Hindawi
Complexity
Volume 2021, Article ID 5573103, 11 pages
https://doi.org/10.1155/2021/5573103

Research Article

Cloud Trust-Driven Hierarchical Sharing Method of Internet of Things Information Resources

Jianpeng Zhang

Information Management Center, Jilin University of Finance and Economics, Jilin, Changchun 130117, China

Correspondence should be addressed to Jianpeng Zhang; zhangjianpeng@jlufe.edu.cn

Received 28 January 2021; Revised 18 May 2021; Accepted 25 May 2021; Published 4 June 2021

Academic Editor: Wei Wang

Short information sharing time is one of the problems to be solved in the traditional Internet. Therefore, this paper proposes a hierarchical simulation of the Internet of Things sharing structure framework that trusts the cloud to drive Internet information resource sharing. By setting thresholds and iterative adjustment parameters, a complementary judgment matrix is constructed to obtain the minimum nonnegative deviation value and the optimal weight vector. This paper sorts according to the value of the Internet information security model, obtains the optimal model to avoid human tampering, and designs the information resource acquisition process to ensure the reliability of the source data. We use radio frequency identification (RFID) equipment in the preprocessing of massive heterogeneous data in the Internet of Things. In a network environment where resources are limited and heterogeneous are fully considered, the trust-based adaptive detection algorithm is used to evaluate the credibility of the trust-driven algorithm for hierarchical information resource sharing services in the cloud environment of the Internet of Things. We propose a cloud trust-driven hierarchical information resource sharing Internet information resource model. Firstly, the key characteristics of hierarchical information resource sharing are analyzed. Then, a hierarchical information resource sharing model was established by using specific constraints, trust steepness function, cloud trust evaluation criteria, and trust constraint coefficient. Finally, an example of IoT system is designed to verify the effectiveness of the model. Experimental results show that, compared with the traditional model or algorithm, this model has a good hierarchical sharing effect of the underlying resource information.

1. Introduction

Information resource center is the hub between communication and IT information system; that is, information resource center is the collection of information resources. Among them, the most important function is the centralized management and storage of information, so as to realize the centralized benefit of information [1]. The Internet of Things needs to share massive data to facilitate users' use, but the processing capacity of traditional servers has been unable to meet the development needs at the present stage [2]. The overall storage scale of data is large, and the traditional grid technology has problems such as low-resource utilization rate, slow running speed, etc. How to integrate and effectively share these resources has become a hot topic of current research.

This technology is mainly studied from two aspects: one is the research on the underlying technology, including the RFID equipment related to the Internet of Things, the Savant middleware, and the trusted query mechanism, to extract the model of how the Internet of Things resources search for websites. The second is the research on the management of Internet or resources and how to carry out scheduling and computing. The research is based on the trust-driven mechanism. Through the above research, the security positioning under the dynamic information of the Internet of Things is controlled to a certain extent, making it easy to control and unique. This research promotes the dynamic

evolution mechanism to be more perfect and reasonable, and this mechanism has the trust driving relationship in the underlying resources of the network [3]. In such a complex environment, RFID and the Internet share the underlying security mechanism. This still has the problem that the underlying network drive system and trust mechanism cannot be connected, resulting in separation, and there is no unified communication protocol standard between information resource sharing. [4, 5]. Therefore, there is still a long way to go between the above research and the ultimate goal of ideal layering of information resources sharing in the Internet of Things. This is only the first step of the research, especially in the dynamic description of the trust-driven algorithm, which is mainly aimed at multidomain collaboration.

Related research shows that most of the information resource center server utilization is only 10%; the main reason is that the smaller part of the server load and application of the unit is very single, and even some servers in the idle state, so these servers need to be dynamic adjustment, so as to improve server utilization efficiency. Aiming at these problems, the paper proposed an IoT of trust cloud drive method of hierarchical information resource sharing, with the trust-driven platform design, and through the calculation algorithm of particle swarm algorithm to realize the rapid resource sharing, proved by the simulation, the proposed method is effective to overcome the insufficiency of the traditional method, and more satisfactory results were obtained. By taking advantage of the advantages that explicit information resources and hidden information resources (i.e., underlying code) are closely combined with the Internet of Things system, the information resource model of layered sharing of underlying generic information resources driven by cloud trust in the Internet of Things is realized to a certain extent. The first part of the paper is the introduction, the second part introduces the relevant work, the third part studies hierarchical sharing of information resources in the Internet of Things, and the fourth part analyzes the results. The fifth part is the conclusion.

2. Related Work

Internet of Things (IoT) is a next-generation information network that integrates the radio frequency identification technology and sensor technology based on induction equipment into the Internet. Hierarchical sharing technology of information resources has become a hot topic in the research of the Internet of Things [6, 7], which enables items' information to be accurately, safely, and efficiently located and queried. At present, the Internet of things and the underlying information resources information resources sharing layering technology research mainly focuses on two basic aspects: one is about the Internet of things RFID Savant middleware [8], hierarchy, found [9, 10] RFID information service, trusted query mechanism [11], and the Internet information resources in the center of the recognition named or information resources sharing layered model [12]; the underlying technologies such as research put forward is the most representative of Internet information resources sharing layered model; the second is the research on the trust-driven management and scheduling algorithm of Internet resources or cloud resources [13].

The above studies have better improved the dynamic evolution mechanism of the trust-driven relationship among the underlying resources of the network, thus realizing the security positioning of dynamic information resources in the changeable and uncontrollable Internet of Things environment to a certain extent. But on the whole, these studies still lay particular stress on traditional Internet information resources in information resource sharing layers, and owing to the high complexity of Internet resources, based on RFID and the Internet information resources, sharing of the bottom of layer technology is difficult to effectively implement in the complex network environment [14]; overall, the driving mechanism of trust and the Internet of the underlying system, communication protocol, and information resource sharing layered orientation standard is not unified, the underlying single encoding does not agree, trust function definition, and so on. Therefore, compared with the overall goal of hierarchical research on the Internet of Things information resource sharing, the above work is still relatively preliminary. In particular, the dynamic description of trust-driven algorithm of multidomain collaboration is insufficient, and there are few studies on generic or even relatively low-level hierarchical technology of the Internet of Things resource information resource sharing.

Cloud computing is the representative computing model for the development of the Internet (the current Internet of Things supporting environment). In the open cloud environment, RFID can read a large number of item tags with fast speed and short response time, which can meet the real-time and security requirements of the underlying information resource sharing layer of the Internet of Things. Therefore, cloud computing will have a significant impact on the computing environment and application mode of the Internet of Things [15, 16]. Trust based on cloud drive mechanism, on the other hand, as one of the key technologies in the cloud resource scheduling and management, to effectively support the trust of trust decision process, better solve fuzziness and uncertainty in the expression of trust problem [17]; at the bottom of Internet information resources information resources sharing, stratification research is playing an increasingly important role. In multitenant sharing of physical network, the emergence of network resource competition is inevitable; the academic community mainly studies the network resource sharing mechanism based on virtual network under the competition. The traditional way of sharing network resources is based on TCP stream. It is assumed that all the data streams in cloud data centers are based on TCP transmission mode. The number of TCP streams generated by virtual network determines the size of network bandwidth it can obtain in competitive environment [18, 19]. If a cloud tenant's application generates more TCP traffic, then that tenant will get higher bandwidth, which is obviously unfair to other cloud tenants. If the cloud tenant generates UDP stream, UDP is a connectionless service, which will preempt bandwidth resources and affect the network service experience of other cloud tenants [20]. In order to ensure a

certain degree of fairness, the academic circles carry out researches on the fair bandwidth sharing methods with the granularity of virtual machine, cloud service, and cloud tenant virtual data center, respectively. The core idea of the fair bandwidth sharing method with virtual machine as granularity is to realize a distributed congestion control system based on hypervisor and share the link bandwidth proportionally according to all virtual machine flows on the link [21]. The method of realizing congestion control is to rewrite the idle bits of IP packet header. The sender marks the serial number of each packet; the receiver determines the end-to-end packet loss, gets the link congestion status, and gives feedback to the sender. The packet sending rate of each stream is calculated based on the weight of the sender. Gatekeeper made some improvements on the basis work and improved the algorithm of defining link sharing ratio based on single-aspect weight of the sender to a method that takes into account the joint decision of weight of both the sender and the receiver [22, 23]. Considering the time-efficiency of virtual network allocation and the efficient utilization of network resources, heuristic algorithm is usually adopted to improve the allocation time efficiency. According to the different number of mapping stages, it can be divided into two categories: two-stage mapping [24, 25] and single-stage mapping [26, 27]. The two-stage mapping is divided into two stages: node mapping and link mapping. After node mapping, link mapping is completed. Node mapping refers to mapping virtual machines to appropriate physical hosts, while link mapping refers to mapping virtual links between virtual machines in virtual network to physical links. However, the traditional resource reservation method RSVP [28, 29], which provides bandwidth isolation between tenants, requires the storage of a large amount of resource states in the intermediate switch, which is actually not feasible for the large-scale cloud data center that uses commodity switch to network. In addition, RSVP is a static bandwidth resource reservation. Due to the dynamic nature of cloud, the bandwidth demand of cloud tenant application changes dynamically, resulting in the waste of physical network resources. Therefore, there is still a long way to go between the above research and the ultimate goal of the ideal hierarchical sharing of information resources in the Internet of Things. This is only the first step of the research, especially in the dynamic description of the trust-driven algorithm, which is mainly aimed at multidomain collaboration.

3. Hierarchical Sharing of Information Resources in the Internet of Things

In terms of data structure, it can be divided into two platforms at different levels according to their functions, namely, information platform and infrastructure platform. Figure 1 shows the concrete structure of the physical model of the information resource center.

In Figure 1, the bottom layer is cloud trust and information resource collection layer, the middle layer is loading model layer, including secure transmission environment, data acquisition, data mining, load balancing, etc., and the top layer is application service, including reliable trust, information mechanism, and layered application mechanism. According to the different functions of the information resource center resources in the physical model of the information resource center, the IT facilities of the information layer can be called computing resources, which provides a certain environmental basis for the normal operation of data. According to the correlation analysis, the most important computing resource is the server. The server is a high-performance computer in the network environment [30–34], which is responsible for listening to the service requests provided by network clients and providing corresponding services. Therefore, the entire server must have a good capacity to undertake and guarantee the service. The following basic model is built to fully understand the server, through the formula.

(1) The server parameter set shows the parameters needed to be considered in the server design process:

$$T_c = \{T_l, Y_p, H_o\}. \quad (1)$$

(1) *Server Type*. There are many types of servers, so there are differences in their classification criteria. One of the most common classification criteria is classification by server structure.

(2) *Ark*. For the information resource center, the selection of the server first needs to consider the size and power consumption of the server, etc., because the information resource center generally uses large dedicated room for unified deployment and management, so the cabinet server of standard size is selected.

(3) *Comprehensive Performance of the Server*. The server has strict requirements for data throughput and stability, among which the CPU is a comprehensive index to measure the performance of the server as well as the central system of the server. The information resource center can configure the servers according to different requirements.

(4) *Working Environment Requirements*. Due to the server and other related equipment in the process of operation, it will form a larger heat. In order to ensure the safety and reliability of these data, it is necessary to provide the normal operating temperature for the equipment.

Adopting the related ideas of ADP, the layered model of information resources is built. The whole information resource model is divided into time model, Web load model, and information resource center transfer model. The most important function of time model is to obtain the specific evolution process of information resources and information in information resource center.

3.1. Time Model. Server in the center of the information resources played a very important role, so to form a corresponding server model is very important, for a single server, a model of the process seems very simple, but when large, heterogeneous server used together, model of the form will be very difficult, so I need to flatten the server and zoning.

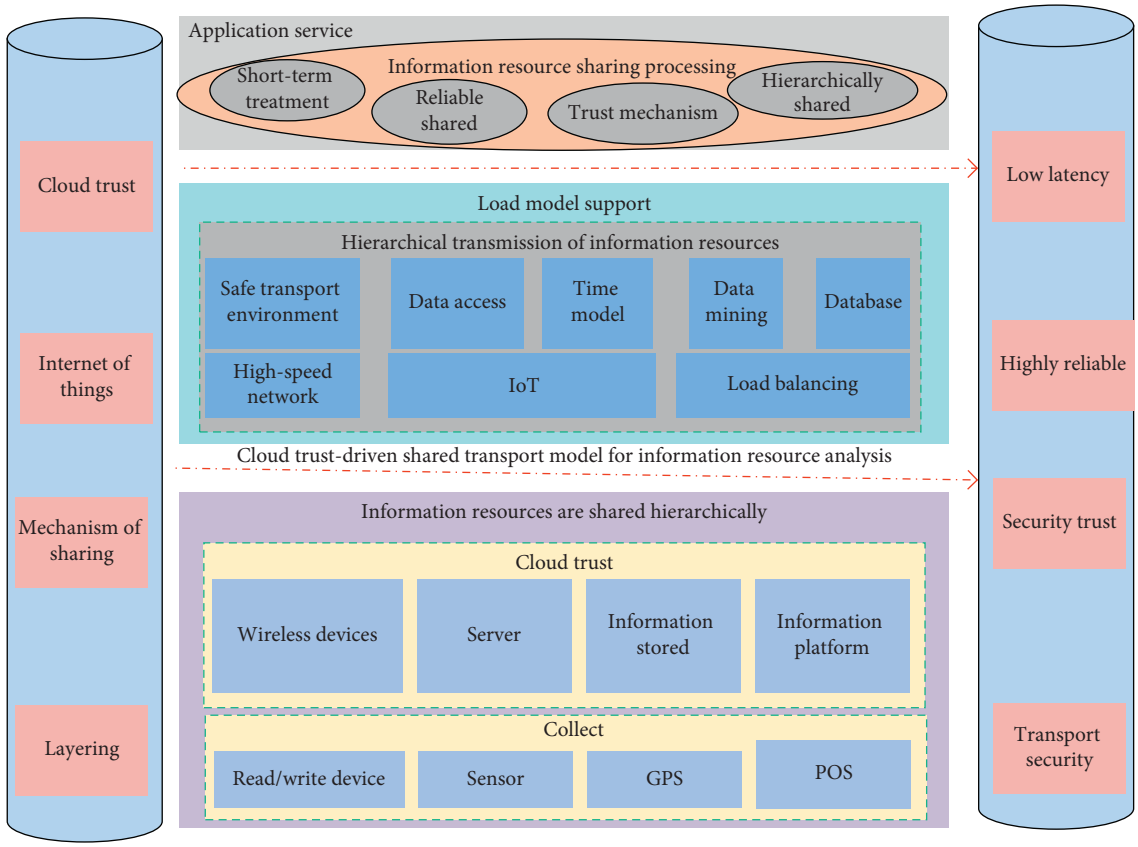

Figure 1: Physical model structure diagram.

After the regionalization process, get the location property of the server. The modeling process of the information resource center is given in detail below. First, important attributes of the server need to be obtained to describe the resource state changes of the server through attributes, and then specific rules of server use are determined to constrain the value of attribute vector space. The specific form of content in the time model is given as follows:

$$T_R = \{T_1, T_2, T_3\},$$
$$T_a = \{a_1, a_2, a_3, a_4\}. \quad (2)$$

3.2. Web Load Model. According to the ADP modeling idea, the task request information can be regarded as the system resource, because the task that the information resource center handles is the load request information. Therefore, the focus is on the cloud trust driver as the basis for modeling. Through the above correlation analysis, it can be seen that the number of servers in most models is determined by the peak of cycle load at this stage. Therefore, at the beginning of each long cycle, the peak of the load needs to be predicted from historical data. Among them, the load task model needs to depict multiple attributes of different aspects, including the static attributes and dynamic attributes of the load task. The operation state of the task can be described in detail through the attribute vector, and the constraint rules of the task execution can also be defined.

The following details give the form of the web load model:

$$R_c = \int t_m \cdot m \cdot \text{lowd}t. \quad (3)$$

3.3. Information Resource Center Transmission Model. For the information resource center, the building facilities provide a certain working environment for it. The following is a detailed description of the established information resource center transmission model.

In addition, in the process of model building, not only the specific name of the information resource center, but also the physical location, total area, total number of floors of the computer room, and the connectivity of the server should be considered.

Through the construction of the above model, the hierarchical research of information resource sharing platform is realized. In order to optimize the performance of the platform, premature convergence in the model should be considered and avoided.

4. Hierarchical Sharing of Information Resources in the Internet of Things Driven by Cloud Trust

In the cloud environment, the most important thing to achieve the goal and network connection is to build the goal

of Internet of Things coding. As the carrier of the underlying information resources, it has a hierarchical structure, which is explicit and implicit, which can be said to be the underlying target of digital informatization. It is mainly realized through data mining technology, through the use of RFID and digital information technology to enable people to access the network through the network.. The function of the encoding structure hierarchy is to map the resolution of item addresses completely by maximizing the tracking of the details encoded in the cloud environment, which is constantly changing and cross-domain. In order to form a rich and relatively fixed representation mode, it is necessary to express the basic inherent information of the target code completely and cooperatively. To a large extent, the Internet of Things limits the computing and storage resources of various sensing devices, such as RFID devices and other nodes. In addition, the efficiency of data computing and storage with certain capabilities or relatively lightweight should be improved, such as wearable intelligent devices. Therefore, a large number of heterogeneous data in the Internet of Things need to be classified and other operations.

Considering that resources of heterogeneous networks are limited, normal nodes in the Internet of Things will legally publish messages on the network, while malicious nodes will illegally publish messages, whether true or false, on the network. Traditional static security mechanism, in order to prevent malicious nodes publish false news as well as to the website of malicious tampering with real news, will add a message authentication code sent to the real message of what has been released on the Internet, so that we can conveniently confirm the data source and relay nodes authentication, to achieve reliable data integrity, to the largest extent, prohibit false news. However, this mechanism is not suitable for the IoT environment, which is dynamic and low power consumption. This method requires the relay node to authenticate all messages, which is very costly and wasteful to resources.

An adaptive detection algorithm is proposed to detect whether there is a malicious node in the Internet of Things, and the overall trust value of the node is greater than the trust threshold. The specific algorithm process is shown in Figure 2.

The system can directly return the nodes whose overall trust value is insufficient or whose trust threshold has been given. Instead, the return will be periodic, but the period is not fixed, but random. The role of trust threshold is to decompose the value of the relay node, which makes the data source authentication on whether the message is received. If the value is set too high, it cannot play the role of saving the node. In contrast, malicious data attacking the node cannot be detected. Therefore, it is still necessary to set up according to the needs of the actual network.

Architecturally, the Internet of Things is composed of three parts: the perception layer, the network layer, and the application layer. The bottom layer is the sensing layer, which is composed of sensors and sensor network. The middle layer is the network layer, which is mainly composed of mobile communication network and Internet. The top layer is the application layer, which refers to intelligent operation and intelligent processing. The sensing layer is composed of sensor node, sensor gateway, and wireless sensor network. It mainly completes the monitoring patient node to form a wireless sensor network in the form of self-organization and transfers the monitoring data to the sensor gateway to complete the collection of information. The network layer is composed of Internet, mobile communication network, information center, and management center. The network layer transmits the information acquired by the perception layer to the information management center by means of wireless communication or wired communication for transmission and processing. Application layer realizes the intelligent processing of data, the use of computers or PDA at any time to view the data, according to the actual situation of the patient to take appropriate measures.

The Internet of Things can capture the computing, storage, and processing power of information from cloud computing. Internet service providers can process tens of millions or even billions of pieces of information in a fraction of a second, achieving the same power as supercomputers, and users can use these services on demand, fulfilling the dream of providing computing as a utility.

Cloud computing services are divided into infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) levels. IaaS is the basic layer of cloud computing services, which encapsulates basic resources into services. PaaS is responsible for dynamic resource expansion and fault-tolerant management; SaaS is the top layer of cloud computing services that encapsulate specific application software functions as services. Cloud computing technology system can be divided into four levels: physical resource layer, virtual resource layer, management middleware layer, and service interface layer. The physical resource layer provides physical facilities services, such as server cluster, memory, network equipment, database, software, etc. The virtualization layer integrates the same type of resources into a homogeneous resource pool, such as computing resource pool, storage resource pool, etc. The management middleware layer is responsible for resource management, task management, user management, and security management. The service interface layer encapsulates cloud computing capabilities into standard WebServices services.

The cloud environment is the management level, also known as the middle layer, which is mainly used to convert the input target coding into explicit resources. This operation requires the support of the open cloud environment to quickly realize the search and evaluation of system resources. The highest level is the Internet of Things environment. It mainly locates the encoded information of the target name, identifies the basic information, and then uses RFID equipment and Savant middleware to identify the formed electronic note (electronic code) encoded by the item in the Internet of Things environment. The hierarchical sharing of information resources based on cloud trust-driven structure is shown in Figure 3.

As can be seen from Figure 3, the realization process of this model is as follows: firstly, the information of the item

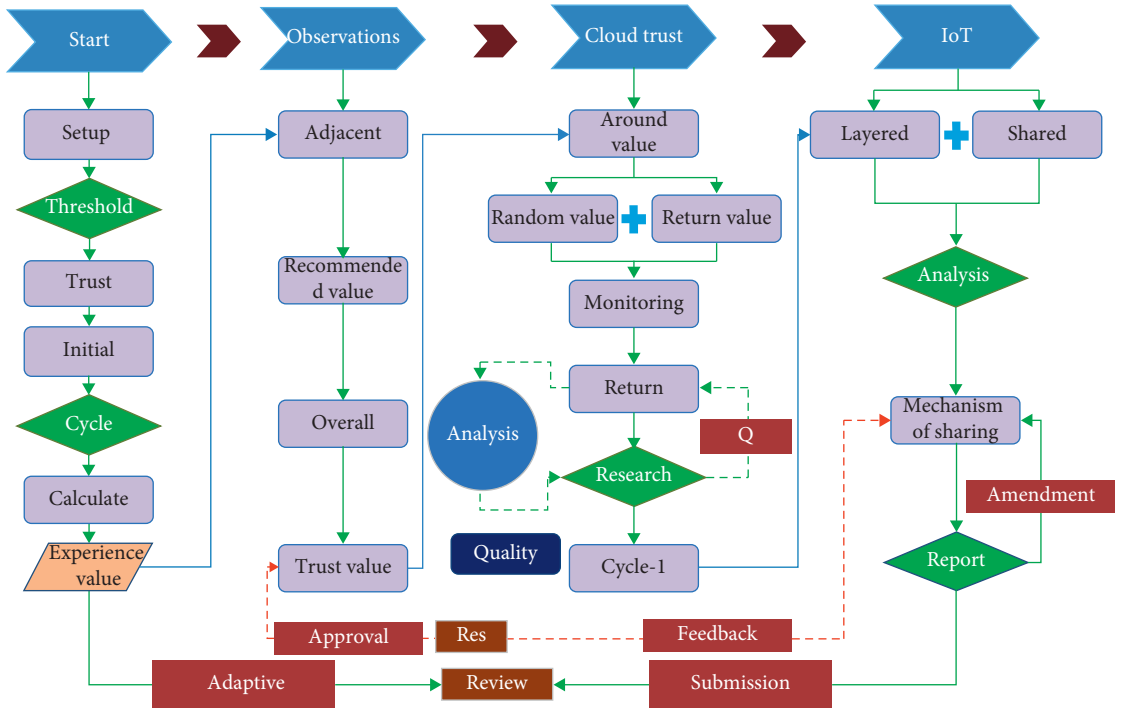

Figure 2: Adaptive detection algorithm based on trust.

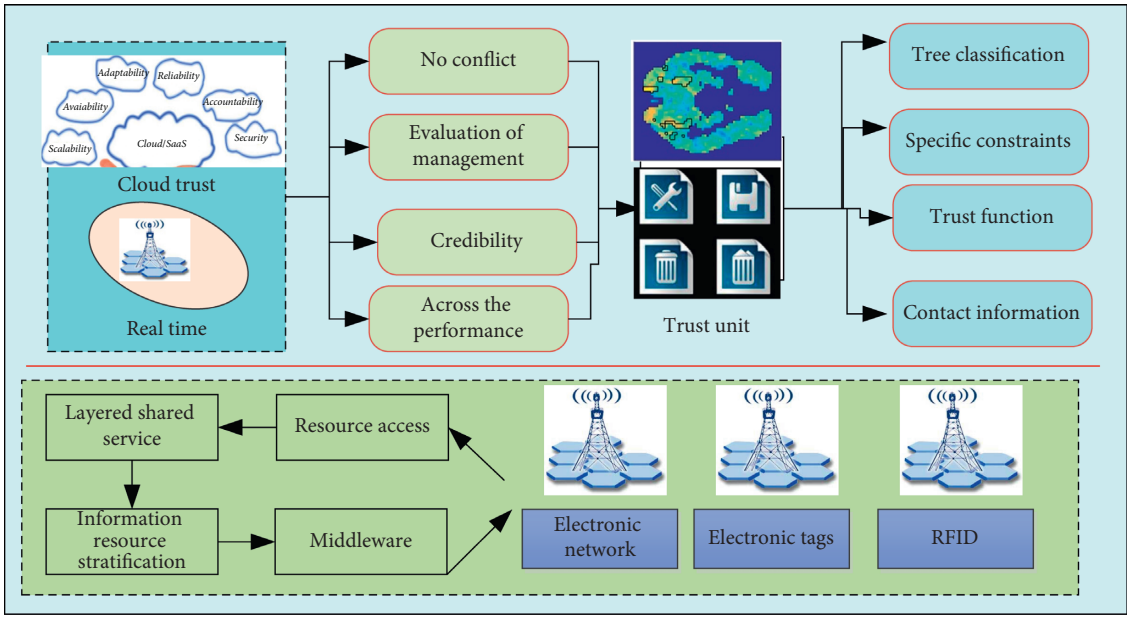

Figure 3: Hierarchical sharing of information resources driven by cloud trust.

shall be collected; then the electronic tag or electronic code of the item shall be formed, and the resource search shall be conducted in the cloud environment. Then, the hierarchical service of information resource sharing under the Internet of Things environment is required. The environment is cross-domain and constantly changing, but this service should be completed with the support of RFID equipment and Savant middleware, and then the explicit information encoded by the item is identified and processed. The hierarchical structure is compliance tree. In order to ensure the compatibility and integrity of information, it is necessary to check the source address of items in the Internet of Things, so as to track the basic information encoded by the target to the maximum extent. This requires that the trust of information in the Internet of Things is based on the trust driving mechanism, and then the invisible information is identified under the RFID device. Finally, the model is evaluated effectively through the feedback result in the cloud

environment, which is the hierarchical service of information resource sharing. A large number of dialog control functions in IRAMCTDIOT information resource sharing layer still need to be provided through the communication management model to achieve many dialog control functions.

5. Results Analysis

Cooja network emulator is used to make simulation, which is carried out under Contiki operating system. The message authentication code generated by Hash-based Message Authentication Mode Minimum Discernible Signal (HMAC MDS) algorithm is used, and the data source is authenticated by combining with TinyDTLS library.

In the process of simulation, information delay is not taken into account. The importance of the previous trust value in the current trust value is the same as that of the newly generated trust value, so the weight factor is set to 0.7. In order to comprehensively evaluate the overall trust value of nodes and avoid the wrong judgement caused by the high proportion of direct experience value, the decline of the overall trust value of normal nodes caused by the mistransmission of messages can be ignored during the simulation. There are three types of attack, and the attack mode and system defense mode are shown in Table 1.

Under attack type 1, the shared time of the two mechanisms is compared and analyzed, and the results are shown in Figure 4. As can be seen from Figure 4, in the case of additional attack, the maximum sharing time is 29 s when the click order of Internet of Things information is login.acpx5 using the traditional method. When the click order of Internet of Things information is login.acpxl, the shortest sharing time is 9.2 s. Using the sharing mechanism studied, the longest sharing time is 78 s when the click order of Internet of Things information is login.acpx6. When the click order of Internet of Things information is login.acpxl and login.acpx9, the shortest sharing time is 42 s.

Experiment focuses on specific constraints increasing, trust constraint coefficients before and after, trust steepness function before and after improvement, cloud trust assessment criteria to improve the performance of the system before and after the change, overall embodied in the underlying information resource sharing a layered credibility, accuracy (magnitude), no conflict and mergence, real time, and changes of the coding performance indexes such as unity. In fact, this implies that the following experimental results need to be achieved: express the one-to-one constraint of the hierarchical service of information resource sharing with specific constraints to avoid the hierarchical conflict of information resource sharing. In order to solve the problem of low trust, the trust value among the low-level information resource sharing hierarchical services is expressed by the cloud trust evaluation criteria. The dynamic description of multidomain collaboration is expressed by the trust-benefit function. The trust constraint coefficient is used to express the constraint of the trust relationship between the hierarchical service of information resource sharing and the underlying information resource and the hierarchical trust constraint of information resource sharing when the underlying information resource is dynamically added or deleted. The experimental comprehensive performance comparison results of various models and algorithms are presented, as shown in Table 2.

From Table 2, experimental results show that, compared with the traditional trust benefit function and cloud credibility assessment criteria, the improved trust benefit function and cloud credibility assessment criteria in the credibility of the information resources sharing layered service, accuracy, no conflict all have good effect, have realized the dynamic multidomain collaborative description, and solve fuzziness and uncertainty in the expression of trust problem. This also reflects actual increase after certain constraint conditions of the underlying information resources sharing service one-on-one constraints of stratification and the underlying information resources dynamically add or delete the trust of the constraints, solving the lack of the constraint condition of subjective trust cloud drive mechanism of information resources sharing layered conflict and the contradiction between low trust.

As can be seen from Figure 5, with the increase of the total system load, the average waiting time of the new method also increases. Specifically, the higher the priority, the shorter the waiting time, while the lower the priority, the longer the waiting time. In the case of the same total system load, the waiting time is proportional to the priority level, and the higher the priority level is, the earlier the system response will be obtained. Compared with the traditional algorithm, the average waiting time is significantly reduced, which is mainly because the algorithm classifies the request and improves the parallelism of the system, while the traditional algorithm only carries out simple first-come, first-served processing on the request, which only guarantees absolute fairness and pays little attention to the scheduling efficiency. Compared with the traditional algorithm, the results of the two algorithms tend to be consistent when the load is low. However, when the load increases, the average waiting time of the new algorithm changes little, mainly because the queue is sorted and the requests with high-comprehension QoS are prioritized. Therefore, on the premise of ensuring service fairness, the model proposed in this paper can ensure that high-priority services get priority system resources and solve the optimal allocation of resources to a certain extent.

Figure 6 shows the average optimal degree of service. The experimental results of each cohort are inversely proportional to the system load, and the lower the grade is, the more obvious the change trend is. Compared with SQOSM algorithm, the average optimal service degree of the new algorithm is maintained at a high level, which is attributed to the classification and scheduling of requests according to the priority of the new algorithm and priority processing of urgent requests, so as to ensure the personalized requirements of the system. Compared with the MQOSM algorithm, the average and optimal service of various types of the system decreases less, which is determined by the processing process of QoS information fidelity. It can be observed from Figure 6 that all kinds of

Table 1: Three attack modes.

No.	Types of attacks	Attacks	Defense mechanism
1	Additional attacks	The attacker generates blocks by creating false information	By verifying the output, false blocks are detected due to asymmetric encryption key management mechanism, which makes it difficult for the interference device nodes to use the unique private key and partial blind name identification algorithm
2	Distributed denial of service attacks	The attacker exploits multiple nodes	
3	Links to attack	An attacker links multiple pieces of data together using the same 1D	

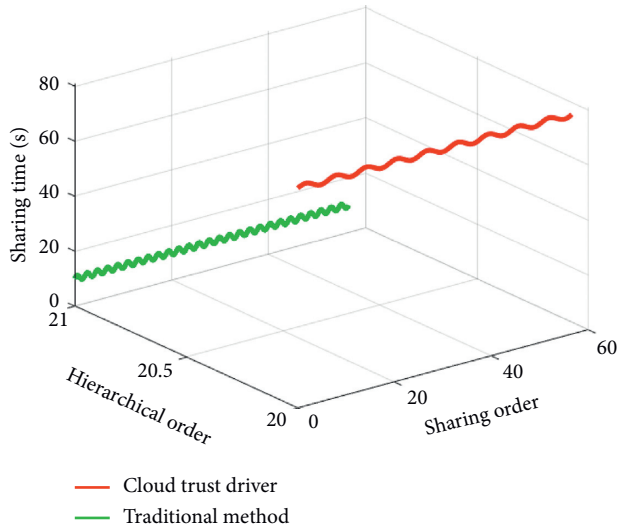

Figure 4: A comparative analysis of the shared time between the two mechanisms under attack type 1.

Table 2: Comparison results of experimental comprehensive performance of various models and algorithms.

Instance	Credibility	Accuracy	No conflict	Across the performance	Real time	Coding unity
Management Reform Act Information Technology (MRAIT)	5.9	10.6	Medium	General	General	Good
Driver Test Manager (DTM)	6.6	8. 2	Good	Good	Medium	General
TableDatacell Hentai Computer Graphics (TDJSHCG)	6.7	8. 1	Good	Medium	Medium	Medium
EAST Block-Coded Modulation (EASTBCM)	7.3	9. 6	Good	Medium	Medium	Good
Cloud trust driver	8.2	11.8	Good	Good	Good	Good

results are higher than 84%, and the comprehensive value is 93%. Therefore, this model can meet the appropriate personalized needs of users.

In order to further verify the superiority of this method, 10 different data-intensive access services were designed by comparing the success rate of service request with the original two algorithms, and the simulation results were compared as shown in Figure 7.

The priority of request service tends to be the same. It can be seen from Figure 7 that the success rate of service request of the three algorithms in the first experiment is roughly equal, equal to 98.8%. However, when the service requests with higher priority are gradually increased, there is a significant difference between the success rate of the original algorithm and the proposed algorithm. Only from the 6th experiment, it can be observed that the success rate of the original algorithm is close to 98.7%, while the success rate of the proposed algorithm is as high as 99.5%. This fully shows that the algorithm in this paper does play an important role in first classifying the service request, then processing the in-queue information, and finally responding to the request with high comprehensive QoS first. All the 10 simulation experiments show that the average success rate of this algorithm is higher than that of the traditional first-come-first-served strategy.

Figure 8 shows the rate comparison diagram of each D2D device when the third and fourth D2D propose QoS service requirements. It is not difficult to see from the figure that when the QoS of the third and fourth D2D devices is low, such that the QoS of the third and fourth D2D devices is 6 bits/Hz/s, it can be achieved even if there is no constraint for each D2D. When D2D QoS constraint is large and then has to sacrifice no QoS constraint, D2D device performance meets the quality of service of D2D switching device. At the same time, it is noted

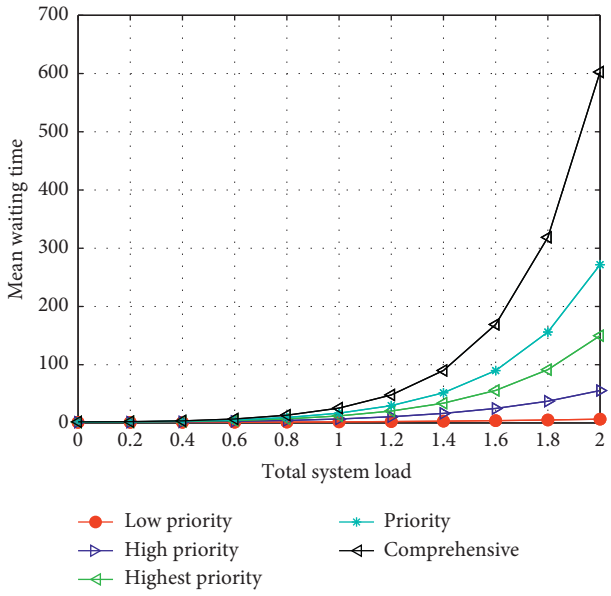

Figure 5: Average waiting time.

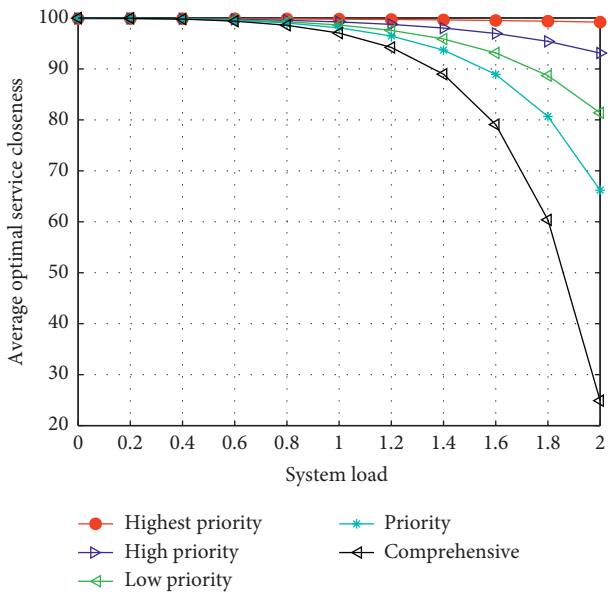

Figure 6: Average optimal service degree.

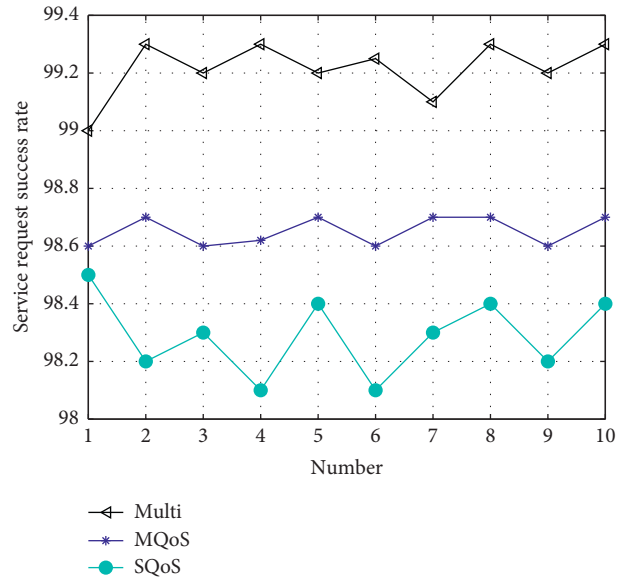

Figure 7: Service request success rate.

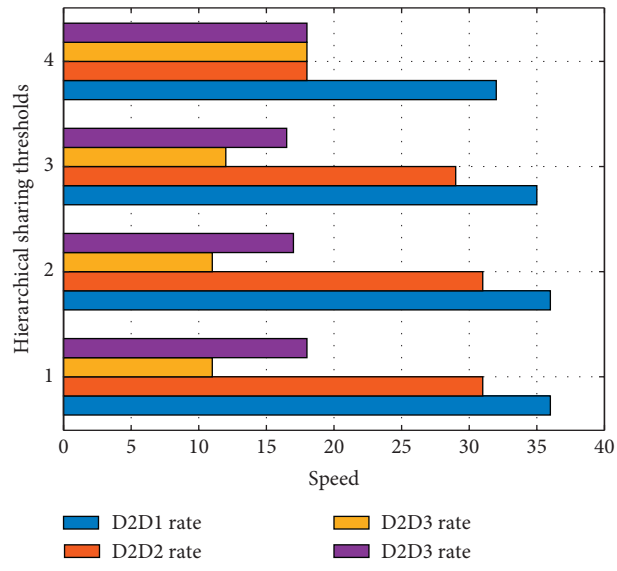

Figure 8: Rate of each D2D under different layer sharing requirements.

that when QoS is from 12 bits/Hz/s to 18 bits/Hz/s, the performance of the first D2D generated to protect the performance of the third D2D drops sharply, even to almost zero. This tells us that in practice, we need to be careful in using D2D devices for QoS requirements; otherwise, the performance of other D2D devices will decline sharply in terms of protecting the user's QoS requirements, and even communication will not be able to be achieved.

6. Conclusion

Hierarchical sharing of information resources of the Internet of Things information is studied, and the simulation innovation of the mechanism is mainly studied. The Internet of Things information is driven by 100 trust, mainly to realize the remote sharing of database information under the Internet of Things architecture, and the sharing is real-time. The user experience can be realized by attracting 100 trusts.

In the self-organizing network, the method proposed in this paper has the high dynamic characteristics of the links between objects, resulting in a very short lifetime. Therefore, to achieve efficient data transmission in this environment is a problem that needs further research in the future. Based on specific constraints and constraints, the trust value of trust cloud drive method makes hierarchical information resource sharing service position accurately; there is no conflict into explicit information resources and recessive information resources at all levels (i.e., the underlying code), thus embodying the driving mechanism of trust cloud and closely combining the advantages of the Internet of things system, to some extent to achieve the cloud trust-driven IoT underlying the general model of hierarchical information resources sharing of information resources. But, given the height of the Internet of things system complexity, the model design of the Internet of things based on the proposed hierarchical information resource sharing system may not apply to all of the information resources of stratified sharing service; sharing service of information resources management and evaluation of communication research is still insufficient; this also is to continue the research direction.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2020.

[2] C Zhang, G. Zeng and H. Wang, Correction to: hierarchical resource scheduling method using improved cuckoo search algorithm for internet of things," *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 1606–1614, 2020.

[3] S. Mu and Z. Zhong, "Computation offloading to edge cloud and dynamically resource-sharing collaborators in Internet of Things," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 13684–12698, 2020.

[4] R. R. Darwish, "A congestion-aware decision-driven architecture for information-centric Internet-of-Things applications," *International Journal of Computers and Applications*, no. 3, pp. 31–44, 2020.

[5] P. P. Jayaraman, C. Perera, D. Georgakopoulos, S. Dustdar, D. Thakker, and R. Ranjan, "Analytics-as-a-service in a multi-cloud environment through semantically-enabled hierarchical data processing," *Software: Practice and Experience*, vol. 47, no. 8, pp. 1139–1156, 2016.

[6] H. Ning, H. Liu, and L. T. Yang, "Aggregated-proof based hierarchical authentication scheme for the internet of things," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 657–667, 2015.

[7] A. Akbarzadeh, M. Bayat, B. Zahednejad, A. Payandeh, and M. R. Aref, "A lightweight hierarchical authentication scheme for internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 7, pp. 2607–2619, 2019.

[8] X. Zhou, T. Xu, and Q. Shi, "Research on highway slope stability based on hierarchical fuzzy comprehensive evaluation method," *IOP Conference Series Materials Science and Engineering*, vol. 569, pp. 32003–32024, 2019.

[9] W. Xia, J. Zhang, T. Q. S. Quek, S. Jin, and H. Zhu, "Mobile edge cloud-based industrial internet of things: improving edge intelligence with hierarchical SDN controllers," *IEEE Vehicular Technology Magazine*, vol. 15, no. 1, pp. 36–45, 2020.

[10] C. Zhang, G. Zeng, and H. Wang, "Hierarchical resource scheduling method using improved cuckoo search algorithm for internet of things," *Peer-to-Peer Networking and Applications*, vol. 12, no. 99, pp. 1606–1614, 2019.

[11] H. Ma and Z. Zhang, "A new private information encryption method in internet of things under cloud computing environment," *Wireless Communications and Mobile Computing*, vol. 2020, no. 6, pp. 51–59, Article ID 8810987, 2020.

[12] S. Jeong, W. Na, and J. Kim, "Internet of things for smart manufacturing system: trust issues in resource allocation," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4418–4427, 2019.

[13] Y. He, S. Zhang, L. Tang, and Y. Ren, "Large scale resource allocation for the internet of things network based on ADMM," *IEEE Access*, vol. 8, pp. 57192–57203, 2020.

[14] R. Rani, S. Kumar, and U. Dohare, "Trust evaluation for light weight security in sensor enabled internet of things: game theory oriented approach," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8421–8432, 2019.

[15] J. Sathish Kumar and M. A. Zaveri, "Hierarchical clustering for dynamic and heterogeneous internet of things," *Procedia Computer Science*, vol. 93, pp. 276–282, 2016.

[16] M. S. Pour, A. Mangino, K. Friday et al., "On data-driven curation, learning, and analysis for inferring evolving internet-of-things (IoT) botnets in the wild," *Computers & Security*, vol. 91, pp. 101707–101723, 2020.

[17] B. Li, X. Sun, and S. Yu, "Designing of internet of things sensor based information gateway using SDN concept," *International Journal of Distributed Systems and Technologies*, vol. 10, no. 1, pp. 13–24, 2019.

[18] X. Yin, S. Li, and Y. Lin, "A novel hierarchical data aggregation with particle swarm optimization for internet of things," *Mobile Networks and Applications*, vol. 24, no. 6, pp. 928–944, 2019.

[19] B.-N. Yan, T.-S. Lee, and T.-P. Lee, "Mapping the intellectual structure of the Internet of Things (IoT) field (2000-2014): a co-word analysis," *Scientometrics*, vol. 105, no. 2, pp. 1285–1300, 2015.

[20] E. A. Abdellaoui Alaoui, S. C. KOumetio Tekouabou, K. O. Tekouabou, A. Gallais, and S. Agoujil, "DTN routing hierarchical topology for the internet of things," *Procedia Computer Science*, vol. 170, pp. 490–497, 2020.

[21] C. Qin, J. Du, J. Wang, and Y. Ren, "A hierarchical information acquisition system for AUV assisted internet of underwater things," *IEEE Access*, vol. 8, pp. 176089–176100, 2020.

[22] Y. Yang, H. Zhang, D. Yuan et al., "Hierarchical extreme learning machine based image denoising network for visual Internet of Things-ScienceDirect," *Applied Soft Computing*, vol. 74, pp. 747–759, 2019.

[23] L. Guo, J. Wang, and W.-C. Yau, "Efficient hierarchical identity-based encryption system for internet of things infrastructure," *Symmetry*, vol. 11, no. 7, pp. 913–932, 2019.

[24] J. He, Z. Zhang, and M. Li, "Provable data integrity of cloud storage service with enhanced security in internet of things," *IEEE Access*, vol. 9, pp. 6226–6239, 2018.
[25] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile edge computing and networking for green and low-latency internet of things," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 39–45, 2018.
[26] Y.-T. Lee, W.-H. Hsiao, Y.-S. Lin, and S.-C. T. Chou, "Privacy-preserving data analytics in cloud-based smart home with community hierarchy," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 2, pp. 200–207, 2017.
[27] Y. Peng, A. Tan, J. Wu, and Y. Bi, "Hierarchical edge computing: a novel multi-source multi-dimensional data anomaly detection scheme for industrial internet of things," *IEEE Access*, vol. 7, pp. 111257–111270, 2019.
[28] S. Chen, H. Wen, J. Wu et al., "Internet of things based smart grids supported by intelligent edge computing," *IEEE Access*, vol. 7, no. 1, pp. 74089–74102, 2019.
[29] L. Yang, C. Ding, M. Wu, and K. Wang, "Robust detection of false data injection attacks for data aggregation in an Internet of Things-based environmental surveillance," *Computer Networks*, vol. 129, no. 24, pp. 410–428, 2017.
[30] J. A. Okoye, I. E. Achumba, K. C. Okafor, and O. U. Oparaku, "Baseline parametric survey on causes of traffic congestion in datacenter networks," *Circulation in Computer Science*, vol. 1, no. 1, pp. 21–29, 2016.
[31] W. W, X. Xia, M. Wozniak, X. Fan, R. Damaševičius, and Y. Li, "Multi-sink distributed power control algorithm for Cyber-physical-systems in coal mine tunnels," *Computer Networks*, vol. 161, pp. 210–219, 2019.
[32] W. Li, I. Santos, F. C. Delicato et al., "System modelling and performance evaluation of a three-tier Cloud of Things," *Future Generation Computer Systems*, vol. 70, pp. 104–125, 2017.
[33] J. Yang, J. Zhou, Z. Lv, W. Wei, and H. Song, "A real-time monitoring system of industry carbon monoxide based on wireless sensor networks," *Sensors*, vol. 15, no. 11, pp. 29535–29546, 2015.
[34] Y. Lin, J. Yang, Z. Lv, W. Wei, and H. Song, "A self-assessment stereo capture model applicable to the internet of things," *Sensors*, vol. 15, no. 8, pp. 20925–20944, 2015.