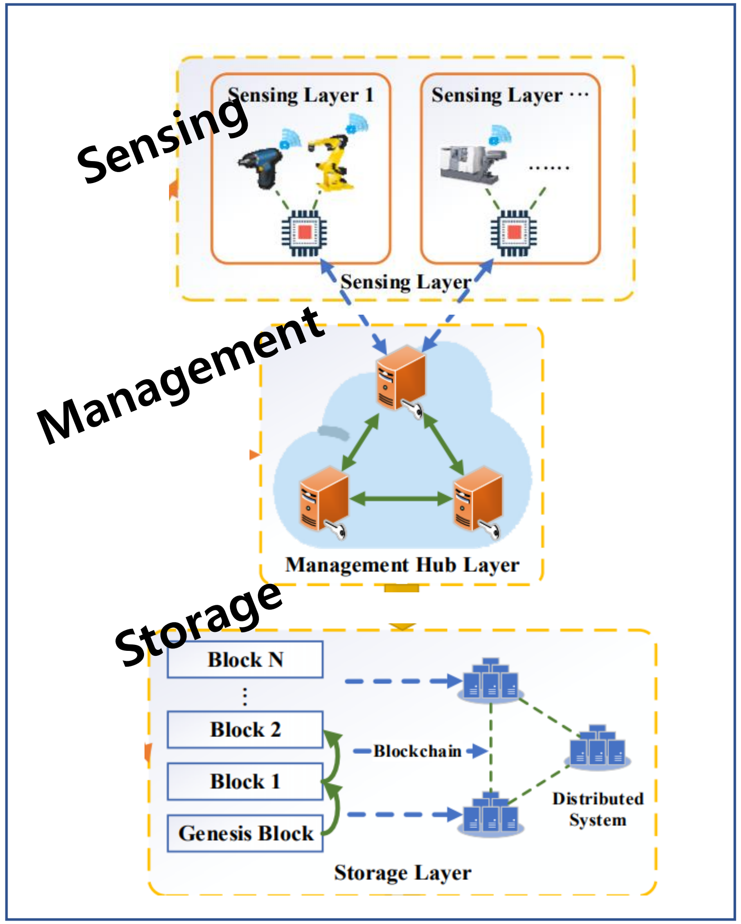
B. Management hub layer

C. Private blockchain

2. Blockchain-Based IIoT Architecture For Smart Factory

A. Division of the architecture

- Architecture is divided into the **intranet** and the **extranet**



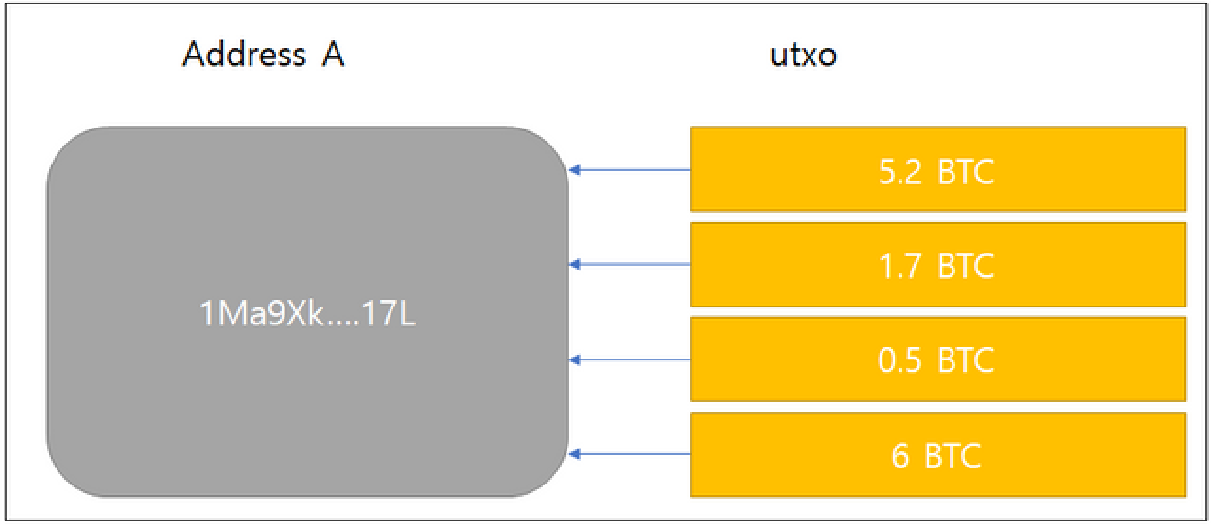
[Intranet]

- **Limitation on Computing power**
  → No Peer-to-Peer (P2P) network
- **Managed by the Management hub**
  → The data of each equipment node need management.
- **Permission**
  → If equipment node needs different operations, needs to request permission from the management hub.
- **Different from Bitcoin Using UTXO(Unspent Transaction Output)**
  → For anonymity and security
  → Nodes's number and authority of participating state record directly

2. Blockchain-Based IIoT Architecture For Smart Factory

A. Division of the architecture(Con't)

- UTXO



[UTXO]

- **A wallet with many address**
  → Each UTXO is similar with 'Check Draft'

- **Generate of UTXO**
  → When some one send BTC to your wallet, then generated utxo, endorsed address.

- **Expiration of UTXO**
  → When you send BTC to other wallet with more than each UTXO.

- So, in the IIoT system, Considering the diversity, complexity etc

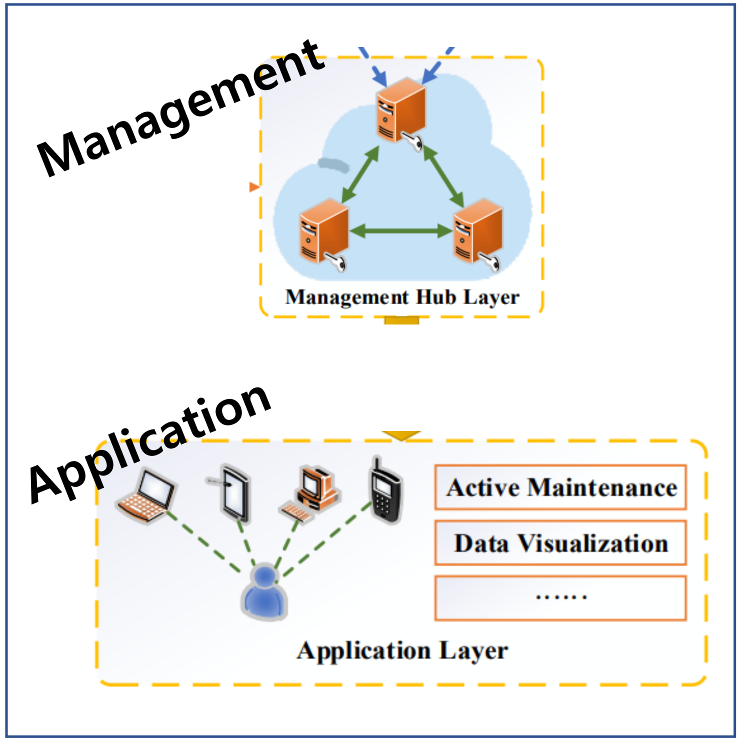
→ Record the state of sensors directly is more reduce the overhead.

https://steemit.com/coinkorea/@goldenman/utxo

2. Blockchain-Based IIoT Architecture For Smart Factory

A. Division of the architecture

- Architecture is divided into the **intranet** and the **extranet**



[Extranet]

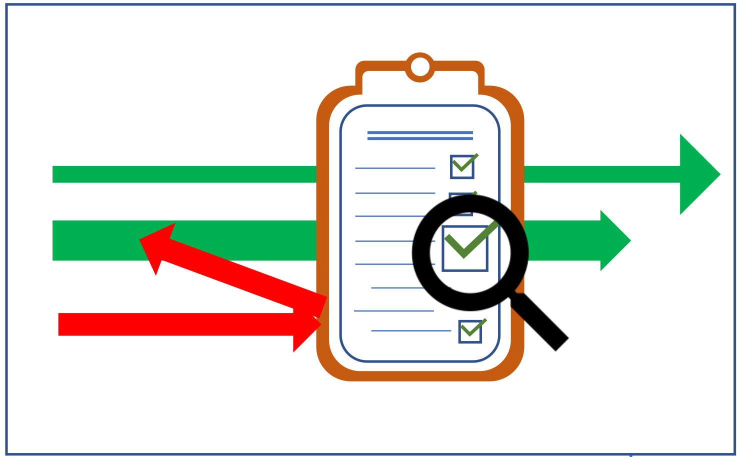
- **Need to connect Internet**
  → Consider connection, algorithms, tools.

- **Quality of Service(QOS)**
  → Users can customize diverse management their own needs.

2. Blockchain-Based IIoT Architecture For Smart Factory

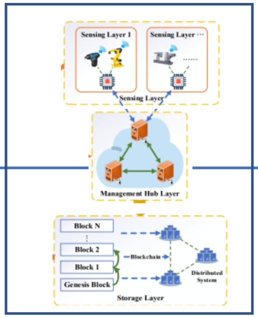
A. Division of the architecture

- Ensuring data security and privacy (**Whitelist** and Dynamic authentication)

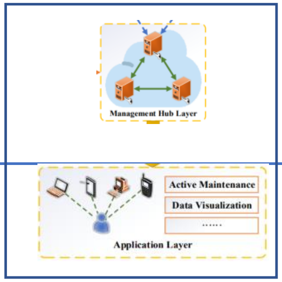


[Whitelist]

- **Determines the right to access or deny**
- **Benefits**
  → Quickly verify the access traffic
  → Filter the malicious traffic
  → Providing fast and convenient security and privacy



[Intranet]

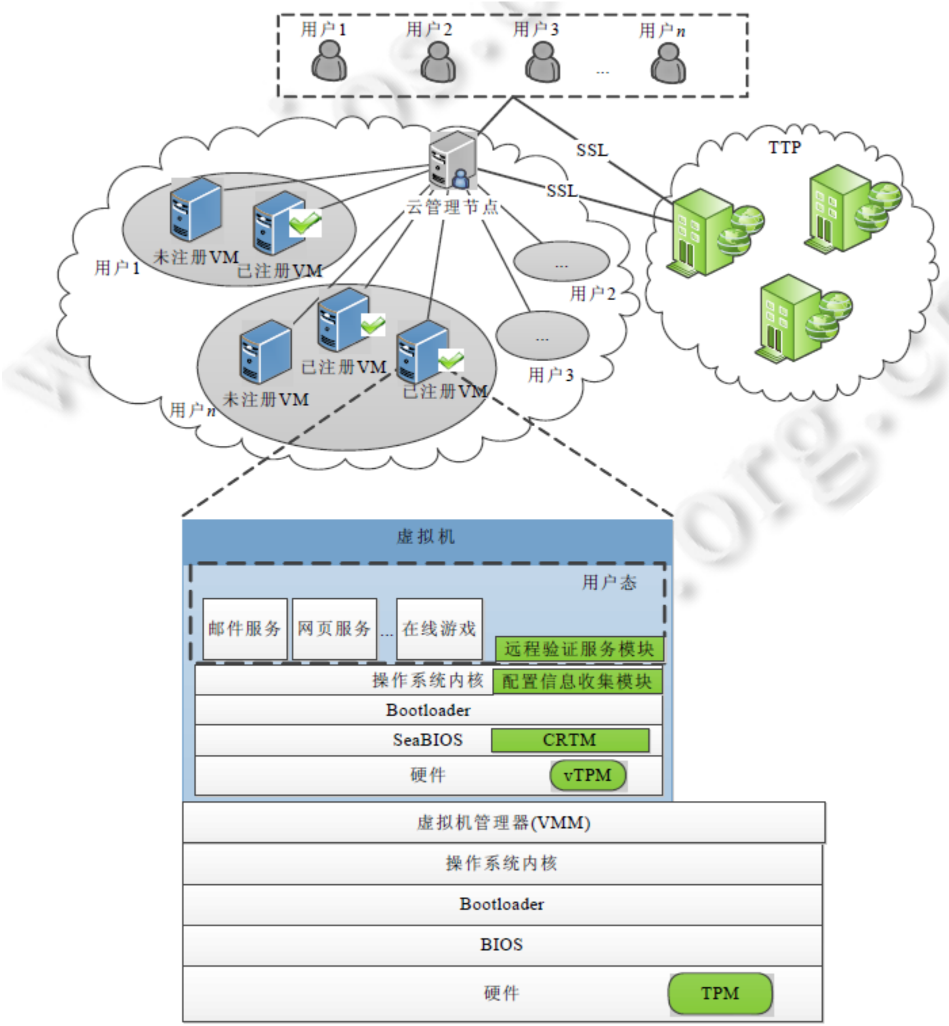


[Extranet]

2. Blockchain-Based IIoT Architecture For Smart Factory

A. Division of the architecture

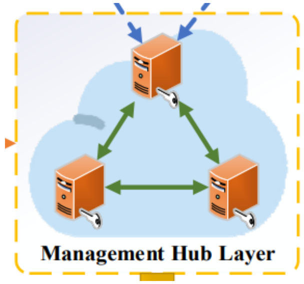
- Ensuring data security and privacy (Whitelist and **Dynamic authentication[18]**)



[Dynamic authentication in cloud systems]

- **Time-limited**
  → Permission and the Proof of Work (PoW) need to be re-verified

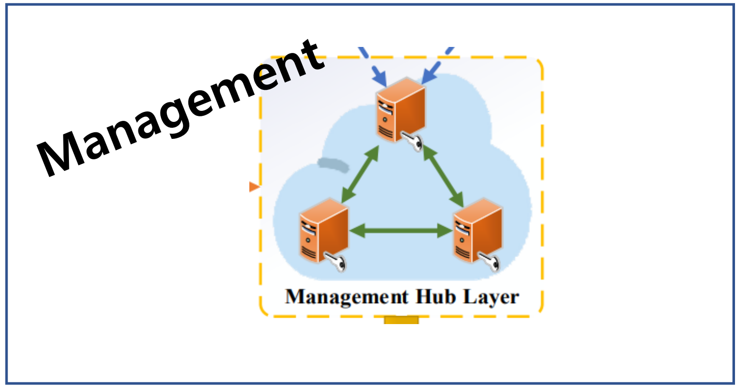
- **Self-running algorithm**
  → If user maintain access permission, he need to re-verifying



2. Blockchain-Based IIoT Architecture For Smart Factory

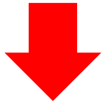
B. Management hub layer

- Special node responsible for recording blocks



[responsible for recording blocks]

- **PoW, PoS, PBFT* algorithms needed**
  → To ensure that all management hubs are trusted
- **Mathematically Problem solving**
  → Solving makes the malicious operation costly.



- **Problem of Reward**
  → Computational resources
  → Scalability

https://steemit.com/crypto/@energist/blockchain-study-pbft-practical-byzantine-fault-tolerance

2. Blockchain-Based IIoT Architecture For Smart Factory

B. Management hub layer

- Special node responsible for recording blocks(Con't)

- Need more attention to the **utilization of resources** and the **efficiency of data interaction** in IIoT System.

- Initially, all nodes trusted in IIoT System.

- So, no need reward system like on blockchain, Use management hubs for data management.

→ Apply Statistical Process Control (*SPC) or other comparison algorithms to make PoW.

→ By using data like eigenvalues such as control limits, average values data.

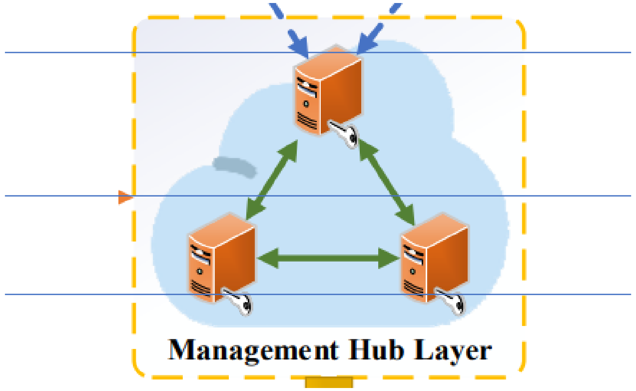
*Statistical Process Control : 통계적 공정관리
→management method that manages the process by statistical method in order to stably produce a product that can pass the quality standard

2. Blockchain-Based IIoT Architecture For Smart Factory

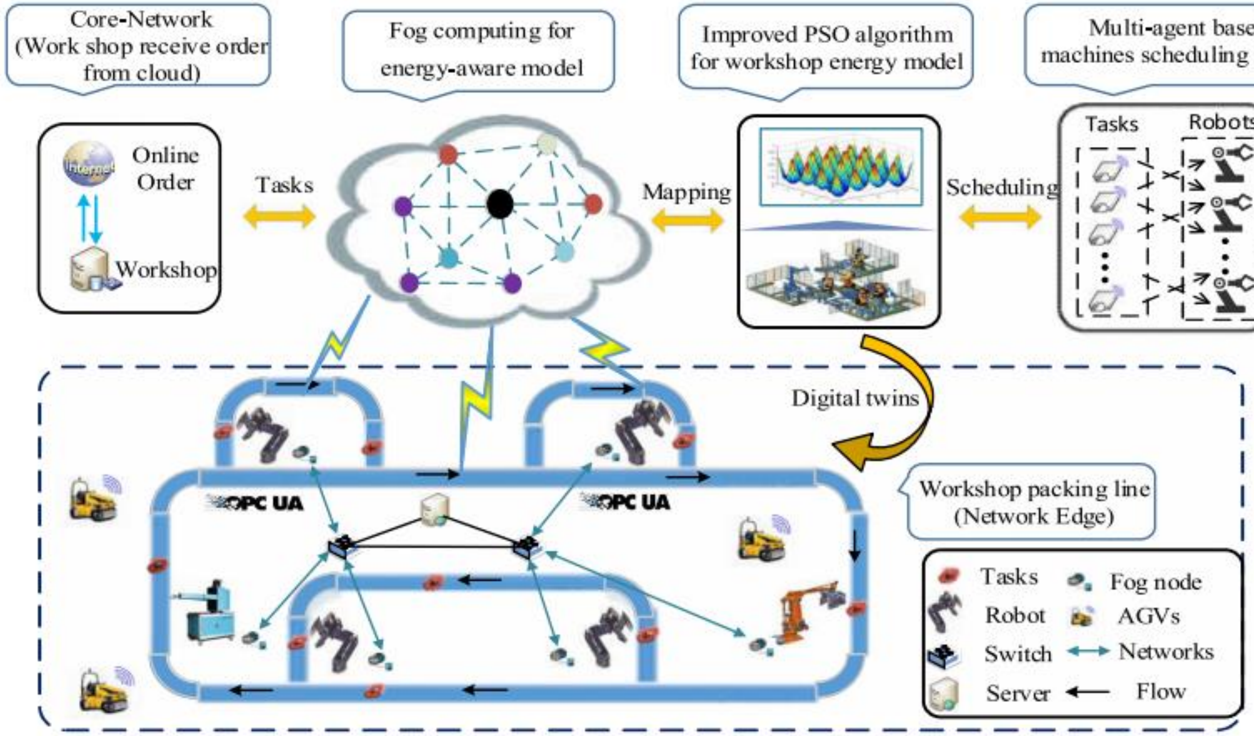
B. Management hub layer

- Special node responsible for recording blocks(Con't)

- Using multiple management hubs instead of cloud system.[22]
- Make hubs partially decentralized system



Simplify



[Architecture of fog computing for ELBS in smart factory] [22]

2. Blockchain-Based IIoT Architecture For Smart Factory

C. Private blockchain

- Unique block structure

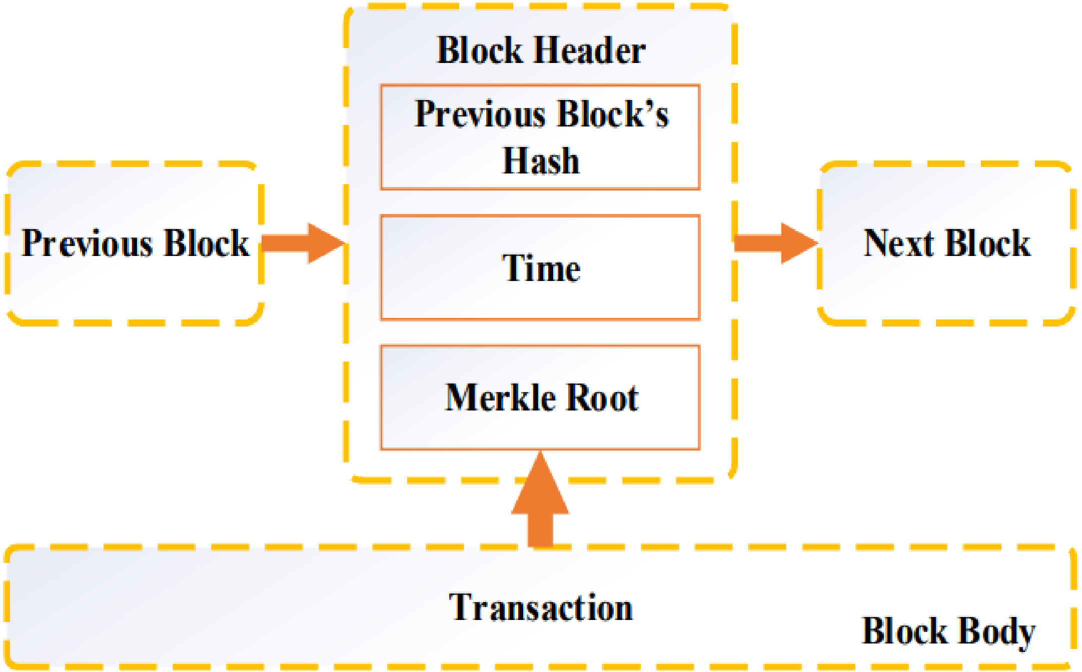


Fig. 2. Block structure.

- Traced and the data interaction can be highly protected.

2. Blockchain-Based IIoT Architecture For Smart Factory

C. Private blockchain

- Unique block structure(Con't)

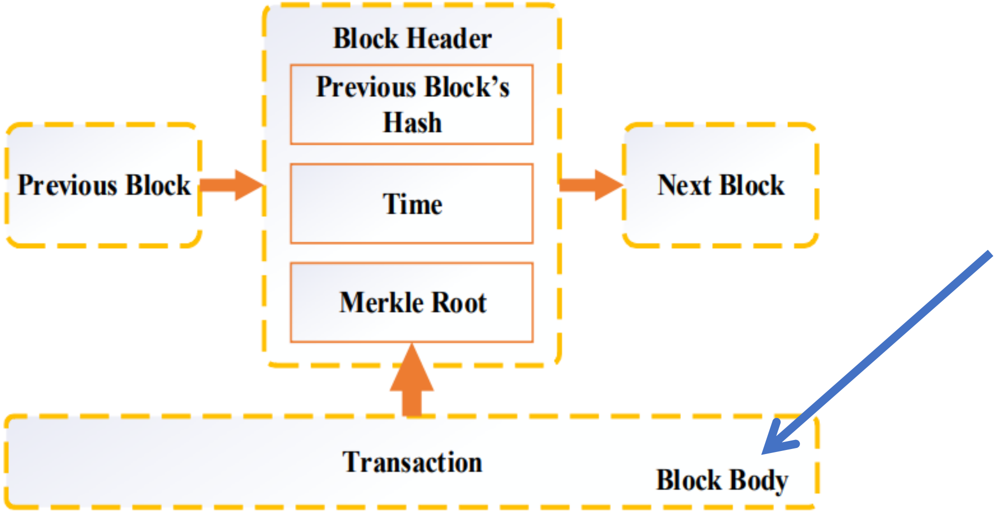


TABLE I
TRANSACTION IN THE BLOCK BODY

Address	Request	Merkle Root	Action
1	Store	1	Deny
2	Read	2	Deny
3	Control	3	Deny

- Example of Block body information (request address, the request content..)

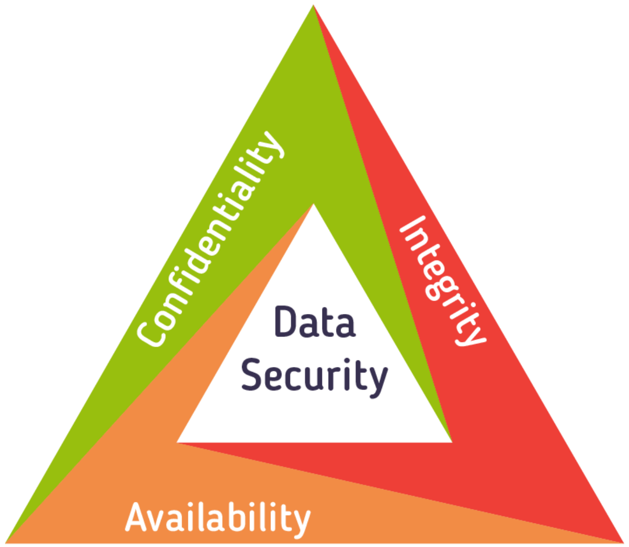
- For good privacy using SHA256 and Elliptic Curve Cryptography (ECC) algorithm.

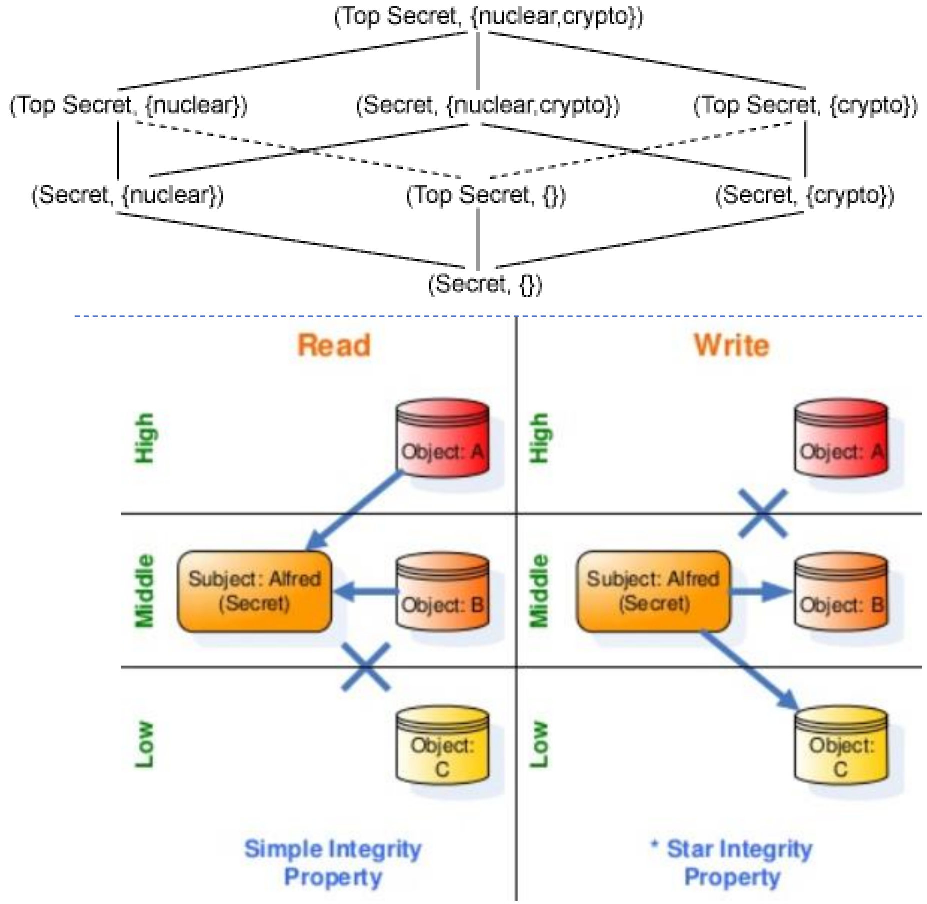
- Integrity : SHA256
- Encryption : ECC → Make public and private keys

https://m.blog.naver.com/aepkoreanet/221178375642

3. DATA SECURITY AND PRIVACY MODEL

CIA requirements





[BLP and Biba model]

- Three major requirements = Confidentiality, Integrity, Availability (CIA)
- Combining Bell-La Padula (BLP) model with Biba model

https://hyunhong.tistory.com/entry/%EC%A0%95%EB%B3%B4%EB%B3%B4%EC%95%88Information-Security%EC%9D%B4%EB%9E%80

https://themeat.tistory.com/70

3. DATA SECURITY AND PRIVACY MODEL

Access Control

$$S = \{s_1, s_2, s_3, \cdots, s_n\}$$
$$O = \{o_1, o_2, o_3, \cdots, o_n\}$$
$$\mu = \{M_1, M_2, M_3, \cdots, M_n\}$$
$$A = \{w, r, c\}$$
$$L = \{l_1, l_2\}$$

TABLE II
ACCESS CONTROL LIST

Subject \ Object	l_1	l_2
l_1	$\{w, r, c\}$	$\{r, c\}$
l_2	$\emptyset$	$\{w, r, c\}$

- S : set of subjects
- O : set of objects
- μ : set of access matrixes
- A : set of access attributes
- w : storing
- L : different privilege levels

$$V = S \times O \times A \times \mu \times L$$

TABLE III
DEFENSIVE MECHANISMS

Subject \ Object	Equipment nodes	Management hubs	User nodes
Equipment nodes		Whitelist, PoW, Dynamic verification, Merkle Root	
Management hubs			
User nodes		Whitelist, Dynamic verification, Asymmetric encryption, Merkle Root	

[formula to determine if the current state is safe]

4. DATA INTERACTION PROCESS DESIGN

Prevent the possible attacks and threats

- Difference IoT architecture, but architecture derived from the IoT.

- Possible attacks and threats

- Leakage of permissions
- DoS or DDoS
- Network sniffer
- Compromised-key attack and invasion

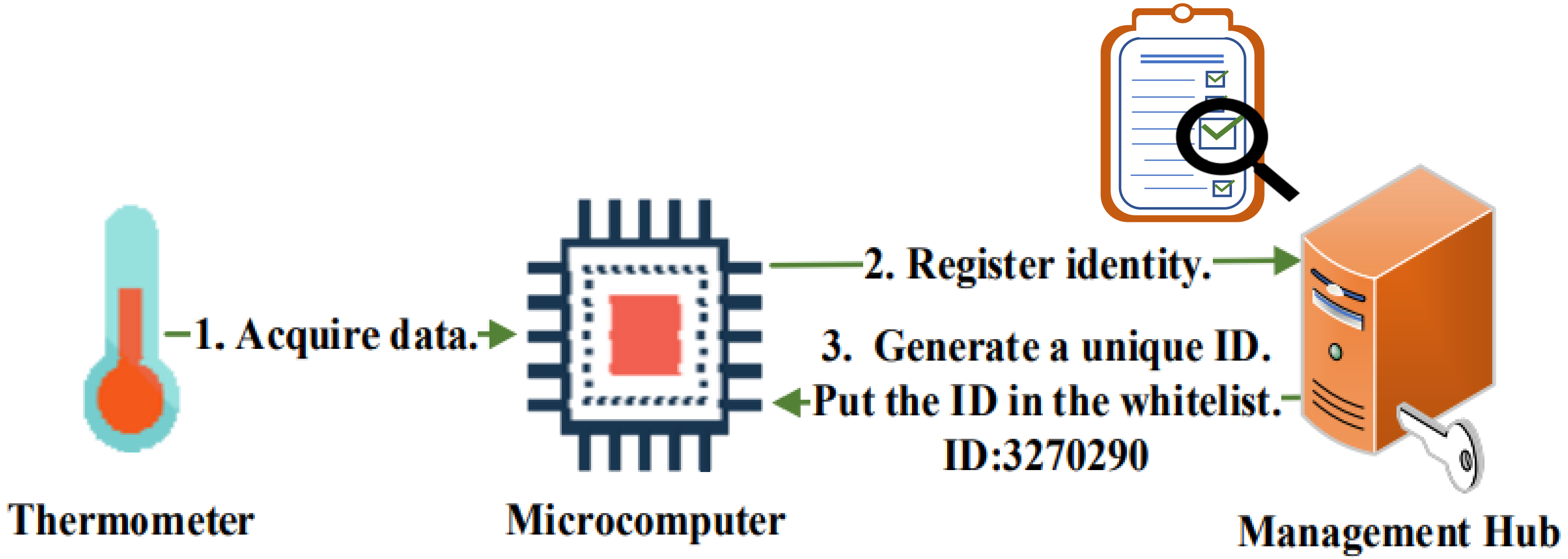
TABLE IV
NOTATION

Notation	Definition
whitelist[1...*a*]	Record trusted ID. There are backups in each management hub
mComputer[1...*b*]	Record all microcomputers in the system
mHub[1...*c*]	Record all management hubs in the system
requestReceived	Indicate if data arrives
users[1...*d*]	Record all users in the system
time	Record the running time in the system

4. DATA INTERACTION PROCESS DESIGN

Prevent the possible attacks and threats(Con't)

- Example (temperature collection)

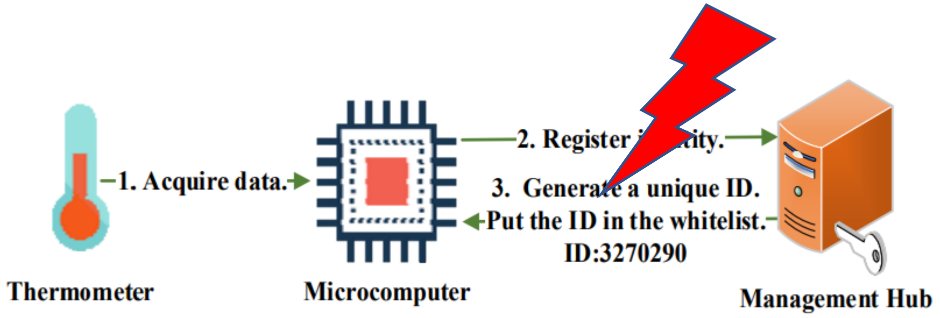


[Fig. 3. Data preparation flowchart.]

4. DATA INTERACTION PROCESS DESIGN

Prevent the possible attacks and threats(Con't)

- Example (temperature collection)



- When attacks of stealing and abusing node permissions, design two defense mechanisms.

1. Sensing Layer

➔ whitelist mechanism
➔ the dynamic verification mechanism
➔ PoW consensus algorithm

'Stable'

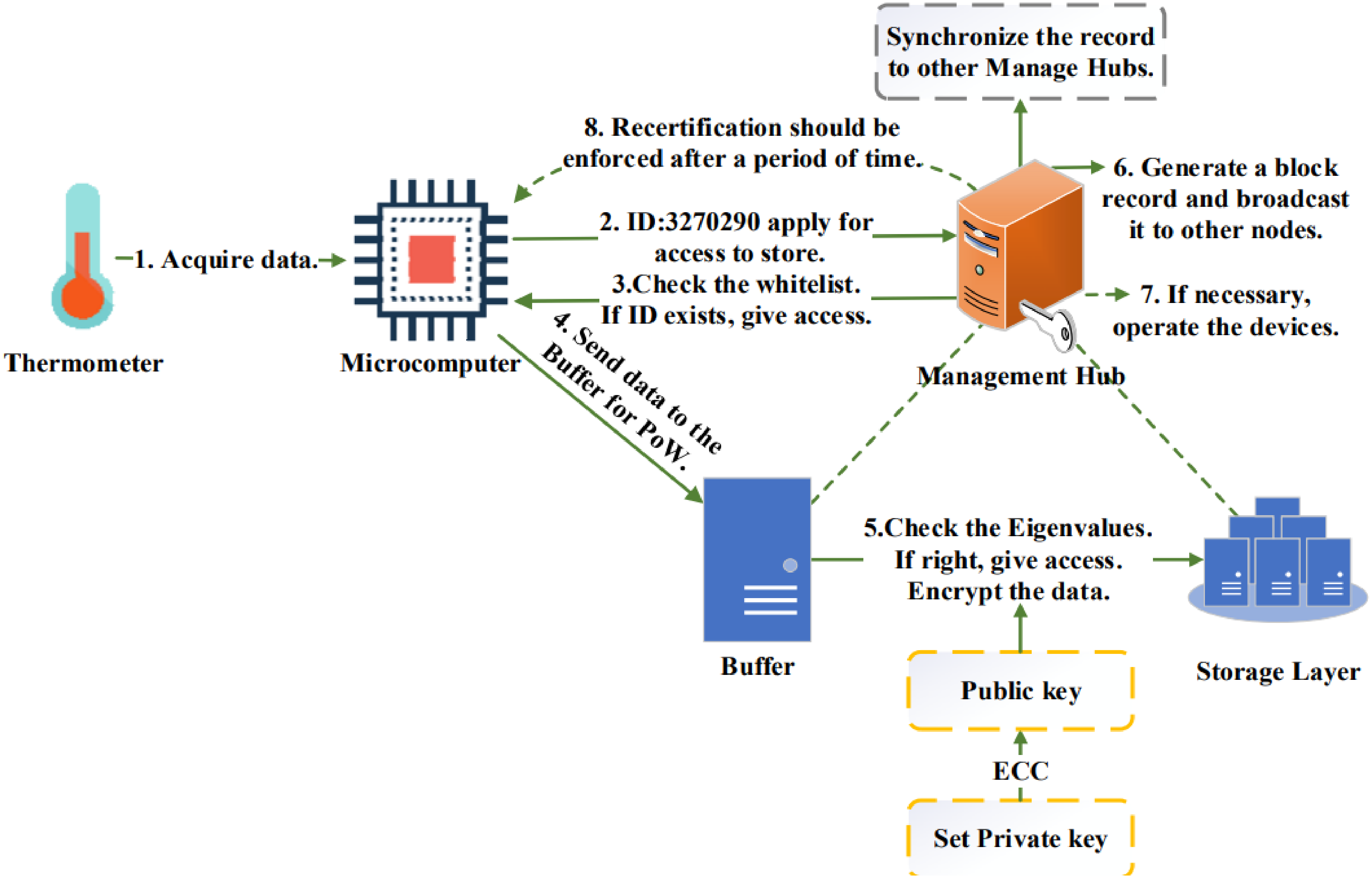
2. Search and Changing the hub

Algorithm1: Data interaction in the intranet

```
begin
  for i←1 to mComputer[1...a]
    find the connected mComputer[j] for mComputer[i]
    register ID
  end for
  wait()   //wait for application
  if(requestReceived == true)
    if(compare the mComputer with whitelist[1...a] == true)
      tick()   //record the running time
      wait for enough insertions in the buffer for the PoW
      if(execute PoW == true)
        generate and broadcast a block record
        subsequent data is uploaded to the database directly
      else
        deny and generate a block record
        discard the data in the buffer
      end if
      if(time == set value)  close the connection
      end if
    else
      deny, generate and broadcast a block record
    end if
  end if
end
```

4. DATA INTERACTION PROCESS DESIGN

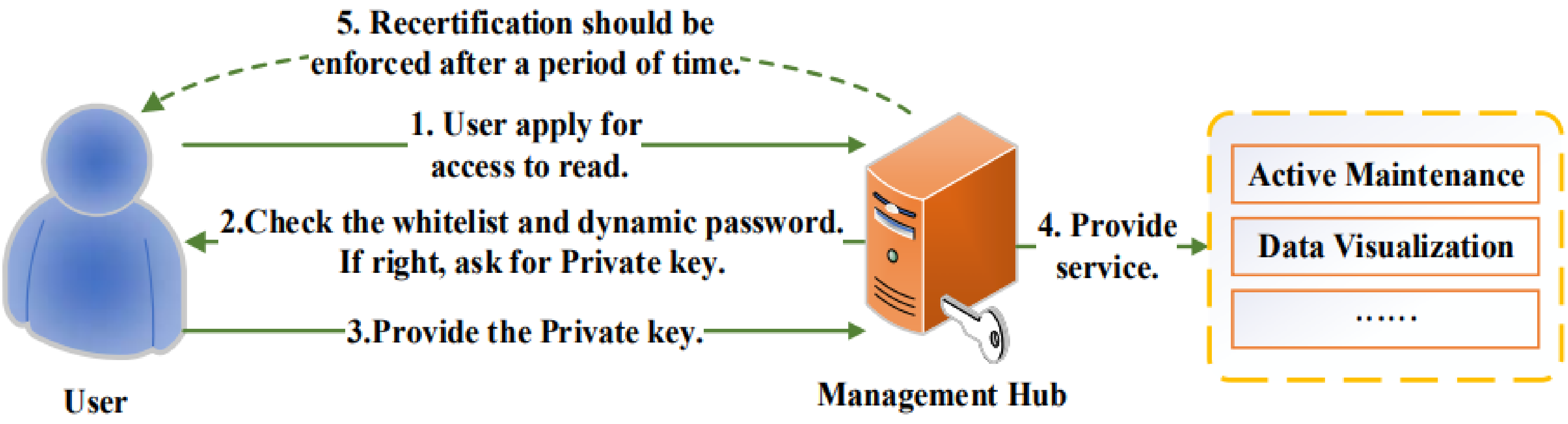
Prevent the possible attacks and threats(Con't)



[Fig. 4. The intranet flowchart (equipment interaction).]

4. DATA INTERACTION PROCESS DESIGN

Prevent the possible attacks and threats(Con’t)



Algorithm2: Data interaction in the extranet

```
begin
  for i←1 to user[1…d]
    find the connected mComputer[j] for users[i]
    register ID
  end for
  wait()   //wait for application
  if(requestReceived == true)
    if(compare with the whitelist[1…a] and password == true)
        tick()   //record the running time
        user verify the data, provide private key to get service
        generate and broadcast a block record
          if(time == set value)  close the connection
          end if
    else  deny, generate and broadcast a block record
    end if
```

[Fig. 5. The extranet flowchart (users apply for service)]

4. DATA INTERACTION PROCESS DESIGN

Prevent the possible attacks and threats(Con’t)

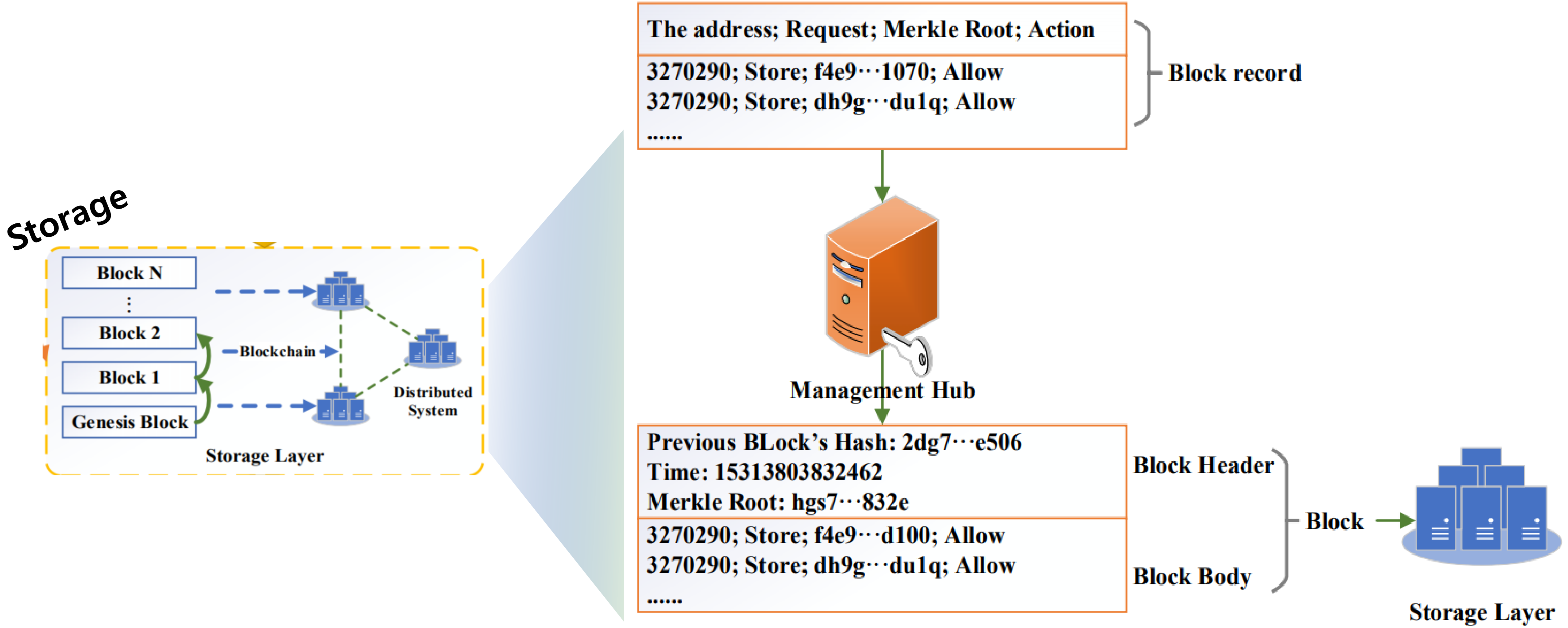


Fig. 6. Block generation.

5. A CASE STUDY: A BLOCKCHAIN-BASED AUTOMATIC PRODUCTION PLATFORM

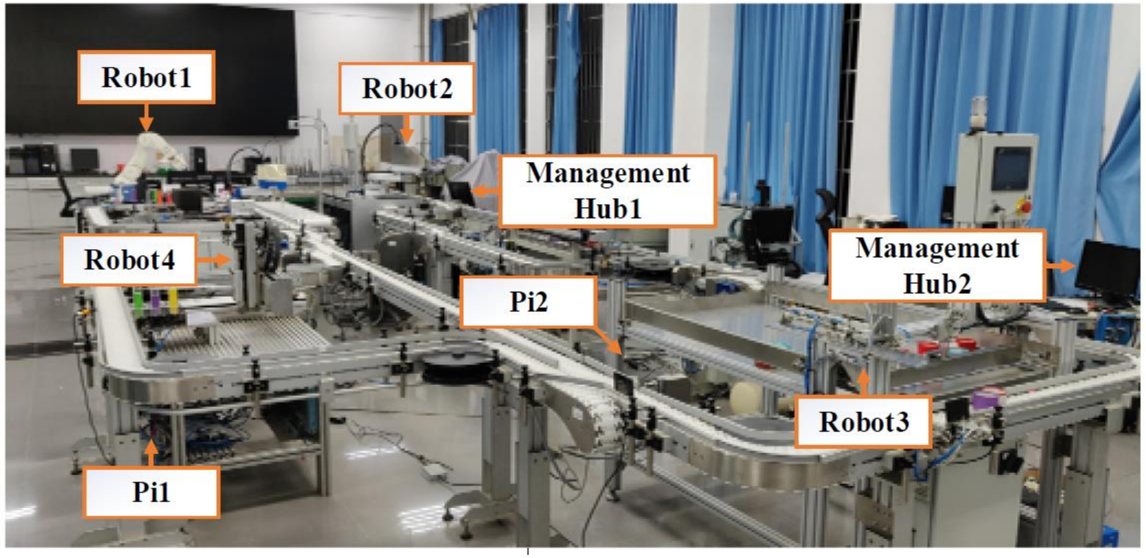


Fig. 7. Automatic production platform.

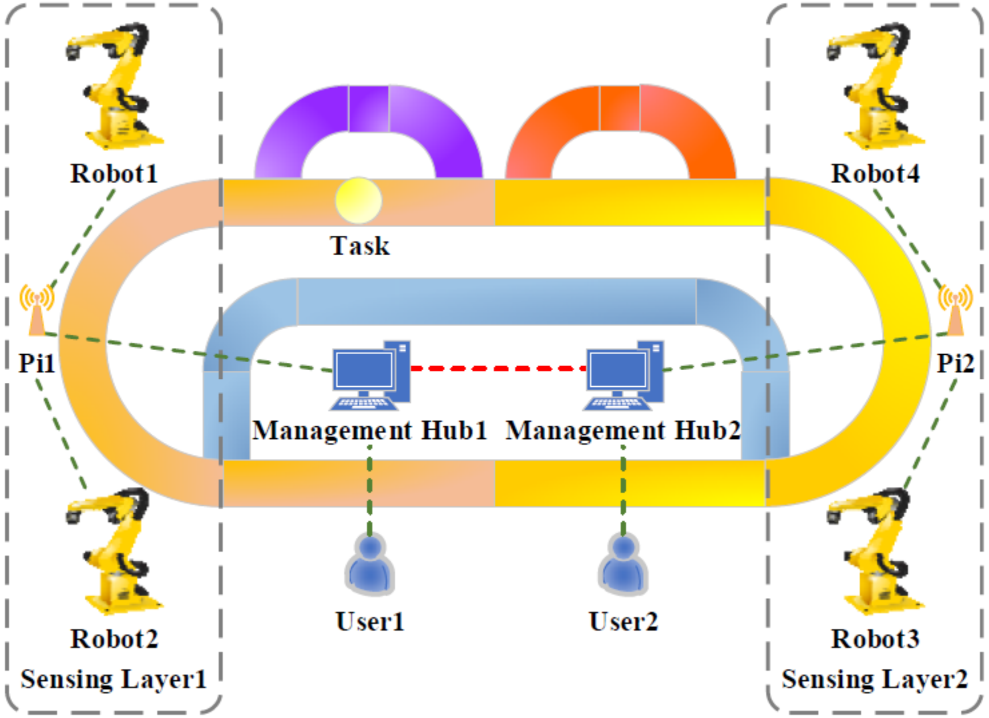


Fig. 8. The architecture of the automatic production platform.

- Automatic production platform according to the proposed architecture

5. A CASE STUDY: A BLOCKCHAIN-BASED AUTOMATIC PRODUCTION PLATFORM

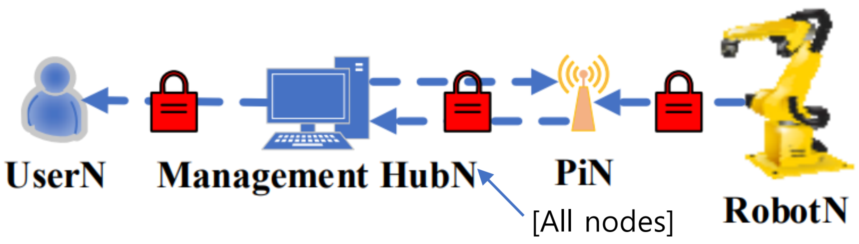


Fig. 9. Data interaction in the transformed platform.

TABLE V
DEFENSIVE MECHANISMS FOR THE PLATFORM

	Equipment nodes to Management hubs	User nodes to Management hubs
Whitelist	Connected through the Ethernet and assigned a fixed IP address.	Connected through the Internet. The malicious access IP will be banned for a period.
PoW	Setting control value by SPC theory.	
Dynamic Verification	PoW should be re-accomplished for access authorization after a period.	The dynamic password should be re-provided for access authorization after a period.
Merkle Root	Generated from the data in the buffer.	Generated from the data in the block body.
Asymmetric Encryption	Using public key to encrypt the uploaded data.	Using private key to decrypt the return data for services.

- Defensive Mechanism

TABLE VI
COMPARISON OF THE ARCHITECTURES

Properties	Cloud-based IIoT architecture	Blockchain-based IIoT architecture
Identity and Authentication	Specific accounts	Specific IP address or accounts
Access control	Static password	PoW, dynamic password
Storage	Plaintext	Ciphertext
Protocol and network security	Pre-defined with static password	Pre-defined with Whitelist, PoW, Dynamic Verification
Privacy and Non-Reputation		Asymmetric Encryption, Hash, Merkle Root
Real-time capability	High	High
Resource overhead	Medium	Medium
Fault tolerance	Medium	High
Scalability	High	Medium

- Compare with traditional IIoT architecture.

6. Conclusion and Opinion

- Innovative blockchain-based IIoT architecture to help build a more secure and reliable IIoT system than traditional industry.
- Advantages of the Blockchain technology, IIoT system introduce a new architecture and give a detailed analysis of all architecture layers.
- BLP model as well as Biba model to design secure assurance in theory.
- But, there is no specific value about result.
- If there were various attack scenarios, it could be applied to a more complete industrial system.
- IIoT, as well as a variety of smart cities, smart homes, and can be used in a variety of infra system.

THANK YOU