ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

Key technologies of Secure Multi-Party Computing for Perceived Data Transmission in Internet of Things

Haijun Xu

Shenzhen Zheyang Technology co., LTD, Shenzhen, 518000, Guangdong, China
navyxu-cn@qq.com

Abstract: *With the "wisdom of the Earth, connected to physical objects" makes it independent from the Internet gradually connected to the network and the Internet of Things. Internet of Things is another industrial upgrading of information industry after computer and mobile communication. The Internet of Things is based on the Internet. It uses technologies such as RFID, sensors and wireless sensor hardware to build a network information system covering all people and things in the world. It enables human economic, social life, production and operation and personal activities to operate in the intelligent Internet of Things. As an important support of national strategic emerging industries, the Internet of Things is the core and foundation of smart cities, national defense and intelligent manufacturing industries, and multi-domain, open and security are the theoretical requirements of the application of the Internet of Things. Aiming at the resource fragmentation problems caused by the closure of traditional the Internet of Things architecture, such as closure, tight coupling, poor scalability, and some security problems for the open sharing of the Internet of Things resources, this paper proposes an improved multi-domain Web of Things (MWoT) architecture based on the relevant standards of the Web of Things (WoT) architecture. Some related technologies, such as Internet of Things identification and edge cloud computing, are used to realize cross-domain sharing of Internet of Things resources and cross-domain collaboration of services, as well as to solve the problem of data transmission security.*

Keywords: *Internet of Things, Network Information System, Internet of Things Identification, Edge Cloud Computing.*

1. Introduction

The Internet of Things [1-2] is the national strategy and the core and foundation of the major industries such as smart cities, industrial control, and military defense and so on. With the development of the Internet of Things, multi-fields, the public, openness and security have gradually become the basic characteristics of the Internet of Things.

The development trend of the Internet of Things can be summarized as ubiquitous and ubiquitous. To realize the open sharing of resources in the Internet of Things, but reducing the access threshold of resources in the Internet of Things makes the Internet of Things system more vulnerable to attacks. Especially in the multi-domain The Internet of Things scheme [3], the Internet of Things system has many components, widely distributed, and different definitions of privacy in various fields, which makes the security problems faced by the Internet of Things more serious. This is mainly reflected in two aspects: (1) access control of resources: in the multi-domain The Internet of Things scheme, the definition of sensitive data is different in different industries, and there are different requirements for the openness of resources. These requirements increase the difficulty of resource access rights management. A resource permission management framework for the Internet of Things is needed, which can refine the whole resource of the Internet of Things and dynamically set access rights to any resource. Guarantee the legitimate use of resources. (2) System intrusion detection: In the multi-domain The Internet of Things scheme, The Internet of Things system has many modules and a wide range of distribution. The physical and network environments of each domain are different. Natural or human factors can easily lead to server downtime and hard disk damage. As many system components are deployed in different corners of the Internet of Things, attackers can easily find breakthroughs to break the system. Illegal operation and multi-domain Internet of Things system is huge. It is difficult for operation and maintenance managers to find intrusions and find them in time. It causes immeasurable

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

loss to users.

Current WoT studies [4-5] still focus on resource opening and sharing in multi-domain scenarios, small and medium-scale single-domain scenarios. To study large-scale heterogeneous devices, high concurrent resource access and complex security issues, the Internet of Things service delivery platform for large-scale scenarios relies on a large amount of funds to build strong cloud support. It is difficult to implement and requires low cost implementation, which is suitable for WoT architecture in multi-domain Internet of Things. Aiming at the problems of tight coupling, high independence between systems and closed architecture of the Internet of Things in multi-domain scenarios, this paper studies related technologies such as Internet of Things identification [6-7], edge cloud computing [8-9]. Based on the relevant technical standards of WoT architecture, a MWoT architecture for multi-domain scenarios is proposed, which breaks the information independence between applications and achieves cross-domain sharing of resources and services of the Internet of Things. Coordination. The openness of MWoT architecture leads to user privacy disclosure. This paper presents a framework of MWoT privilege management. Through the triple authentication and authorization mechanism of platform, sub-domain and user, the fine-grained management and control of access privileges of resources in various domains can be realized. To protect user privacy and data security, a high availability system deployment scheme integrating backup, storage and monitoring is proposed to solve the problem of multi-domain scene system with many modules, wide distribution and high reliability. Redundant backup is used to solve the problem of data loss caused by natural disasters and man-made damage, and hybrid storage is used to improve the efficiency of data storage and query.

Based on the above technologies and methods, MWoT architecture in multi-domain scenarios is designed and implemented, and an open platform for micro-target sharing is developed. A single domain can support access to millions of devices. Experiments show that the functions and technical indicators of the Internet of Things gateway meet the requirements of the Internet of Things security supervision platform. The information encryption algorithm of the Internet of Things also ensures the safe transmission of the information of the Internet of Things. The gateway of the Internet of Things implements data conversion between general protocols in the existing Internet of Things, and each communication module adopts the idea of modular design. It can be used not only in security monitoring system, but also in most Internet of Things network environments.

2. Internet of Things Related Technologies

The World Wide Web of Things (WWIT) is an implementation mode of the Internet of Things, which provides a way to open resources and improve the utilization of resources. Compared with the traditional Internet of Things, WoT based on Web technology can integrate and communicate with other Web-based systems. It has incomparable advantages in openness. But WoT's open design reduces the participation threshold of the Internet of Things and improves the utilization rate of resources, at the same time, it is easier to expose the defects of the Internet of Things system, which makes the security of the Internet of Things face more severe challenges.

2.1. Web-based Internet of Things Business Environment

In essence, the Internet of Things connects the only identifiable objects in the physical world by using Internet technology. It provides The Internet of Things services based on these objects and the data generated by the objects. Therefore, it is necessary to uniquely identify the huge amount of resources to realize the open sharing of the Internet of Things.

The idea of identifying physical objects has been widely used in the real world, such as identifying network cards through MAC addresses and mobile phones by SN serial numbers. These entities correspond to and correlate with each other. There are also some technologies for identifying virtual objects in the information world, the most common of which is through unified resource locators (URLs).) To identify network services. Identity is not only used to uniquely identify an object, but also may contain attribute information of the associated object for describing the identified object. At present, the identification of the Internet of Things can be divided into three categories: the object identification of the Internet of Things, the communication identification of the Internet of Things and the application identification of the Internet of Things. The object identification of the Internet of Things is mainly used to uniquely identify the physical object or the logical object of the information world, such as uniquely identifying a sensor of the Internet of Things through the MAC address. IPv4, IPv6 and so on are used to identify the network nodes with communication capabilities. Internet of

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

Things application identification is mainly used to identify the applications of the Internet of Things, among which URI and DOM are the most common.

With the development of the Internet of Things industry, all kinds of Internet of Things services and industry applications will be applied on a large scale, and the interaction between entities in the physical world and virtual objects in the information world will be more frequent, which requires the identification technology of the Internet of Things to establish an effective and unique distinction between massive objects. At present, the technical standards of the Internet of Things in China are not uniform, and there is a lack of a complete set of Internet of Things. The unified management system of logos is difficult to achieve cross-system, cross-industry and cross-domain information exchange. Although a series of technical schemes have been formulated to solve this problem in China, there are still many problems to be solved urgently in the face of the interconnection and interoperability of massive resources in the multi-domain and large-scale scenarios is shown in Figure 1.

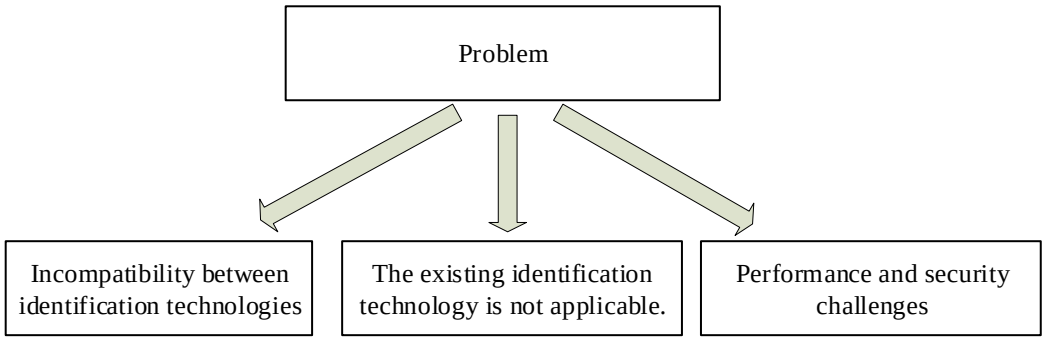

Figure 1: Existing problems

Incompatibility between identification technologies: At present, many kinds of identification technologies coexist in China, and some identification technologies have been applied in a certain range and provide perfect identification services for their respective application areas. However, these identification technology architectures cannot be compatible with each other. In a multi-domain scenario, information exchange between different industries is required, and Internet of Things identification technology architecture compatible with different industries is needed to provide support for cross-domain collaboration of Internet of Things services.

The existing identification technology is not applicable: only a few of the existing identification technology architecture of the Internet of Things are designed for the Internet of Things industry at the beginning, so the existing identification technology directly applied to the Internet of Things will have inherent technical defects, especially in the multi-domain scenario, the application and service types of the Internet of Things are increasing, and the limitations of the existing standard technology will become more and more obvious.

Performance and security challenges: The identification technology of the Internet of Things is currently in the stage of continuous improvement, and has not been fully considered in terms of performance and security. Especially in multi-domain scenarios, the massive hardware and software resources of the Internet of Things need to be identified. The identification resolution server needs to provide real-time addressing and discovery services for these objects, and to ensure that Internet of Things applications and services are secure and reliable.

2.2. Internet of Things Architecture

The definition of the Internet of Things is dynamic and expanding. At present, the earliest known Internet of Things at home and abroad is the sensor network proposed by the United States in 1999. After that, the International Telecommunication Union redefined the Internet of Things. With the development of the Internet of Things technology, the definition of the Internet of Things has already exceeded the above scope, and the architecture of the Internet of Things [10] has changed with the expansion of the definition. At the beginning of the development of the Internet of Things, the industry scale is small, the number of access devices is small, and the industry demand is single. Therefore, most Internet of Things service providers adopt vertical Internet of Things architecture solutions to develop specific Internet of Things applications for specific industry needs. They can provide Internet of Things services well in small-scale scenarios, enough to meet the specific needs of various industries at that time, vertical Internet of Things. The architecture is shown in Figure 2.

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

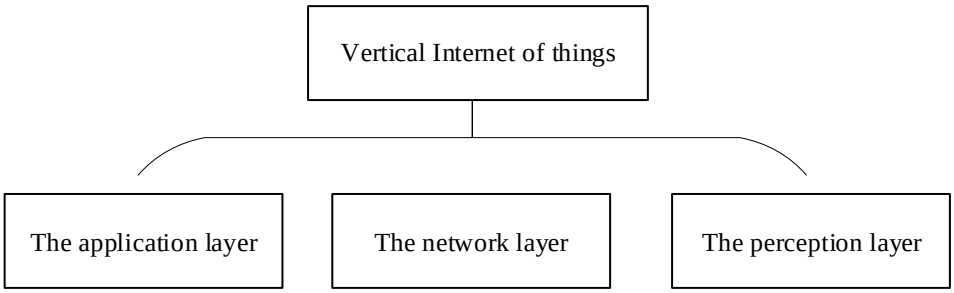

Figure 2: Vertical Internet of Things Architecture

Perception Layer: Including data acquisition devices and short-distance transmission network. It is at the end of the Internet of Things. It has the ability of comprehensive perception. It collects real-time information of the physical world. It is simply encapsulated and uploaded to the network layer through heterogeneous networks. Network layer: The network layer parses, processes and stores the data uploaded by the perception layer. This layer is the interactive channel between the perception layer and the application layer. It manages the perception layer devices and the data generated by them, shields the differences of the perception layer devices, opens a unified resource access interface for the application layer, and provides service support for the upper application layer. Application layer: Web site, mobile app, desktop client and so on all belong to this layer. This layer directly interacts with user, analyses and processes the original data provided by the network layer, develops customized applications according to users' needs and realizes intelligent management and services in combination with specific application scenarios. The development and deployment of Internet of Things applications are completely completed by third-party developers, developers. It does not need to care about the implementation principle of the network layer and the perception layer. It only needs to face the unified interface development of the network layer and focus on the implementation of the business logic of the Internet of Things application.

Vertical Internet of Things architecture is simple and easy to implement, which plays a positive role in promoting the development of the Internet of Things in the early stage. With the continuous expansion of the scale of the Internet of Things industry, a large number of Internet of Things services and applications have been deployed in various industries, and the limitations of vertical architecture have gradually emerged. Vertical Internet of Things architecture applications are independent of each other, data is difficult to share, and managers are difficult to manage a large number of Internet of Things applications in a unified manner; the number of sensor layer nodes deployed in various industries increases dynamically, and the performance requirements of the Internet of Things system are increased, which requires the system to be scalable; the diversification of industry needs requires application developers to develop personality quickly according to their needs. However, the application layer and equipment layer of the traditional vertical Internet of Things are tightly coupled, and the reusability of each module is low, resulting in a long application development cycle. In summary, the traditional vertical Internet of Things architecture is closed, poor scalability, low modular reusability, and it is difficult to meet the new needs of industry users.

2.3. Internet of Things Security

At present, the industry is generally based on the three-tier architecture of the Internet of Things to provide a platform for Internet of Things services. In order to make problem analysis more pertinent, this paper abstracts data processing, data storage and other supporting services in application layer and network layer into service layer. Next, we will analyze the perception layer, network layer, service layer and application layer.

Perception Layer Security: The number of sensor devices in the Internet of Things is huge, processing capacity is low, functions are single, and even many devices are deployed in remote areas where no one is on duty. These characteristics make it difficult for managers to manage these massive devices in a unified way, resulting in many security problems: 1) nodes are easy to eavesdrop and control: due to cost constraints, most of the sensing devices in the Internet of Things have low performance and are difficult to support. With complex security algorithms, nodes are easy to be eavesdropped by attackers, resulting in information leakage, and even malicious control by attackers, resulting in serious security incidents. 2) Node camouflage: Internet of Things network has the characteristics of multi-mode heterogeneity, complex and changeable topology, once an attacker acquires the authentication information of a node, it is easy to disguise as a legitimate node to join the

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

network. Normal perception nodes establish connections and carry out various illegal operations; 3) Physical damage: the number of perception nodes is huge, many of them are deployed in harsh natural environment, unattended, vulnerable to natural disasters, man-made damage and other effects, resulting in equipment damage, increasing the difficulty of equipment maintenance and management.

Network layer security: Compared with the traditional Internet, Internet of Things network topology is complex and diverse, and faces more security problems in the network. The main manifestations are as follows: 1) inherent problems of communication network: the Internet of Things is an extension of the Internet, so the vulnerabilities of Internet protocols still exist in the Internet of Things, such as denial of service attacks, virus intrusion, and so on; 2) communication protocols; Compatibility issues: Many existing communication protocols are not designed for the use of the Internet of Things environment at the beginning, and are not suitable for communication between sensor devices. Direct application in the Internet of Things will lead to many compatibility problems, which will easily expose more security vulnerabilities. 3) Multimode heterogeneity of communication networks: the Internet of Things has the characteristics of multi-mode heterogeneity. Multiple networks coexist and provide services. Miscellaneous network environment is more likely to produce security vulnerabilities; 4) Performance pressure: Internet of Things data has the characteristics of massive, real-time, high concurrency, a large number of data transmission brings tremendous pressure to the network, prone to network congestion and other issues.

Service layer security: The service layer mainly provides support services to the upper layer. The data collected by the sensor layer nodes are uploaded to the service layer through the network layer, and are parsed, processed and stored by the service layer. Based on these data, a series of services are extended and encapsulated as standard interfaces for upper application invocation.

Application-level security: The open nature of the Internet of Things reduces the difficulty of application development, but at the same time leads to confusion in application development, lack of uniform specifications and uneven application quality. It is mainly reflected in the following aspects: 1) user resource access rights; 2) user privacy issues; 3) malicious applications.

Internet of Things has penetrated into all aspects of human life. Intelligent families, intelligent parks, mobile payment and so on are the results of Internet of Things technology support. Therefore, once the Internet of Things security incidents occur, users' privacy data will be leaked at a low level, and huge property losses will be caused. Safety first is the most critical origin of the Internet of Things. Then.

3. MWoT Multi-Domain Architecture Design

The core of MWoT is the cross-domain sharing of resources. Through mature Web technology, sensors, data generated and extended services in the physical world are abstracted into a unified resource model to access the Internet, forming an open and shared business environment, reducing the access and access threshold of resources in the Internet of Things, and realizing cross-domain sharing of resources and cross-domain collaboration of services in the Internet of Things.

3.1. MWoT Proposal and Demand

Traditional Internet of Things applications are mostly developed for specific scenarios, with closed architecture and confused standards, which make it difficult to realize the interconnection between applications and give full play to the potential value of Internet of Things resources. Tight coupling between system modules, low reusability, difficult application development and long cycle limit the development of the Internet of Things. To solve these problems, WoT architecture based on Web has been proposed, which solves the problems of closed, tight coupling and poor scalability of traditional The Internet of Things architecture. Through the design of unified resource modeling and open interface, the fine-grained access of The Internet of Things resources has been realized, and a more open The Internet of Things environment has been constructed. However, with the wide application of Internet of Things technology, the number of access devices increases rapidly, and the data generated increases exponentially. Computing-centric WoT architecture has been difficult to meet the performance requirements of the Internet of Things. Amazon, Microsoft, Alibaba and other enterprises rely on high investment to purchase hardware devices and build strong cloud support to provide performance assurance for the Internet of Things system. Obstacles, in order to meet the user's performance requirements for the Internet of Things, however, for small businesses, universities, and

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

entrepreneurial teams, only through the purchase of cloud services at high prices to build the Internet of Things service delivery platform, so the traditional WoT architecture in large-scale scenarios, especially in multi-domain scenarios, has high implementation costs and poor operability.

The overall goal of MWoT architecture is to achieve rapid access to Internet of Things devices, secure and controllable data interaction, fine-grained access to Internet of Things resources and cross-domain sharing in a multi-domain scenario, with low cost, easy implementation and strong operability is shown in Figure 3.

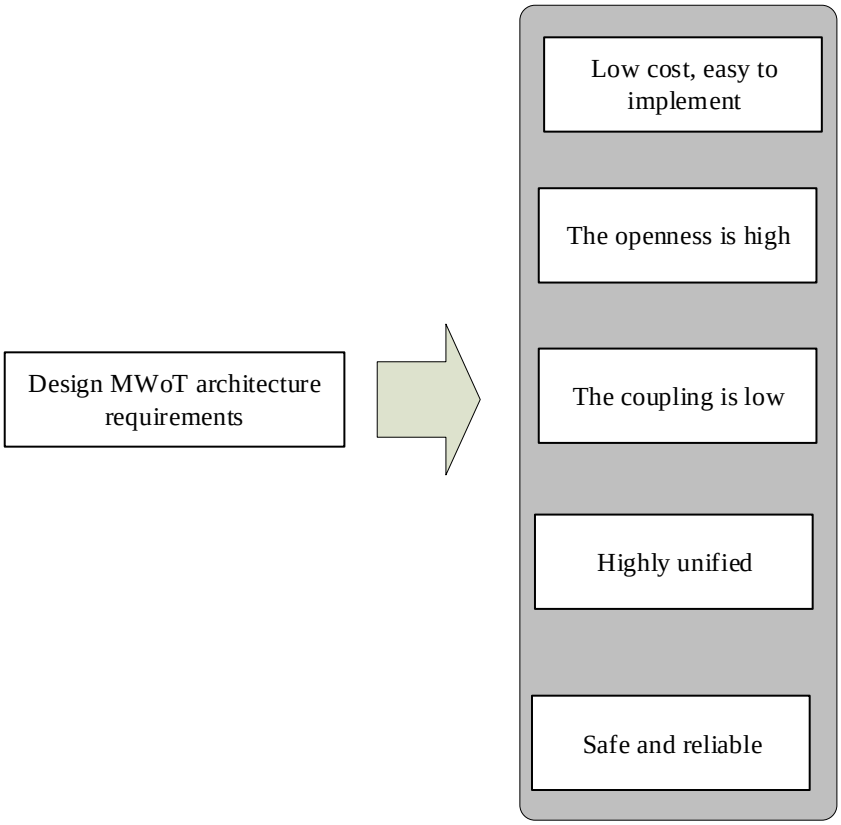

Figure 3: Design of MWoT Architecture Requirements

(1) Low investment and easy implementation: Based on this architecture, the cost of implementing the Internet of Things service delivery platform is small and easy to implement. Small and medium-sized enterprises, universities and start-up teams can quickly build a sub-domain system of the Internet of Things based on this architecture to provide services for the domain.

(2) High openness: MWoT architecture is an open architecture. In principle, there are infinite subsystems of the Internet of Things based on MWoT architecture. Various Internet of Things teams realize the entire Internet of Things ecosystem. After successfully building a multi-domain management center, any team can implement a subsystem based on MWoT architecture and become part of the entire platforms for the whole Internet of Things service delivery. Sub-domains cannot only open resources to the entire Internet of Things platform, but also enjoy the services provided by other sub-domains, and the normal operation of the entire Internet of Things service delivery platform will not be affected by the entry or exit of any sub-domains.

(3) Low coupling degree: low coupling degree is reflected in various aspects. Firstly, the coupling degree between The Internet of Things application based on the interface of The Internet of Things platform and sub-domains and heterogeneous resources is low, and any application can be used in any sub-domains. Low coupling degree between sub-domains does not affect the normal operation of the whole The Internet of Things service delivery platform. Because of the low coupling degree, users can only modify the relevant modules without affecting the normal operation of other modules when they put forward new requirements.

(4) Highly unified: The MWoT architecture needs to establish perfect standards. It can model and uniquely identify all the sub-domains, nodes, data, applications, services, users and other resources joined in the Internet of Things service delivery platform, and integrate all the resources participating in

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

the platform, so as to open up a unified interface and realize the interconnection and open sharing of all things.

(5) Safety and reliability: In multi-domain scenarios, the number and distribution of distributed architecture modules are large, and the system is more vulnerable to natural disasters and human destruction, resulting in server downtime, data damage and other issues. Perfect data backup and data recovery mechanisms and accurate intrusion detection methods are the basis to ensure that MWoT can provide stable and reliable services.

3.2. MWoT Multi-Domain Architecture Design

As shown in Figure 4, the MWoT architecture is characterized by multi-domain collaboration and cross-layer linkage. MWoT breaks down barriers between domains and realizes open sharing of resources and services in the Internet of Things. It mainly embodies cross-regional management of equipment, cross-industry collaboration of services and vertical cross-layer linkage of resources.

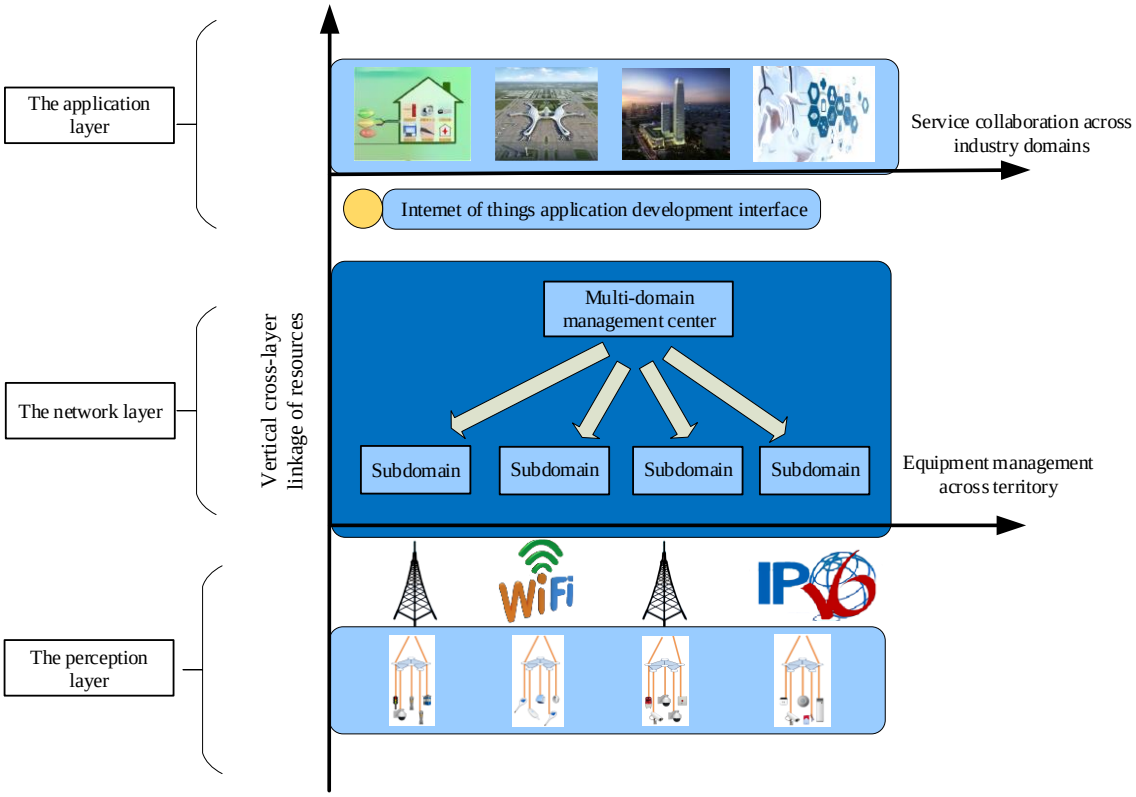

Figure 4: MWoT multi-domain architecture

Equipment cross-regional management: In the Internet of Things, access to a large number of sensing devices is limited by network, bandwidth and storage resources. It is difficult to deploy a single Internet of Things system for access management of all Internet of Things devices. Therefore, Internet of Things service providers divide the whole Internet of Things into sub-domains according to industry or region, and the local devices are managed by sub-domain systems. In MWoT architecture, each sub-domain is connected by multi-domain management center, and the whole perception layer is integrated into a whole. The cross-domain management of perception layer is realized, which provides service support for cross-domain linkage of devices.

Inter-industry and inter-domain collaboration: Multi-domain management center integrates all service interfaces of sub-domain, forms a unified Internet of Things application development interface to provide support services for upper application. All industry applications develop unified interface for network layer according to actual needs and follow unified standards. It shortens the application development cycle and opens up the interactive channel between industry applications. Compatible with other applications in the same industry, it can cooperate with external services and achieve cross-industry collaboration of services.

Longitudinal Cross-Layer Linkage of Resources: Internet of Things resources are heterogeneous. Taking the life cycle of a data as an example, multi-mode heterogeneous devices are generated in the

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

perception layer and transmitted in the complex heterogeneous network at the network layer. They are applied to rich upper applications. They exist in different forms in different periods. This complex The Internet of Things environment makes it difficult for users to monitor and control the whole life cycle of resources. Management, MWoT architecture abstracts each resource of the Internet of Things into a unified model through virtualization technology, carries out unique identification, and realizes the vertical interaction of resources across application layer, network layer and perception layer.

The resources mentioned in MWoT architecture refer to all physical and virtual entities that can uniquely identify hardware, software, applications, data and services in the Internet of Things. The MWoT architecture formulates a perfect method of resource identification, generates a unique identification for all resources in the whole architecture, and provides support for the open sharing of resources. The MWoT architecture stipulates the adoption of all service interfaces. With RESTful style architecture, unified standard operation interfaces for resources are unified. The basic operation of Internet of Things resources is realized through PUT, GET, POST and DELETE methods, and the threshold of Internet of Things resource interaction is lowered. The RESTful style architecture connection is stateless and adapts to the dynamic business environment of Internet of Things. It is suitable for building distributed and scalable Internet of Things in multi-domain scenarios. Service Provision Platform.

3.3. Triple Verification Mechanism of Access Control Framework

The interaction in MWoT architecture is mainly the interaction between the application and the perception layer of the Internet of Things. A resource interaction request is generated in the application layer, transmitted in the network layer, and finally acts on the perception layer. According to the characteristics of each layer of MWoT architecture, a triple verification method is proposed is shown in Figure 5.

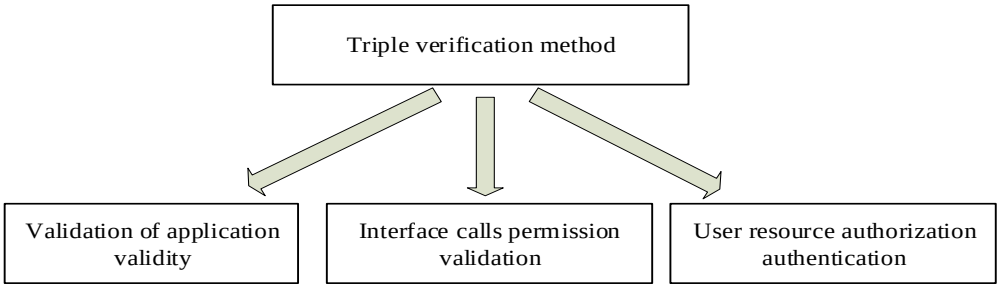

Figure 5: Triple validation method

Validation of application legitimacy: The multi-domain management center validates the legitimacy of the application of perception layer, each application has a unique identity and APP password, and only binds to the developer account registered with the multi-domain management center to ensure the traceability of the application; the multi-domain management center validates the application developer and the application, and allows the application to call OpenAPI after validation to ensure resource interaction. The validity of the request. Interface Call Authority Verification: Because MWoT architecture is designed for multi-domain scenarios, resource interaction requests are ultimately processed by specific sub-domain systems, and the second verification content is mainly set by domain administrators. There are three kinds of resources open authority settings: public, private and semi-public, public state is to make the domain information completely public, and private means that the domain data is totally closed. Deny access in any form; semi-disclosure is the disclosure of specific resources to specific applications. After receiving the resource interaction request, the sub-domain system parses it according to the MWoT architecture standard to determine whether the application has permission to call the access interface and whether the request resource is in the open range. This layer filters the resource interaction request in a coarse-grained way. User Resource Authorization Verification: All resources in the whole MWoT architecture belong to one user. Users have the highest access rights to the resources they own, and can set the open scope of resources freely. The third level of verification is fine-grained permission filtering, which verifies whether the application that makes resource interaction requests has been authorized by users. Users can configure flexibly for each attribute value, command operation and allowable time period of interaction of any device to protect the reasonable and legitimate use of user resources. Take Smart Home as an example: Users can configure any property of any device in their home to allow which applications, which users and at what time, such as not allowing bedroom devices to be accessed by any application at night, controlling

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

access rights to each data of the device from two dimensions of time and space, and protecting users'privacy.

In this paper, a better congestion control protocol is proposed. It has two advantages and takes into account two indicators. It combines the quality of service of data transmission and weighted fairness measurement, and theoretically defines the lower bound. Because different sensors have different nodes, this makes their own value and importance in the document have a weight relationship. Each node i is given a weight w_i. The larger the w_i, the more important the data generated by the node i. And use formula (1) as a measure of fairness.

$$f_t = \frac{\left(\sum_{i=1}^{N} p_{j,t} / w_j\right)^2}{N\left(\sum_{i=1}^{N} p_{i,t} / w_i\right)^2} \tag{1}$$

In this formula, $p_{i,t}$ indicates that the $\sin k$ node receives the number of packets from the node i during the time period [0,t]. When $p_{j,t} / w_j$ is positive and $p_{i,t} / w_i = 0 \ \ (j \in [1,N], j \neq i)$, $f_t = 1/N$, the minimum fairness is reached at this time. When $p_{j,t} / w_j = p_{i,t} / w_i \ \ (j \in [1,N], j \neq i)$ was established, $f_t = 1$ achieved maximum fairness at this time. This paper rigorously proves $f_t \geq 1 - (10c/9)^2$ in theory, where c is a constant and $0 < c \leq 0.2$.

3.4. Triple Verification Mechanism of Access Control Framework

Strictly speaking, public service authorization in multi-domain scenario is not for users, but for applications. Sub-domain administrators have the highest management authority over the resources opened by local users. They can integrate these resources and provide personalized services according to the specific needs of the industries in which the sub-domain belongs. The management authority of these services belongs to the sub-domain rather than to the ordinary users in the sub-domain. For example, the industry of this region is environment detection, and most of the data collected by sensor types are related to air quality. Subdomain can integrate all the data opened by users in this region, extract the required information, and provide air quality inquiry service based on these information. This service does not involve user privacy, and can be completely open, so it only needs. Verify the validity of the upper application and ensure the normal use of the service. The authentication process is shown in Figure 6.

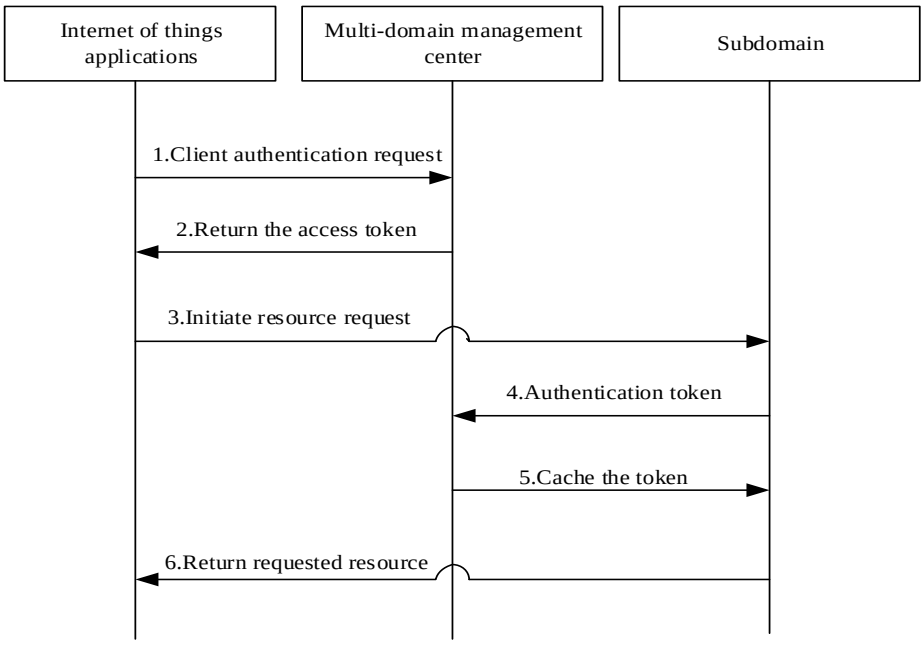

Figure 6: Public service authorization in a multi-domain scenario

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

1) Internet of Things applications initiate identity authentication requests to multi-domain management centers with application unique identity and application password; 2) multi-domain management centers return resource access tokens (Token) after application authentication is successful; 3) applications initiate resource access requests to sub-domains with application unique identity and Token information; 4) sub-domains carry Token to multi-domain management centers to verify legitimacy; 5) Return the validation result; 6) If the validation is successful, return the accessed resources. It is important to note that the fourth and fifth steps only authenticate once in a period of time. After successful authentication, the sub-domain caches the resource access token of the application. Next authentication does not need to be repeated to the multi-domain management center until the token expires, so as to prevent the authentication storm to the multi-domain management center in high concurrency scenarios.

4. Experiments

In order to realize cross-domain sharing of resources, MWoT architecture integrates all sub-domains into a whole. Through identification technology, all resources of the whole Internet of Things architecture are unified modeled, uniquely identified, and the differences of resources in different domains are shielded. It provides basic guarantee for the open sharing of resources. The resources identified by MWoT architecture include sub-domains, gateways, sensors, and so on. Sensor data, sensor commands, applications, services and users are classified according to the above resources, and uniform identification rules are formulated as follows:

Domain identification is represented by 11 bits, which consists of 1 bit identification type and 10 bit domain coding, and 0 bit identification type. Domain coding is composed of national code, administrative code and domain ID, totally 10 bits. Among them, national code adopts national standard code, accounting for 3 bits; administrative code accounts for 6 bits, using postal code identification; domain ID accounts for 1 bit, marking from the beginning, can represent 9 domains; all the above fields are reserved fields, indicating all. As shown in Table 1.

Table 1: Domain coding

Country Code	Administrative Region Code	Domain ID
3	6	1

The gateway identifier is represented by 24 bits, and is composed of an identifier type, a domain code, and a gateway code, and 1 represents the identifier type. Gateway coding consists of gateway use, communication protocol, whether gateway data is public or not, and gateway ID, totally 13 bits. Among them, the gateway uses are divided into smart home, smart city and so on, accounting for 2 places; communication protocols include MQTT, TCP, HTTP, etc., accounting for 2 places; whether the gateway data is public or not, 1 is not public, 2 is public; the gateway code accounts for 5 places can represent 99999999 gateways; all the fields above are reserved fields, indicating all. The details are shown in Table 2.

Table 2: Gateway Coding

Gateway use	Communication mode	Whether the gateway data is public	Gateway ID
2	2	1	8

The perceptual data identification consists of 44 bits, including identification type, domain coding, gateway coding, node coding and data coding. 4 bits represent the identification type, and the data number is composed of data type, node attribute and data ID, totally 14 bits. Among them, the data type occupies 2 bits, including: picture, video, audio, text, numeric data and character data, which are identified by 1-6 and retained by 7-99 respectively; the attribute of node occupies 2 bits, which refers to the data type collected by sensor, including temperature, wind speed, infrared, PM2.5, etc., as shown in Table 3, marked from the beginning; the data ID occupies 10 bits and follows the Unix timestamp. Standard, that is, the time of data generation; all the above fields are reserved fields, indicating all. The details are shown in Table 4.

Table 3: Attribute Coding

Attribute Coding	Identification key	Describe	Company	Symbol
01	tem	temperature	centigrade	℃
02	hum	humidity	percentage	%
03	lux	photosensitive	lux	lux

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

04	vol	voltage	volt	V
05	curr	electric current	ann	A
06	power	power	watt	W
07	infra	infra-red	frequency	F
08	gas	combustible gas	concentration	mol
09	hall	magnetic field	tesla	T
10	press	pressure	newton	N

Table 4: Data coding

Data type	Node attributes	Data ID
2	2	10

This research implements the above-mentioned intrusion detection system, takes the detection data upload module as an example to verify the availability of the system, introduces the rate of false alarm and response. The rate of false alarm is the ratio of the number of unrecognized intrusions to the number of all intrusions. The response rate refers to the ratio of the number of times the system responds to intrusions and the number of detected intrusions. Statistical analysis was carried out in this experiment.

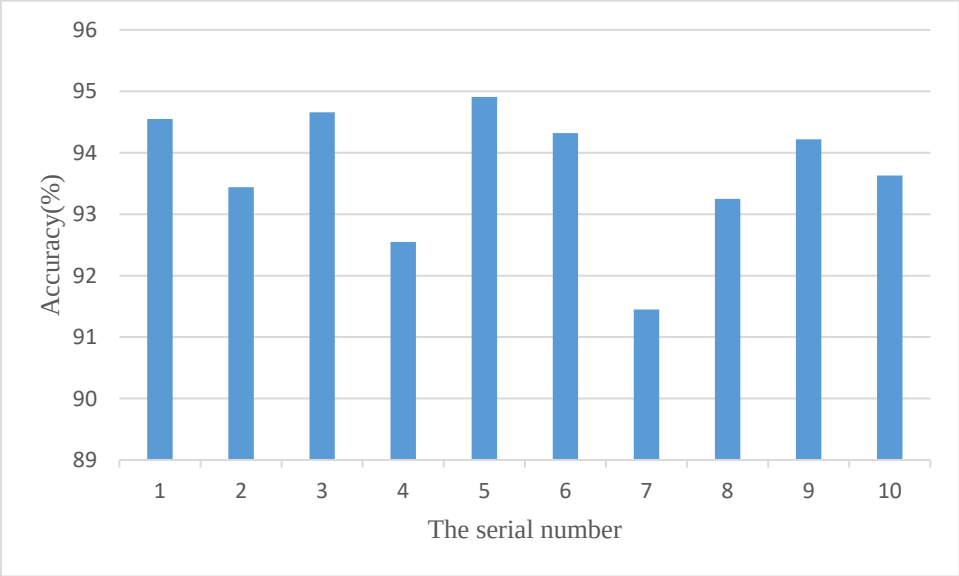

Figure 7: Accuracy of 10 test statistics

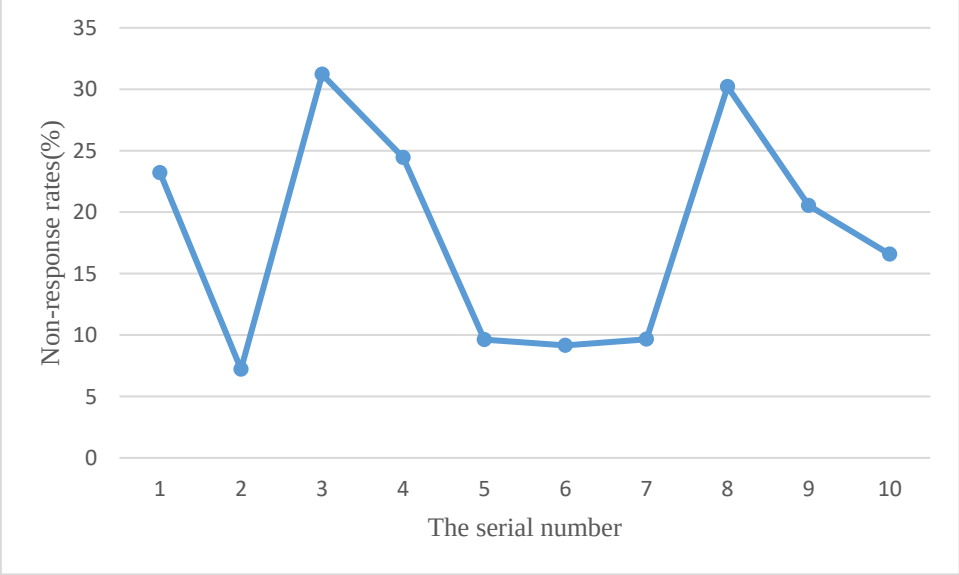

Figure 8: Failure rate of 10 test statistics

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

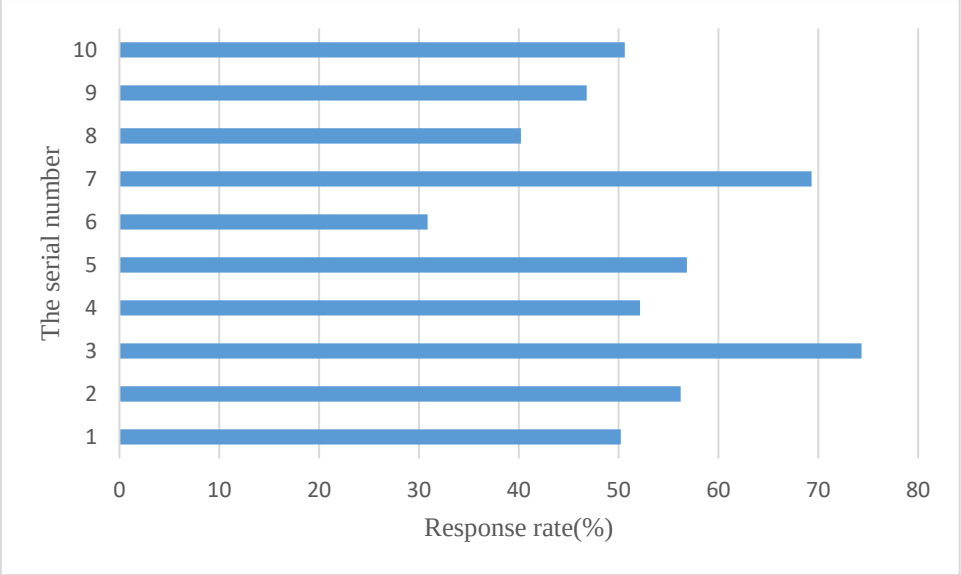

Figure 9: Response rate of 10 test statistics

Analysis of Figures 7 and 8 shows that the results of intrusion detection system judged as intrusive behavior have high reliability, basically can achieve 90% accuracy, and can respond to some intrusive behavior, but there are still about 20% of the intrusive behavior not detected to form a missed report. From Figure 9, we can see that the response rate of each experiment is not very stable, basically between 31% and 74%, and there is still a lot of room to improve the system.

Figure 10 shows the number of data packets in time t, comparing with the amount of ring data and predicted residence. There are many cases where the amount of loop data may be larger than predicted or smaller than the predicted value. However, the inner loop prediction value is larger than the test value here, so the inner loop data will be larger. Therefore, if the data of the inner ring is large, there will be a situation in which the data packet is lost due to the excessive resources occupied, such as a timeout packet. But on the other hand, the gap between them is very small and can be neglected. In this way, the model can be used to solve the problem of uneven distribution of network load.

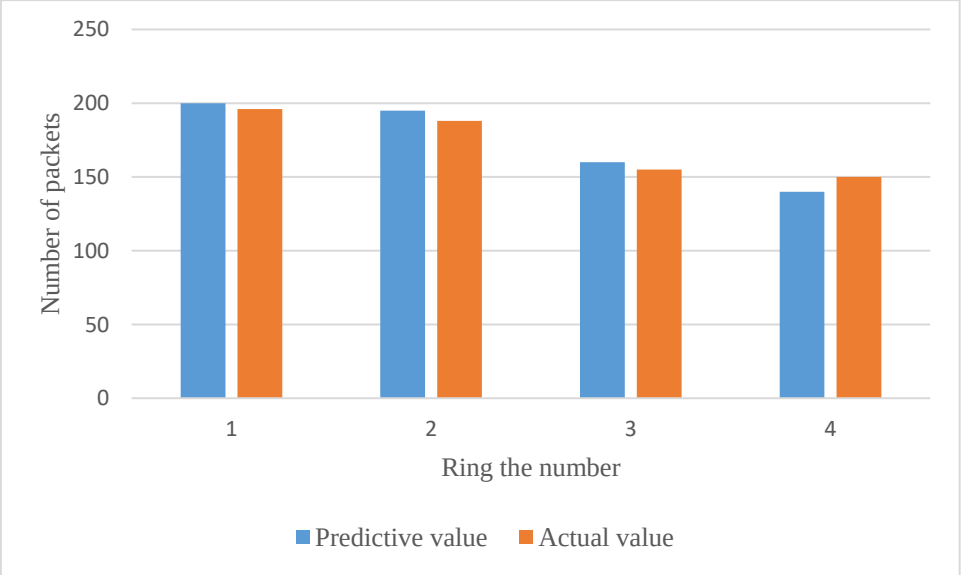

Figure 10. Distribution Chart of Packet Volume in Each Ring

5. Conclusions

With the wide application of the Internet of Things technology, multi-domain, open and security are the basic requirements of the Internet of Things. This paper focuses on the architecture design of the

ISSN 2706-655X Vol.3, Issue 5: 30-42, DOI: 10.25236/IJFET.2021.030504

Internet of Things in multi-domain scenarios to solve the problem of resource fragmentation caused by the closure of the traditional Internet of Things architecture and realize cross-domain sharing of resources of the Internet of Things. Aiming at the problems of closed architecture, tight coupling and poor scalability of traditional Internet of Things, this paper analyses the related technologies such as Internet of Things identification, edge cloud computing and so on. Based on WoT architecture standards, WoT architecture suitable for multi-domain scenarios is proposed to realize cross-domain sharing of resources and cross-domain collaboration of services in the Internet of Things. By analyzing the security challenges faced by MWoT architecture and aiming at the problem of user privacy leakage caused by the openness of MWoT architecture, therefore this paper proposes a MWoT authority management framework, which realizes fine-grained management and control of access rights to resources in various domains through platform, subdomain, user triple authentication and authorization mechanism, and protects user privacy and data security. It is difficult to find and locate intrusions because of its wide distribution. A public service authorization method based on multi-domain scenarios is proposed. It can discover intrusions in real time and make intelligent decisions to improve operation and maintenance efficiency and ensure system security. For different scenarios of the Internet of Things, the accuracy of intrusion detection is over 90%.

References

[1] Razzaque M A, Milojevic-Jevric M, Palade A, et al. (2017)"Middleware for Internet of Things: A Survey[J]". IEEE Internet of Things Journal, 3(1), pp.70-95.

[2] Perera C, Chi H L, Jayawardena S. (2017)"The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey[J]". IEEE Transactions on Emerging Topics in Computing, 3(4) , pp.585-598.

[3] Duchemin W, Anselmetti Y, Patterson M, et al. (2017)"DeCoSTAR: Reconstructing the Ancestral Organization of Genes or Genomes Using Reconciled Phylogenies[J]". Genome Biology & Evolution, 9(5) , pp.1312-1319.

[4] Paganelli F, Turchi S, Giuli D. (2017)"A Web of Things Framework for RESTful Applications and Its Experimentation in a Smart City[J]". IEEE Systems Journal, 10(4) , pp.1412-1423.

[5] Liyanage M, Chang C, Srirama S N. (2018)"Adaptive Mobile Web Server Framework for Mist Computing in The Internet of Things[J]". International Journal of Pervasive Computing and Communications, 14(4) , pp.247-267.

[6] Asadpour M, Dashti M T. (2015)"Scalable, Privacy Preserving Radio‐Frequency Identification Protocol for the Internet of Things[J]". Concurrency & Computation Practice & Experience, 27(8) , pp.1932-1950.

[7] Hu P, Ning H, Qiu T, et al. (2017)"Fog Computing Based Face Identification and Resolution Scheme in Internet of Things[J]". IEEE Transactions on Industrial Informatics, 13(4) , pp.1910-1920.

[8] Tao X, Ota K, Dong M, et al. (2017)"Performance Guaranteed Computation Offloading for Mobile-Edge Cloud Computing[J]". IEEE Wireless Communications Letters, 6(6) , pp.774-777.

[9] Esposito C, Castiglione A, Pop F, et al. (2017)"Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective[J]". IEEE Cloud Computing, 4(2) , pp.13-17.

[10] Cartwright R. (2018)"An Internet of Things Architecture for Cloud-Fit Professional Media Workflow[J]". Smpte Motion Imaging Journal, 127(5) , pp.14-25.