Anonymous Storage and Verification Model of IIoT Based on Blockchain

Anonymous storage and verification model of IIoT production status based on blockchain

Tianhao Liu*
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
llllll@bjtu.edu.cn

Jiqiang Liu
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
jqliu@bjtu.edu.cn

Jian Wang†
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
wangjian@bjtu.edu.cn

Di Zhai
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
20120487@bjtu.edu.cn

Yufei Liu
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
yufeiliu@bjtu.edu.cn

Xudong He
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University
hexudong@bjtu.edu.cn

ABSTRACT

With the rapid development of smart industry, the data acquisition ability of edge devices in the perception layer of smart factory is gradually improved. The security of Industrial Internet of Things has increasingly become a common focus. Aiming at the data security problem in the security of industrial Internet of things, combined with the current situation of industrial Internet of things equipment, this paper proposed an anonymous storage and verification model of industrial production status which is based on blockchain. The purpose of this paper is to ensure the storage security and efficient use of industrial production data. We improve the existing Industrial Internet of Things architecture and add blockchain to participate in smart factory privacy protection and data automation processing. On this basis, anonymous storage and verification algorithm for production status, DCB (Double Color Ball) algorithm, is designed. Finally, the simulation industry platform is built, and the architecture is realized by taking the simulation industry platform as an example. The proposed structure can verify data anonymously on the premise of ensuring data security through theoretical analysis and experiment. Besides, the IIoT system still maintains a low overhead.

*First author Tianhao Liu is currently working toward the Master's degree in cyberspace security at Beijing Jiao Tong University, Beijing, China.

†Corresponding author. Jian Wang received Ph.D. degree in cryptography from Beijing University of Posts and Telecommunications, in 2008. Since July 2008, Dr. Wang has been teaching and researching at Beijing Jiaotong University. His current research interests includes big data security and analysis, quantum computing, cryptography application and authentication technology, and computer forensics technology.

ICBTA 2021, December 17–19, 2021, Xi'an, China

ACM ISBN 978-1-4503-8746-0/21/12…$15.00
https://doi.org/10.1145/3510487.3510508

CCS CONCEPTS

• **Information systems**; • **Information storage systems**; • **Storage management**;

KEYWORDS

Blockchain, IIoT, Data security, Privacy protection

ACM Reference Format:
Tianhao Liu, Jiqiang Liu, Jian Wang, Di Zhai, Yufei Liu, and Xudong He. 2021. Anonymous Storage and Verification Model of IIoT Based on Blockchain: Anonymous storage and verification model of IIoT production status based on blockchain. In *2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021), December 17–19, 2021, Xi'an, China.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3510487.3510508

1 INTRODUCTION

Modern industrial has evolved to industry 4.0 since the third scientific and technological revolution. The core of improving industrial productivity is transformed into industrialization and digital intelligence[1]. China, the United States and the United Kingdom attach great importance to the research of industry 4.0.The number of papers of these three countries ranks on the top three Google academic papers.[2] Consequently, a smart factory ,with the Industry Internet of Things (IIoT) as the core and artificial intelligence, augmented reality, big data analysis, cloud computing and other technologies ,has emerged.[3] Smart factories have perceived the operational status of equipment more comprehensively through IIoT. Every unit in the factory can communicate and negotiate with each other through the IIoT to realize self-organization. Massive data can be uploaded to the equipment with scalable storage space and strong computing power for centralized processing, so as to realize the whole system coordination in the factory[4].

Governments around the world have realized the importance of this new generation of manufacturing with active initiatives. Germany put forward High-Tech Strategy 2020 strategy, China put forward Made in China 2025 strategy[5]. Thanks to the national

support and researchers' efforts, there are already many industrial IoT platforms such as Kaa, SiteWhere, DeviceHive and FIWARE[6]. The main function of the IoT platform is to break the data island between factory equipment and realize data interconnection. The digitization and intelligence of the factory is effectively improved through the industrial IoT platform. The deployment of the IoT platform makes the smart factory have the following functions: extracting data from devices, sensors and devices, connecting and analyzing edge devices, storing a large amount of data, analyzing, and finally controlling data in real time[7]. In terms of industrial IoT platform, data processing involves all processes and plays a significant role. If the IoT platform can reasonably process a large amount of data, it will improve the production efficiency of the factory. However, the smart factory is a large and complex system with IIoT devices, making critical devices vulnerable to attack. In [8], George et al. analyzed the threat and impact of different vulnerabilities on industrial 4.0 system. On the other hand, several attack cases against devices in smart factories were shown in [9]. Such threats and assaults would result in not only the release of sensitive data, but also a slew of social and economic concerns, as well as a threat to national security. As a result, there is a pressing need to address the present IIoT architecture's security and privacy flaws[10].

The advent and development of blockchain technology has opened up new possibilities for IIoT research. Nakamoto introduced a peer-to-peer digital currency system in 2008[11], and blockchain technology has since been a focus for study. From the period of blockchain 1.0 to the era of blockchain 3.0[12]. The blockchain has progressed beyond its basic encrypted currency to various aspects of field, making several positive effects. To get effective outcomes, blockchain technology is deployed to the industrial Internet of Things. In [13] Jiafu Wan et al introduced a security and privacy model based on Bitcoin blockchain. It makes the IIoT system more secure and reliable. Javaid et al [14] proposed a blockchain architecture that uses a dynamic proof-of-work consensus with a block checkpoint mechanism. In order to popularize blockchain technology in the IIoT, [15] analyzed the logic and requirements of different industrial IoT scenarios to abstracts them into a universal model. The above work discusses and analyzes the current security problems of IIoT, and puts forward the corresponding solutions. However, in addition to ensuring data security and privacy, an excellent IIoT architecture also needs strong capability of data processing[16]. On the basis of data security, it can have better data capability and effectively improve the competitiveness of the IIoT platform. The novelty of this study is as follows:

- Combined with the blockchain, the permissioned blockchain design is introduced to build an IIoT architecture for automatic data processing to ensure data security and privacy protection for the smart factory.
- Realize the anonymous storage of production status based on the blockchain ledger, and design a fast query index based on polynomial interpolation algorithm—DCB Algorithm.
- Build a simulation industrial production platform and verify the effect of the architecture.

This paper is organized as follows. In Section 2, the architecture of IIoT data automatic processing based on blockchain technology is presented; in Section 3, we proposed the design of anonymous storage and verification of production status–DCB algorithm; in Section 4, the flow of automatic data processing of blockchain is given, and the specific flow of contract execution is given; in Section 5, we use more specific settings to transform an automatic production platform, and analyze the security and performance of the proposed architecture in practice. Finally, a brief conclusion and future research direction are provided in Section 6.

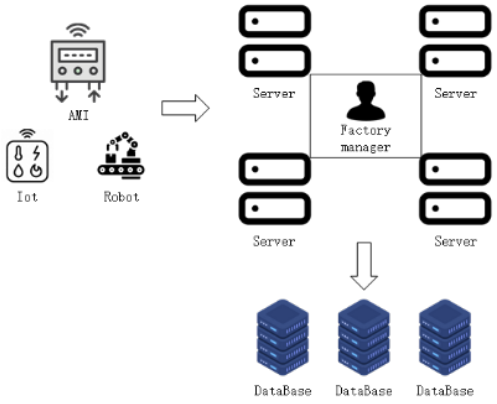

Figure 1: Blockchain-based IIoT architecture for a smart factory.

2 BLOCKCHAIN-BASED IIOT ARCHITECTURE

Through the blockchain service to connect to the IIoT, the smart factory has established a decentralized system in which nodes supervise each other. The proposed smart factory IIoT architecture based on blockchain is shown in figure 1

Industrial data of each smart factory is collected by various sensors, and the sensor data is safely transmitted and processed through the blockchain layer. Due to the high cost of storing all the data in the blockchain network, the blockchain service carries out tamper-proof tagging and preliminary processing of the data. The processing result and the original data are passed into the data storage device for storage. The stored data can be further utilized. The emergence of a new type of sensor, represented by the intelligent meter[17], strengthens the function of the sensor and improves the communication ability and computing ability of the sensor equipment. In this paper, the sensor layer is further divided. The sensor is divided into ordinary sensor and smart sensor[18]. In this paper, with the help of smart meter and other sensors as the data provider of industrial production, the industrial Internet of things data processing model based on blockchain is constructed. The model classifies the main parts of the production unit in the smart factory into four types of devices, including ordinary IoT, smart IoT, management servers and data servers.

2.1 Smart Factory Architecture

As shown in figure 2, the smart factory is divided into production data layer, blockchain service layer, data storage layer, and factory management layer. The production environment layer is the data

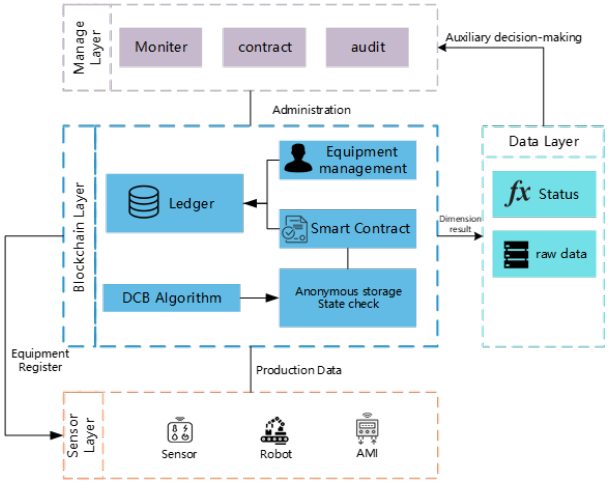

Figure 2: Blockchain based smart factory structure.

source part of the whole factory, and the production environment layer is composed of traditional Internet of things equipment and intelligent Internet of things equipment, which can collect various data in the production process and carry on a certain degree of preprocessing. The equipment in the production environment layer registers the equipment through the blockchain service layer, and the production environment layer provides data for the and data layer in the blockchain service layer in the production process. On the one hand, the original data generated in production is stored in the data storage layer for persistent storage, on the other hand, the core data covered by the production status is submitted to the blockchain service layer for data verification. Due to the weak computing power of the equipment in the production data layer, it cannot undertake a lot of data storage and data verification work, so the management and data evaluation of the IoT equipment are carried out by the factory management.

The blockchain layer maintains a distributed ledger for storing transactions in a distributed network composed of licensed blockchain nodes. Each of these nodes maintains a copy of the ledger by applying transactions that have been verified by the consensus agreement. On the one hand, the blockchain layer is responsible for the registration and data transmission process of the Internet of things equipment within the factory, authentication, and data verification in the production process. For factory managers, monitoring of production status, production status deployment and production data audit can be realized by calling the services of the blockchain layer.

2.2 Blockchain and Factory Management

In the IIoT in smart factories, we pay more attention to the efficiency of data interaction. Different from the public chain that everyone can join, the smart factory blockchain system is a blockchain system deployed in the private domain, and the identity of the nodes is credible. Therefore, the main purpose of the consensus algorithm is to achieve the orderly winding of transactions, and we choose RAFT protocol[19] as the consensus protocol[20]. We use anonymous storage technology to store the production status in the distributed

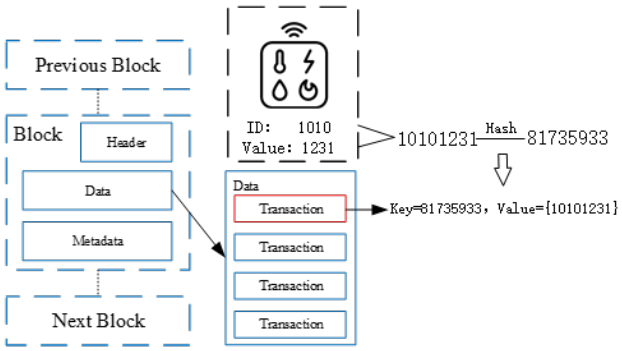

Figure 3: Ledger storage structure.

ledger, and construct data verification algorithm according to the relationship of the data. When verifying the transaction, we can use the data verification algorithm to verify whether the production data meets the production status.

3 ANONYMOUS STORAGE AND VERIFICATION OF PRODUCTION STATUS

Plaintext storage of data by traditional block chain technology there is a risk of data abuse in smart factories.[21] This paper designs a method to anonymize the production status data in the blockchain, and designs a two-color-ball algorithm based on interpolation polynomials to check whether the data generated in the production process is in line with the production status. In order to facilitate the description of the algorithm, the elements of the DCB algorithm are defined, as shown in the table 1

3.1 Anonymous Storage of Production Status

The data in the distributed ledger of the permissioned blockchain, as shown in figure 3, is stored in the form of key values. After the production status is obtained in the blockchain layer, the production status is bound with the equipment number, the bound data is anonymized through the hash function, and the data with practical meaning is transformed into non-repetitive random data.

Sensor (ID : 1010) is bound to a state eigenvalue ($value$: 1231) to construct an indicator data ($value$: 10101231). The data mapping is established through the Hash function, and the index data is mapped to the hash number (Key : 81735933). The anonymously processed hash data is used as the key and the state data as the value($Point\{81735933, 10101231\}$). The blockchain network is submitted in the form of transaction, and the production state eigenvalue is stored anonymously. The following describes how to use anonymous stored metric data for data verification.

As Algorithm 1 shown, we designed a fast and efficient data verification double-color-ball algorithm, that the core idea is to construct interpolation polynomials from state data.

DCB algorithm acts on the anonymous storage of data, the key-value pairs generated by anonymous storage are used as the points of constructing interpolation polynomials to construct production state search polynomials. The index search polynomial can be used for data verification. On the one hand, the anonymous verification of the data can be realized, on the other hand, the smart IoT data

Table 1: Formal definition

Notation	Description
B	Blue data(Smart IoT)
R	Red data(Ordinary IoT)
R_h	Hash(R)
DSet	A set of production data corresponding to a production status
Hash	Hash function
Point	(R, R_h)
Poly	Interpolation polynomials generated by a set of States
Poly(x)	The solution obtained by bringing x into the polynomial
PolyMap(B)	A set of interpolation polynomials. A corresponding polynomial can be found through blue data.
PointMap(R_h)	A set of points, and a corresponding polynomial can be found through R_h

Algorithm 1 DCB algorithm

$DSet = \{r_1 \dots r_n, b | r \in \text{R}, \text{b} \in \text{B}\}$
begin
for i←1 to DSet.R[1..n]
$r_{hi} = Hash(r_i)$
PointMap add Point$\{r_{hi}, r_i\}$
Save Point to Ledger
end for
use PointMap construct Lagrange interpolation Polynomials $Poly_b$
Save Poly$\{b, Poly_b\}$ to Ledger
end

(blue data) and Ordinary IoT data (red data) and mutual verification can be realized. The following describes how to use polynomials to verify production status.

3.2 Anonymous Verification for Production Status

After all the state polynomials are deposited in the ledger. The production status can be validated by calling these polynomials. We validate a set of production status data $D = \{r_1 \dots r_n, b \mid r \in R, b \in B\}$. There are three cases of data verification:

- Red data verify (blue data correct). First of all, the polynomial is determined according to the blue data. $PolyMap(b) = Poly_b$. Let $r_{pi} = Poly_b(r_i)$, if $PointMap(r_{pi})$ equals r_i, then the data is correct, else r_i is error. Note: if the verification of red data in a set of data fails too much, there may be a problem with the blue data. We set a fault tolerance threshold, if the amount of error red data exceeds the fault tolerance threshold.
- Blue data verify. The amount of error red data exceeds the fault tolerance threshold. The polynomial group is verified one by one. It can make the red data check that the blue data corresponding to the polynomial with the largest number is the correct blue data.
- If no result is found that the number of red data validation is higher than the total entry-validation threshold during the process of blue data validation, the data set is considered to be an exception. Label array D as error.

The next section describes how to use the DCB algorithm for automatic data processing.

4 AUTOMATIC CHECKING MODEL OF PRODUCTION STATUS

The automatic verification model of production status applies the DCB algorithm to the blockchain layer of smart factory to realize the automatic processing of industrial production data. At this stage, according to the topology of the smart factory, the ordinary Internet of things devices and intelligent Internet of things devices deployed in the production environment are used as data delivery nodes. Among them, the ordinary IoT devices that collect sound, light, location and other environmental data are used as red data, and the smart meters that monitor the power data of IoT equipment and industrial production equipment belong to intelligent IoT devices as blue data.

As Figure 4 shows, the model is divided into three parts:

- Device registration, the units in this network topology will be submitted to the blockchain network for device registration.
- Initialize the data, input the status data of production into the blockchain ledger, complete the recording of the point set and the polynomial set, and construct the data processing intelligent contract.
- Data processing, in the production process, the blockchain network automatically receives the data and executes the smart contract. Automatically judge whether the status of the production data is normal or not.

5 CASE STUDY: SIMULATING SMART FACTORY ENVIRONMENT FOR AUTOMATIC DATA PROCESSING

In this chapter, we build a simulated smart factory platform based on blockchain architecture and intelligent power system to discuss the role of production data labeling model in the IIoT. The simulation system includes robot, smart meters, raspberry pies, sensors, storage servers. Simulated factory production platform.

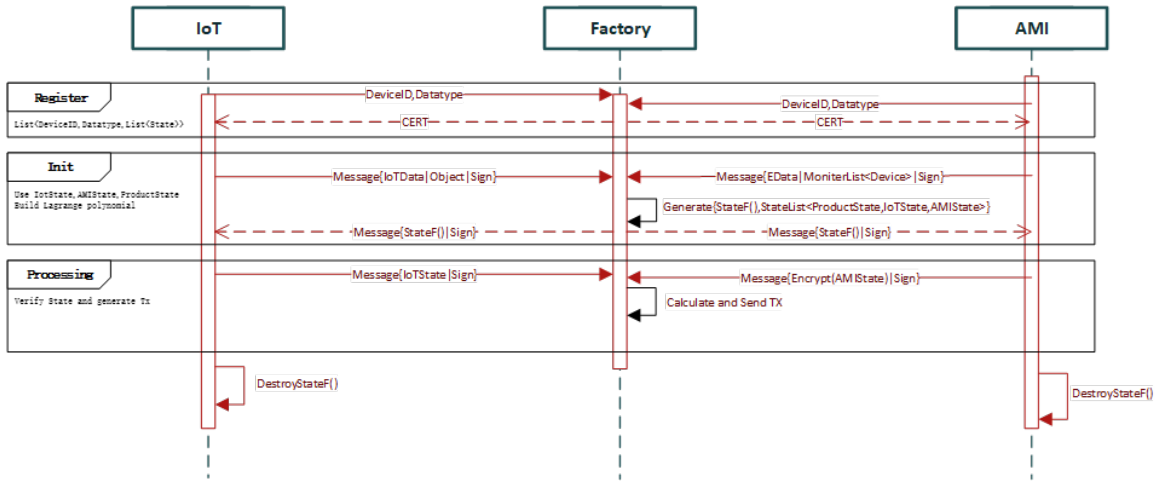

Figure 4: Automatic inspection of production status UML.

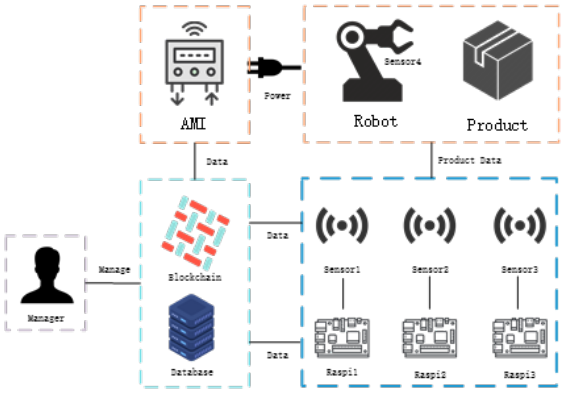

Figure 5: Architecture of the automatic production platform.

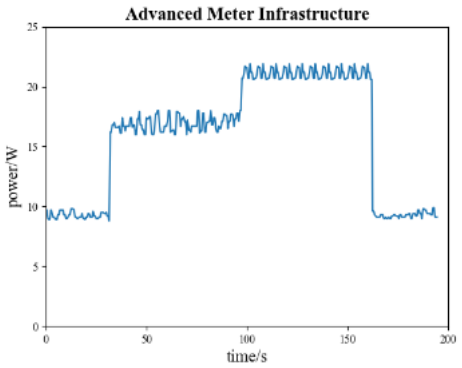

Figure 6: Smart meter data.

As shown in figure 5, an industrial robot is designed to perform product processing tasks on the platform. The intelligent factory system model industry robot is connected to the smart meter, and the intelligent electric meter monitors the power data of the industrial robot. We set up some sensors to collect production data. At the same time, the blockchain network is set up in the simulation factory. The blockchain network is based on Hyperledger fabric[22] and has six nodes. The anonymous storage and verification model of production status is deployed for automatic data processing, and then transmitted to the database for storage. Finally, we set up a manager of intelligent factory manager who can access the blockchain network and the data center.

5.1 Data Acquisition Result

We set three production states of the industrial robot by writing a control program to control the industrial robot, namely, the static state, the action of grabbing goods and the action of moving goods.

The data acquisition result of the smart meter is shown in the figure, and the industrial robot keeps the standby running at low power in the static state. The output power has been improved in the process of grabbing the goods. The power is the highest when the robot is carrying goods. After the completion of the movement, the standby state is restored, and the robot returns to the low power running state.

The data acquisition result of the sensor is shown in figure 7. The distance sensor can detect the change of the distance between the robot and the sensor when the robot reaches the grasping position and leaves. The increase in the value of the photosensitive sensor under the object when the object is removed indicates that the object has been removed correctly. The sound sensor records different sound values with different actions performed by industrial robots. When the industrial robot performs the production action, the ambient temperature has no obvious change.

As shown in Table 3, We record the average values of the sensors in each production state by performing production actions several times. Among them, the ambient temperature sensor has no obvious change, so it is impossible to distinguish the production state and do not record it.

Table 2: Production status

Action	AMI	Distance Sensor	Light Sensor	Sound Sensor
inactivate	8-9	50	34-40	24-28
grab	15-18	9	55-60	17-19
move	20-22	46	55-60	21-23

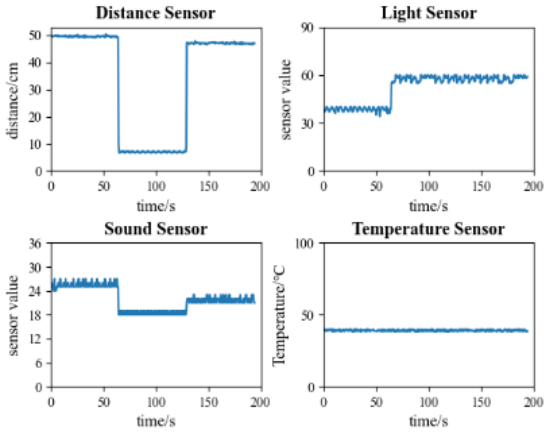

Figure 7: Sensor data.

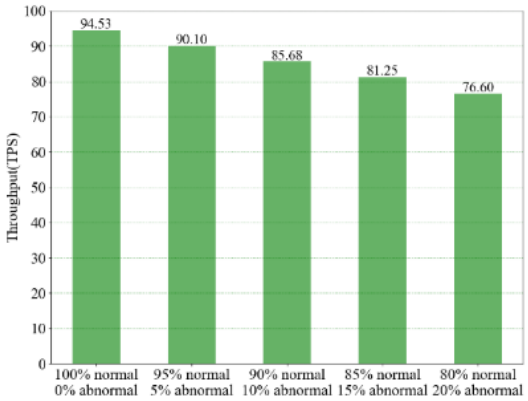

Figure 8: Throughput.

5.2 Performance Analysis

We use the collected set as the input data of the model to test the anonymization of production status and the performance of the verification model. This model is deployed on the Hyperledger Fabric 2.2 version of the blockchain network composed of 6 nodes, and the operation system is Ubuntu 20.04TLS. The configuration of the test computer is as follows: Ryzen 3700x 3.6GHZ 32GB DDR4 2666MHz. data generated by the industrial platform are collected and classified through the operation of the industrial platform, and the data that can cover 3 kinds of the action are selected as the production status data. 50 points and 100 polynomials are obtained.

Suppose that the abnormal proportion of red data in the experimental data set is a, the abnormal proportion of blue data is b, the proportion of complete abnormal data is c, and the proportion of normal data is $1 * a * b * c$. Suppose the communication and consensus time is t, and the execution time of data contracts in different situations is shown in table III. Among them, $T_a < T_b < T_c$, it can be seen that the main factors that affect the execution efficiency are the proportion of blue data anomalies and complete data anomalies, in the actual experiment. The proportion of abnormal data is relatively low, and the blue data collection equipment is usually completed by intelligent Internet of things devices, so the probability of problems is relatively small. The impact of abnormal data on the performance of the model is within the allowable range.

In order to test the impact of abnormal data on execution efficiency, we constructed five datasets with error data ratios of 0%, 5%, 10%, 15%, 20%, respectively, and tested the throughput of 1000 specific transaction records.

As shown in figure 8, the proportion of abnormal data has a certain impact on throughput, and the transaction throughput decreases with the increase of abnormal data. In the real environment, the proportion of abnormal data is small, the system still maintains low overhead.

6 CONCLUSION

We propose a smart industrial architecture based on blockchain, which is suitable for IIoT, which can realize safe and reliable transmission and storage of production data. Aiming at the production status verification scene of industrial production process, an anonymous production status data storage scheme suitable for blockchain system is proposed, and a DCB algorithm based on improved interpolation polynomial is designed to realize the rapid verification of production status. And build a simulation industrial production platform in the laboratory, execute the program for industrial production through the industrial robot, and the sensor collects data to

Table 3: Time cost

DataType	Correct	Red error	Blue Error	All Error
time	t+T	$t+T_a$	$t+T_b$	$t+T_c$

simulate the production data verification process in the industrial production process. At the same time, the federation blockchain is built, the production status is stored anonymously through the distributed ledger, and the check polynomial is deployed in the test network in the form of contract. Taking the data in the industrial production platform as the test data, the experiments for performance analysis are carried out to verify the efficiency of the DCB algorithm in the verification of production data. This paper discusses the possibility of automatic data processing through smart contract. In the future, the decision-making efficiency of intelligent factory can be further improved and the monitoring function of industrial control system can be expanded by improving intelligent contract.

ACKNOWLEDGMENTS

This work was supported in part by the Major Scientific and Technological Innovation Projects of Shandong Province, China (No.2019JZZY020128). Scientific and Technological Development Plan Projects of China National Railway Group Limited (No. N2020W005) also gave significant assistance to finish this work.

REFERENCES

[1] Bodkhe, U., *et al.*, Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access, 2020. 8: p. 79764-79800.
[2] Zhong, R.Y., *et al.*, Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering, 2017. 3(5): p. 616-630.
[3] Sufian, A.T., *et al.*, Six-Gear Roadmap towards the Smart Factory. Applied Sciences, 2021. 11(8): p. 3568.
[4] Wang, S., *et al.*, Implementing smart factory of industrie 4.0: an outlook. International journal of distributed sensor networks, 2016. 12(1): p. 3159805.
[5] Büchi, G., M. Cugno and R. Castagnoli, Smart factory performance and Industry 4.0. Technological Forecasting and Social Change, 2020. 150: p. 119790.
[6] Kim, M., J. Lee and J. Jeong, Open Source Based Industrial IoT Platforms for Smart Factory: Concept, Comparison and Challenges. 2019, Springer International Publishing: Cham. p. 105-120.
[7] Wang, Q., *et al.*, Blockchain for the IoT and industrial IoT: A review. Internet of Things, 2020. 10: p. 100081.
[8] Stergiopoulos, G., P. Dedousis and D. Gritzalis, Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0. International Journal of Information Security, 2021.
[9] Panchal, A.C., V.M. Khadse and P.N. Mahalle. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures. in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). 2018: IEEE.
[10] Chen, B., *et al.*, Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges. IEEE Access, 2018. 6: p. 6505-6519.
[11] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 2008: p. 21260.
[12] Chen, C., *et al.*, A Secure Content Sharing Scheme Based on Blockchain in Vehicular Named Data Networks. IEEE Transactions on Industrial Informatics, 2020. 16(5): p. 3278-3289.
[13] Wan, J., *et al.*, A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory. IEEE transactions on industrial informatics, 2019. 15(6): p. 3652-3660.
[14] Javaid, U. and B. Sikdar, A checkpoint enabled scalable blockchain architecture for industrial internet of things. IEEE Transactions on Industrial Informatics, 2020.
[15] Fang, L., *et al.*, A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City. IEEE Internet of Things Journal, 2020. 7(9): p. 7982-7990.
[16] Novo, O., Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, 2018. 5(2): p. 1184-1195.
[17] Martín, A.A.S., E.G. Guerrero and L.E.B. Santamaría. Prospective integration between Environmental Intelligence (AMI), Data Analytics (DA), and Internet of Things (IoT). in 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI). 2019: IEEE.
[18] Gao, Y., *et al.*, Blockchain Based IIoT Data Sharing Framework for SDN-Enabled Pervasive Edge Computing. IEEE Transactions on Industrial Informatics, 2021. 17(7): p. 5041-5049.
[19] Ongaro, D. and J. Ousterhout. In search of an understandable consensus algorithm. in 2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14). 2014.
[20] Liang, W., *et al.*, A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. IEEE Transactions on Industrial Informatics, 2019. 15(6): p. 3582-3592.
[21] Lax, G. and A. Russo, Blockchain-Based Access Control Supporting Anonymity and Accountability. Journal of Advances in Information Technology Vol, 2020. 11(4).
[22] Androulaki, E., *et al.* Hyperledger fabric: a distributed operating system for permissioned blockchains. in Proceedings of the thirteenth EuroSys conference. 2018.