applied sciences

MDPI

Article

Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing

Peng Zhai [1,2,*], Jingsha He [1] and Nafei Zhu [1]

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China; jhe@bjut.edu.cn (J.H.); znf@bjut.edu.cn (N.Z.)
[2] School of Mathematics and Computer Application Technology, Jining University, Jining 273100, China
* Correspondence: sinomcse@emails.bjut.edu.cn or zbzx@jnxy.edu.cn

Abstract: The integration of information systems and physical systems is the development trend of today's manufacturing industry. Intelligent manufacturing is a new model of manufacturing, based on advanced manufacturing technology with human–machine–material collaboration. Internet of Things technology is the core technology of intelligent manufacturing, and access control technology is one of the main measures to ensure the security of the IoT. In view of the problem that the existing IoT access control model does not support distributed and fine-grained dynamic access control, this paper uses the characteristics of blockchain, such as decentralization and non-tampering, combined with the attribute-based access control (ABAC) method, to propose a distributed access control method, applicable to the IoT environment in the process of intelligent manufacturing. This paper describes a fine-grained access control policy by defining the access control attribute values in a formal language, which supports complex logic operations in the policy and enhances the expressiveness of the model. Distributed access control decision making, using smart contracts for blockchain, improves the decision-making efficiency of the access control model, increases the post-facto audit of the access control behavior, and improves the overall security of IoT data protection. The paper concludes with proof of security and a performance analysis, and the experimental results, such as storage and computing overheads, show that this method can provide fine-grained, dynamic, and distributed access control for devices in intelligent manufacturing, ensuring the security and reliability of access control for IoT devices.

Keywords: access control; blockchain; IoT; intelligent manufacturing

Citation: Zhai, P.; He, J.; Zhu, N. Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing. *Appl. Sci.* **2022**, *12*, 3692. https://doi.org/10.3390/app12073692

Academic Editor: Alexandre Carvalho

Received: 15 March 2022
Accepted: 4 April 2022
Published: 6 April 2022

1. Introduction

In recent years, intelligent manufacturing, with digitalization, informatization, and networking as the main features, has become the main direction for the future development of the manufacturing industry. With the impetus of the digital economy, AI, industrial internet, digital twins, and other emerging technologies, intelligent manufacturing has gradually gained the attention of governments and has become important to them. As a product with high integration of the IoT, big data, blockchain, AI and advanced manufacturing technology, intelligent manufacturing helps to realize the intelligence of the whole process, from product design to production, and promotes the continuous upgrading of the manufacturing industry [1–3].

The industrial IoT is an important part of intelligent manufacturing, which gives the IoT network connection the capability to be used with mechanical equipment, whereby enterprises can collect data from the whole generation process for real-time analysis and processing, and for process visualization. The collection, transmission, and storage of large amounts of IoT data enables intelligent manufacturing capabilities, but also poses security risks. The IoT is not a simple superposition of sensors, communication interfaces, and communication devices, but a variety of instruments and devices in different networks and

fields that are interconnected and collaborated. As the scale of the IoT continues to grow, the probability of collaboration scenarios between devices is increasing [4], especially in the process of digital twin technology. A large number of applications, the entire intelligent manufacturing model, integrate a large number of historical and real-time process data from physical systems. Digital agency needs to monitor the production system or the state of the process, predict the performance of the system, and generate the system behavior or control action; data exchange and data access control put forward higher requirements [5]. Blockchain-based and green Internet of Things' UAV applications [6], as well as blockchain-based face monitoring by drones (used during COVID-19), also face a lot of data access control requirements [7]. In order to ensure security, collaboration between different types of devices should be performed with appropriate access control, according to the security and privacy protection characteristics of the devices.

As a basic mechanism for achieving security in information systems, access control (AC) determines the communication rights between authorized subjects and objects, according to specific security models and policies [8]. An effective access control mechanism can meet the information security requirements, such as system confidentiality, integrity, and availability. For the scenario of the collaboration of IoT devices in intelligent manufacturing, this paper proposes an AC method applicable to the IoT environment. The access control policy is described in a fine-grained manner, using attributes that support complex logic operations in the policy and enhance the expressiveness of the model; the distributed access control determination decision, using smart contracts deployed on the blockchain, improves the decision-making efficiency of the model AC and enhances the IoT data security. Lightweight nodes in the blockchain are introduced to adapt to the complex and diverse heterogeneous devices in the IoT, to enhance the scalability of the system [9].

This article analyzes the deficiencies of access control technology research in the current intelligent manufacturing Internet of Things environment. We propose a distributed, dynamic, fine-grained data access control method, applicable to IoT device terminals in the intelligent manufacturing process. The model has the following characteristics: (1) After registering with the attribute authorization authority, the IoT device will apply to the attribute authorization authority for access control attribute value pairs. The attribute authorization authority will formulate appropriate access control policies, according to the specific functions of the IoT device, in accordance with the attribute-based access control method and will assign them to the IoT device. These policies will be submitted to the blockchain for consensus and saved to the blockchain after the consensus is passed. (2) All access control determination is conducted by the smart contract (chaincode) deployed on the Fabric, which ensures that the access control determination function is distributed and can avoid the single point issue of the access control determination node.

This manuscript is organized as follows: Section 2 introduces the work related to access control and blockchain technology in the Internet of Things. Next, in Section 3, we focus on the access control model, integrating blockchain and big data cloud platforms. Section 4 describes the distributed access control scheme of the Internet of Things, based on blockchain, which mainly involves system initialization, device registration, blockchain address generation, attribute value pair application, access control policy generation, access control policy cancellation, and other processes. Section 5 describes the access control process management, taking Alice and Bob as examples to describe the access control process between the Internet of Things' terminals. Section 6 analyzes the security and performance of the access control method described in this article. Finally, Section 7 summarizes the research content of this paper.

2. Related Technologies

2.1. Access Control in the IoT

With the continuous development of IoT technologies and applications, the IoT has evolved from an industrial network, based on RFID technology in the early days, to a smart planet, where everything can be connected; access control in the IoT environment has also

evolved. Due to the specificity of the IoT, in addition to security and privacy requirements, access control should also consider scalability, flexibility, and lightweight nodes to fit in the IoT environment. Access control methods applied in the IoT include role-based AC (RBAC), attribute-based AC (ABAC), and rights-based AC, etc. [10]. RBAC maps users to roles through which they can enjoy permission. The model defines the different roles, their inheritance relationships, the connections between roles, and the restrictions to which the roles are subject, and regulates the user's behavior [11]. ABAC is a dynamic access control model that uses attributes as the key element of access control. Because attributes are inherent to the subject and object, ABAC can mine independent and complete sets of attributes without manual input from the administrator, by means of the attribute discovery mechanism, and can quickly mine (attributes and permissions) relationships by means of an automated attribute–permission association discovery mechanism [12,13]. The framework of attribute-based access control is shown in Figure 1.

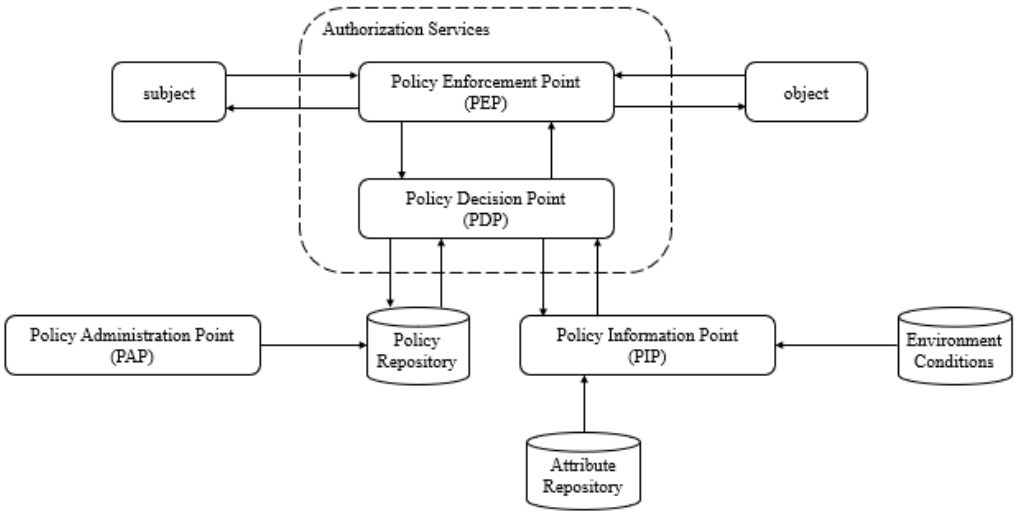

Figure 1. Attribute-based access control foundation framework.

2.2. Blockchain and Internet of Things Technology

Blockchain was first used in the underlying bookkeeping system of Bitcoin [14]. Blockchain includes not only the structure of chained data blocks, but also the product of a combination of P2P network technology, consensus mechanisms, cryptography technology, and a series of other technologies [15]. Blockchain is a chained block data structure with traceable functions established in a distributed network environment, based on trustworthy and transparent rules. The typical characteristics of blockchain include the following six aspects: decentralization, openness, autonomy, distrust, immutability, and anonymity. The application capabilities provided by blockchain include providing infrastructure, such as computing, storage, network and platform resources, through distributed networks or peer-to-peer networks; managing, querying and analyzing data in distributed networks or peer-to-peer networks; and relying on blockchain networks to provide application services, such as digital asset transactions and security certifications [16].

The unique technical characteristics of blockchain enable it to solve the problems of massive data processing, privacy security and trust management, faced in the construction and development of the Internet of Things, thereby promoting the evolution of the Internet of Things to a distributed and intelligent advanced form, such as the following:

(1) In view of the network security architecture, authentication, design authorization, privacy protection and other issues related to the Internet of Things, the security and privacy of the Internet of Things can be ensured in regard to the aspects of storage and information transmission, through authentication and authorization mechanisms.

(2) In view of problems such as the difficulty in ensuring the authenticity of the information obtained by the Internet of Things, the authenticity of the information can be ensured through blockchain traceability.
(3) In view of the problems concerning the multi-network integration of the Internet of Things and intelligent network management, different protocols and devices can be connected through the blockchain, and the ability to manage, query, and analyze data in peer-to-peer networks can be provided.
(4) In view of the fact that the Internet of Things has not yet formed an effective mechanism to open up all links, it can effectively open up all links by providing computing, storage, network, and platform resources through peer-to-peer networks.

3. Attribute-Based AC Method Incorporating Blockchain and CSP

Based on the attribute-based AC method, this paper proposes a distributed AC method based on blockchain and Internet of Things technology, as shown in Figure 2.

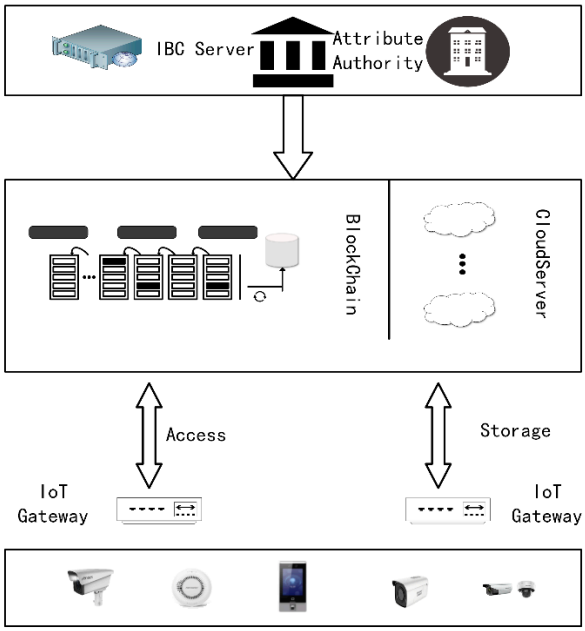

Figure 2. Blockchain-based IoT AC system model.

In this model, the following entities are mainly included: an attribute authorization authority (AAA), an IBC (identity-based cryptograph) [17] server, a cloud service provider (CSP), an IoT gateway, an IoT device, and a federated blockchain network.

The attribute authorization authority (AAA): The AAA is an attribute authorizer of IoT devices. It authorizes i attribute value pairs for each sensing layer terminal, based on its role, identity, etc. Attribute value pairs ($prop\_n_i$, $prop\_v_i$) constitute the set S of attribute value pairs of the device, and the set S is submitted to the blockchain for consensus in the form of transactions, which will be permanently stored on the federated chain after the consensus is passed. The whole system can have multiple attribute authorization authorities.

The IBC server: Every IoT device must complete registration with the IBC server in advance, before joining the system. After successful registration, the device will receive a pair of IBC-based public–private key pairs.

Cloud service provider (CSP): The CSP mainly provides cloud computing and storage services for IoT devices; the IoT data are usually stored with encryption.

The IoT gateway: With strong computing and storage capabilities, it is directly connected to the IoT sensing layer device, and is the intermediary between the IoT terminal and the blockchain and cloud service providers. This largely solves the problem of the limited computing and storage resources in the IoT terminal.

IoT devices: IoT perception layer devices that collect, process, and transmit various device-generated data.

Federated blockchain network: this gives consensus, confirms and stores the transactions submitted to the Fabric network, and also provides a smart contract function to realize the access control function.

4. Blockchain-Based Distributed AC Model for the IoT

The blockchain technology-based distributed AC model for the IoT has the following main steps:

4.1. System Initialization

Generate (G_1, G_2, e) with k as input parameters, where G_1 and G_2 are the order groups of e and q, respectively, and satisfy $G_1 \times G_2 \rightarrow G_2$; randomly select the master key $s \in \mathbb{Z}_q^*$, two secure hash functions defined by the system [17–19].

$$HASH_1 = \{0,1\}^* \rightarrow G_1^*$$
$$HASH_2 = G_2 \rightarrow \{0,1\}^n \quad (1)$$

In addition, the master private key SK_m is stored in the IBC server, and the public key generation is executed by the user generation to generate the public key Pub_m.

4.2. Equipment Registration

When an IoT device needs to join the system, it must apply for the private identity key from the attribute authority it belongs to. The IoT device needs to provide the identity ID to the IBC server it belongs to, and this ID can be used as the device's public key. The IBC server will use its master private key and the identity ID of the IoT device to generate the identity private key and send the identity private key to the IoT device in a secure way.

4.3. Blockchain Address Generation

Each IoT device in the system is allowed to request an attribute value pair ($prop\_n_i$, $prop\_v_i$) from the AAA using a self-generated address and the identity flag ID of the device. The IoT device first randomly selects $s \in \mathbb{Z}_q^*$ as the key SK_i of the device, then the public key corresponding to this key $PK_i = kG$. To obtain the blockchain address corresponding to this public key, the IoT device can hash the $PK_i \| ID_{dev} \|$timestamp, and finally use the *Base58Check* function to encode the blockchain address obtained, as follows:

$$Address = Base58Check(H_2(PK_i \| ID_{dev} \| timestamp)) \quad (2)$$

This address is used to request an attribute value pair from an attribute authorization authority for an IoT device.

4.4. Attribute Value Pair Application

When an IoT device needs to request an attribute value pair ($prop\_n_i$, $prop\_v_i$), the corresponding attribute authorization authority must verify whether the IoT device can have the attribute value pair on a case-by-case basis. If this verification passes, this attribute authority immediately generates an authorization transaction for the attribute value pair, concatenates the transaction with the current timestamp, performs a hash operation to obtain a hash value, and then signs the hash value, as follows:

$$Sig_{SK_i}(H_1(AA \xrightarrow{(prop_{n_i}, prop_{v_i})} Address||timestamp)) \quad (3)$$

Finally, this attribute authorization authority packages the signature value, transaction, and current timestamp together, and submits it to the federated blockchain.

4.5. Access Control Policy Generation

When an IoT device is registered to an attribute authorization authority, a reasonable access control policy file must be developed by the attribute authorization authority, according to the specific situation, and then the transaction and the current timestamp are concatenated and hashed, followed by signing the hash value, as follows:

$$Sig_{SK_{ID}}(H_1(AA \overset{P_{ID}}{\rightarrow} Address||timestamp)) \quad (4)$$

Finally, the AAA will pack the signature value, transaction, and current timestamp together into Fabric.

4.6. Access Control Revocation

Since the IoT system is dynamic and evolving, the access control policies for the IoT terminal may fail, due to the change in business requirements, then it is necessary to revoke the AC policy of the IoT device by connecting the transaction with the current timestamp for the operation and hashing it, followed by signing the hash value, as follows:

$$Sig_{SK_{ID}}(H_1(AA \overset{P_{ID}}{\leftarrow} Address||timestamp)) \quad (5)$$

Finally, the attribute authorizer will package the signature value, transaction, and current timestamp together, and submit it to the federated blockchain.

5. Access Control Process Management

Suppose there are two IoT devices, one of which is Bob, the data resource owner, and the other is Alice, the data resource requester. When Alice needs to request Bob's data resources, Bob must implement access controls on the data resources owned by him, to block unauthorized IoT devices from illegally accessing the resources of his device, etc. In general, Alice can only gain access to Bob's data resources if the set of attribute value pairs owned by Alice and the current environment attributes, etc., can meet the access control policy requirements set by Bob. The execution flow of the access control protocol between these two IoT devices is shown in Figure 3.

(1) Alice first sends the request message for data resource access to Bob, using the identity information IDA, and then Alice and Bob obtain a session key K_m, using standard identity-based authentication and key negotiation protocols, which is used for identification and encryption when data are exchanged between the data requester and the data owner.

(2) Bob generates a random number ($RN \in Z_r$) and sends it to Alice by merging its own set of access control policy attribute names {*P_pname*}, where {*P_pname*} defines the set of attribute names to be used to access the data resources of the device.

(3) Alice looks up the subset of attribute value pairs ($prop\_n_i$, $prop\_v_i$) $\in S$ from the set of attributes owned by the IoT device, as maintained by the attribute names in {*P_pname*}, where the information of the attribute value pairs in this subset is authorized by the attribute authorization authority to the blockchain address that Alice submitted during the access control request. Alice signs the random number (*RN*) using the private key corresponding to each blockchain address in turn, and then sends the random number (*RN*), together with its own signature and its corresponding public key pair {Sig_{SK} (*RN*), PK_i, ($prop\_n_i$, $prop\_v_i$) $\in S$}, corresponding to each attribute value pair in the attribute value pair set S, to Bob.

(4) Bob first hashes the $PK_i||ID_A$ submitted by Alice, and, by running the *Base58Check* function to encode it, Bob then obtains the blockchain address corresponding to this hash value. Then, Bob looks up the Fabric ledger to obtain the latest data corresponding to the blockchain address, and, if the blockchain address has, indeed, been distributed with attribute value pairs ($prop\_n_i$, $prop\_v_i$) by the Authorization Authority, Bob immediately

uses this corresponding public key PK_i submitted by Alice to verify the validity and legitimacy of the signature value, Sig_{SK} (R), as follows:

$$Ver_{PK}\ (Sig_{SK}\ (RN)) \stackrel{?}{=} RN \tag{6}$$

(5) If all of the above holds, it shows that Alice is, indeed, the owner of the blockchain address, and the attribute value pairs ($prop\_n_i$, $prop\_v_i$) corresponding to the blockchain address are declared in advance by the attribute authority. Bob takes the verified set of attribute value pairs (S, PK_B) and his own identity (ID_B) sent by Alice and invokes the access control determination smart contract on the block to make the determination.

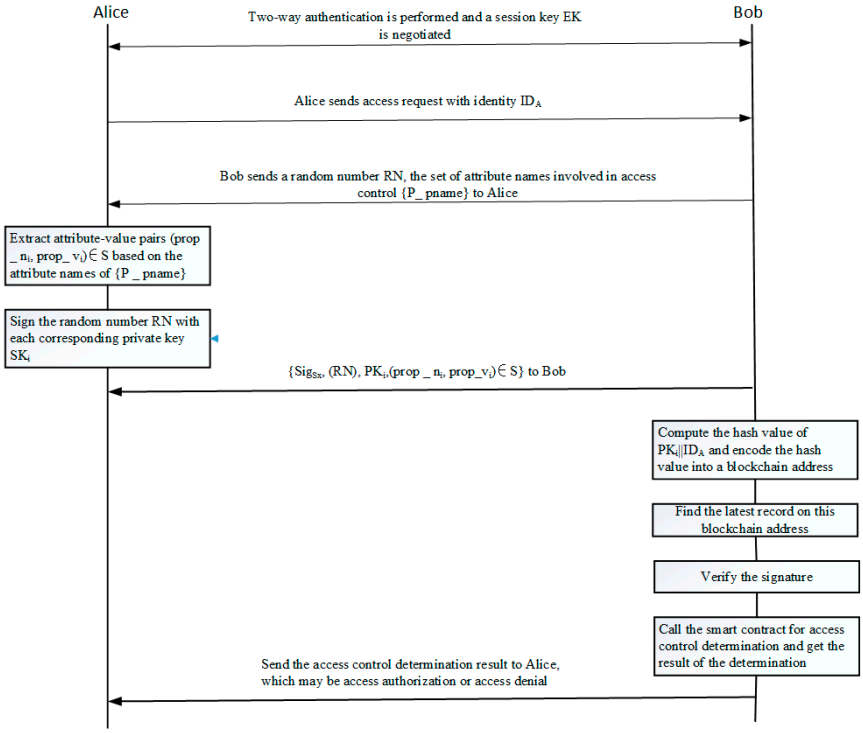

Figure 3. Interaction diagram of access control process between communication parties.

6. Security and Performance Analysis

6.1. Confidentiality

The encrypted transmission of data is achieved with a symmetric cryptographic algorithm [20]. The data resource owner and the data requester use an identification password for authentication and implement the necessary key negotiation to generate a session key; K_m, K_m is a symmetric key that is used to encrypt the transmission of the interaction information between the two parties during the subsequent interaction.

6.2. Performance Analysis Experiment

In order to verify the performance and effectiveness of the proposed solution, this paper analyzed and evaluated the computing and storage performance of the access control scheme. These experiments were conducted under Ubuntu OS. Hyperledger Fabric version 2.0 was used to build the federated chain, and the smart contract algorithm for access control was programmed in Go/Java language. The start operations for the orderer node and peer node are shown in Figure 4.

```
Creating network "docker_test" with the default driver
Creating volume "docker_orderer.example.com" with default driver
Creating volume "docker_peer0.org1.example.com" with default driver
Creating volume "docker_peer0.org2.example.com" with default driver
Creating peer0.org2.example.com ... done
Creating peer0.org1.example.com ... done
Creating orderer.example.com    ... done
Creating cli                    ... done
```

Figure 4. The start of the orderer node and peer node.

Since most of the devices in IoT systems have extremely limited storage resources, the size of the data storage space and the data access performance required for this scenario are important factors to consider. In the scheme proposed in this paper, the IoT devices must store at least four additional types of data locally, including global parameters of the whole system, session keys between the IoT devices, salt values used to generate symmetric keys, and access control policies.

(1) Global parameters of the whole system: The blockchain-based IoT access control system has corresponding global parameters, through which all entities within the system can share data, which contain security parameters, elliptic curves, secure hash functions, authorization authorities for attributes that need to be interacted with, and public keys of the IoT devices. The size of the global parameters is determined after the initialization of the system, and this part of the storage overhead is measured in bytes, which is certainly within the acceptable range.

(2) Session key between IoT devices: To improve the performance of access control across the system, while still ensuring security, a suitable expiration period can be set for the session key of both communication parties. The number of this session key is determined by the number of individual IoT devices and other devices that need to communicate, and, in general, the session key is used as a symmetric key, if the state-secure SM9 encryption algorithm [21] is used. The storage overhead of this part is very small.

(3) Access control policy: A single device keeps an access control policy file, which can be defined based on the Casbin [22] model, and supports common arithmetic, relational and logical operators when defining the matching rules of the policy, making the policy supportive of fine-grained description and powerful expression.

The storage overhead of the file is related to the number of access control policy attributes. In practice, the number of attributes designed for the access control policy of a single device does not exceed 15, and, in this case, only about 200 bytes of space are required, which is obviously an acceptable storage overhead.

The results are shown in Figure 5, which compares the storage overhead with two similar recent solutions.

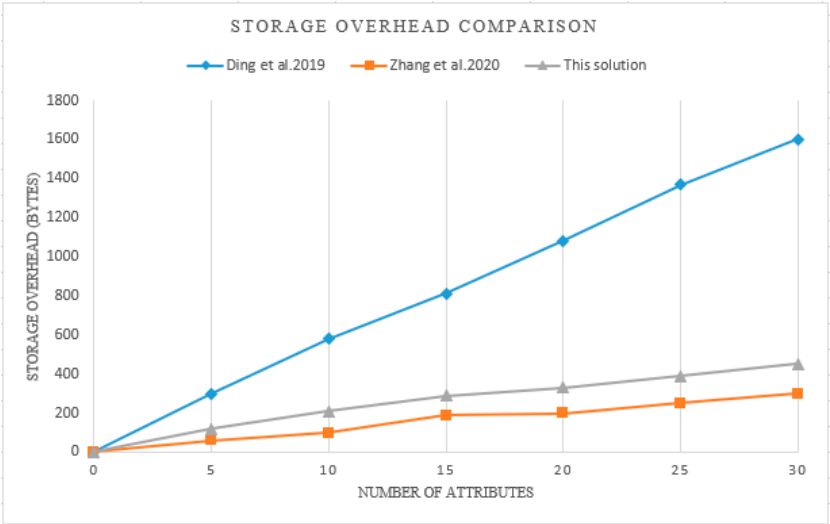

Figure 5. A comparison graph of storage overhead.

From Figure 5, we can observe that the storage performance of the access control methods mentioned in this paper is better than that of schemes such as those in [23]. However, because the scheme of this paper uses attribute value pairs, that is, conditions to describe the ACP policy, while schemes such as those in [24] use attributes to describe the ACP policy, the scheme of this paper is worse than schemes such as those in [24], in terms of the storage overhead, but it is well within the acceptable range.

Compared with two similar schemes, in terms of time cost, the comparison results are shown in Table 1 below.

Table 1. Comparison of time overhead.

Scheme	Time
Ding et al. [23]	19.2 × n
Zhang et al. [24]	25.5
Our scheme	1.6 × m

In terms of the time overhead, this method is significantly better than the other methods because it uses a light-weight access control mechanism and does not involve complex operations; n indicates the number of attributes in the access control policy, and m indicates the number of attribute value pairs or conditions in the access control policy.

7. Conclusions

The IoT access control system, based on the smart contracts designed in this article, combines blockchain with access control technology, solves the problem of centralized trust of central nodes in traditional access control, and improves the reliability and security of access control. The access control model designed in this article can set access control policies for each IoT terminal device, to achieve fine-grained access control and prevent over authorization and unauthorized access. At the same time, the super ledger is used as the blockchain platform to execute smart contracts. Under the condition of retaining the characteristics of blockchain, the system is more flexible and easier to deploy and use, which can meet the needs of large-scale intelligent manufacturing Internet of Things scenarios.

Author Contributions: Conceptualization, P.Z., J.H. and N.Z.; methodology, P.Z. and J.H.; software, N.Z.; validation, P.Z., J.H. and N.Z.; formal analysis, P.Z.; investigation, P.Z.; resources, N.Z.; data curation, N.Z.; writing—original draft preparation, P.Z.; writing—review and editing, J.H. and P.Z.; visualization, N.Z.; supervision, J.H.; project administration, N.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access* **2020**, *8*, 797–800.
2. Bera, B.; Saha, S.; Das, A.K.; Vasilakos, A.V. Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System. *IEEE Internet Things J.* **2021**, *8*, 5744–5761. [CrossRef]
3. Zhao, S.; Li, S.; Yao, Y. Blockchain Enabled Industrial Internet of Things Technology. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1442–1453. [CrossRef]
4. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput. Secur.* **2020**, *97*, 101966. [CrossRef]
5. Corallo, A.; Del Vecchio, V.D.; Lezzi, M.; Morciano, P. Shop Floor Digital Twin in Smart Manufacturing: A Systematic Literature Review. *Sustainability* **2021**, *13*, 12987. [CrossRef]
6. Liu, X.; Liu, Z.; Zhou, M. Fair Energy-Efficient Resource Optimization for Green Multi-NOMA-UAV assisted Internet of Things. *IEEE Trans. Green Commun. Netw.* **2021**, *10*, 1–13. [CrossRef]
7. Elsayed, E.K.; Alsayed, A.M.; Salama, O.M.; Alnour, A.M.; Mohammed, H.A. Deep learning for COVID-19 Facemask Detection using Autonomous Drone Based on IoT. In Proceedings of the 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering, Khartoum, Sudan, 26 February–1 March 2021; pp. 1–5.

8. Sandhu, R.S.; Samarati, P. Access-Control—Principles and Practice. *IEEE Commun. Mag.* **1994**, *32*, 40–48. [CrossRef]
9. Patil, P.; Sangeetha, M.; Bhaskar, V. Blockchain for IoT Access Control, Security and Privacy: A Review. *Wirel. Pers. Commun.* **2021**, *117*, 1815–1834. [CrossRef]
10. Cai, F.; Zhu, N.; He, J.; Mu, P.; Li, W.; Yu, Y. Survey of access control models and technologies for cloud computing. *Clust. Comput.* **2018**, *22*, 6111–6122. [CrossRef]
11. Zhang, P.; Chen, Z.H.; Liu, J.K.; Liang, K.; Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Gener. Comput. Syst.-Int. J. Escience* **2018**, *78*, 753–762. [CrossRef]
12. Imine, Y.; Lounis, A.; Bouabdallah, A. Revocable attribute-based access control in mutli-authority systems. *J. Netw. Comput. Appl.* **2018**, *122*, 61–76. [CrossRef]
13. Liu, H.; Han, D.Z.; Li, D. Fabric-Iot: A Blockchain-Based Access Control System in IoT. *IEEE Access* **2020**, *8*, 18207–18218. [CrossRef]
14. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, *39*, 21260.
15. Alansari, S.; Paci, F.; Sassone, V. A Distributed Access Control System for Cloud Federations. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; p. 2131.
16. Ali, G.; Ahmad, N.; Cao, Y.; Ali, Q.E.; Azim, F.; Cruickshank, H. BCON: Blockchain based access CONtrol across multiple conflict of interest domains. *J. Netw. Comput. Appl.* **2019**, *147*, 102440. [CrossRef]
17. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, 9–11 April 1984; pp. 47–53.
18. Saleem, N.; Abbas, M.; Bin-Mohsin, B.; Radenovic, S. Pata type best proximity point results in metric spaces. *Miskolc Math. Notes* **2020**, *21*, 367–386. [CrossRef]
19. Saleem, N.; Işık, H.; Furqan, S.; Park, C. Fuzzy double controlled metric spaces and related results. *J. Intell. Fuzzy Syst.* **2021**, *40*, 9977–9985. [CrossRef]
20. Cheng, X.; Zhang, Z.; Chen, F.; Zhao, C.; Wang, T.; Sun, H.; Huang, C. Secure Identity Authentication of Community Medical Internet of Things. *IEEE Access* **2019**, *7*, 115966–115977. [CrossRef]
21. Diaz Sanchez, D.; Marin Lopez, A.; Mendoza, F.A.; Cabarcos, P.A.; Sherratt, R.S. TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3502–3531. [CrossRef]
22. Bertin, E.; Hussein, D.; Sengul, C.; Frey, V. Access control in the Internet of Things: A survey of existing approaches and open research questions. *Ann. Telecommun.* **2019**, *74*, 375–388. [CrossRef]
23. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
24. Zhang, Y.; Li, B.; Liu, B.; Wu, J.; Wang, Y.; Yang, X. An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. *Electronics* **2020**, *9*, 285. [CrossRef]