Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2297733, 10 pages
https://doi.org/10.1155/2021/2297733

Research Article

Computer Network Information Security Protection Faced by Digital Art Museums Based on the Internet of Things

Qi Wang[1,2] **Ling Li**[3] **and Shuai Hu**[3]

[1]*Taiyuan R & D Center, Beijing Green Rock Technology Development Co. Ltd., Taiyuan, 030051 Shanxi, China*
[2]*College of Big Data, North University of China, Taiyuan, 030051 Shanxi, China*
[3]*College of Software, North University of China, Taiyuan, 030051 Shanxi, China*

Correspondence should be addressed to Qi Wang; cdma6344@sina.com

Received 5 August 2021; Revised 18 November 2021; Accepted 24 November 2021; Published 15 December 2021

Academic Editor: Zhihan Lv

The development of the Internet of things provides a great opportunity for the development of all walks of life, but it also brings many risks in the process, of which the most important thing is the protection of computer network information security. Digital art museums play a great role in viewing, education, and other functions. This article is aimed at analyzing the computer network information security protection problems faced by digital art museums. Analyze the application of the digital art gallery in the computer Internet of things, and combine the different aspects involved in the two parts to carry out experimental analysis and comparison. The difference between the various subjects of the digital art gallery, such as exhibits, writers, and visitors, is to maintain the security of Internet computer information. Introduce the application. The results show that compared with that of fog computing technology and that of edge computing technology, the performance of the Internet of things is generally better, with faster data processing speed, shorter processing time, higher quality, and stronger scalability. But at the same time, it is also facing greater computer network security threats. According to statistics, 83.3% of consumers worry about its usability but people are more concerned about its safety performance. Nearly 87.5% of consumers worry about whether their information will be leaked. When cloud computing technology is applied to digital art museums, how to protect computer network information security is particularly important. Based on the traditional firewall, this paper designs a hybrid firewall, which can better solve the problem of computer network information security.

1. Introduction

A museum is a public exhibition platform for studying the development of human civilization and inheriting history and culture. It gathers the development information of history, arts and crafts, fine arts, and so on of each dynasty. However, with the popularization of Internet technology and the rapid development of information technology, the traditional museum has been unable to meet people's demand for information. Therefore, digital art museums emerge as the times require. In this environment, people can understand information and obtain information resources more quickly and efficiently without the limitation of time and space. Therefore, A digital art museum is the development and extension of physical museum resources. However, while the computer network technology brings us convenience, we are also facing the following threats and challenges. Once the computer network software, data, and system data are damaged, it will bring a serious blow to the digital art museum.

According to the survey, computer network information security is causing a heated discussion. Even with the continuous improvement of network technology, many users still feel "insecure." These security issues involve the safety of system information, information dissemination, safety of the consequences of information dissemination, and information content security on the network where the system is not damaged, modified, or leaked due to accidental or malicious reasons, and the system operates continuously, reliably, and normally. Involving the confidentiality, integrity, availability, authenticity, and controllability of information on the network, they continue to pay attention to this

problem and hope that information can be truly protected. In order to make the digital art museum develop healthily and sustainably, we must pay attention to its potential network information security and put forward solutions and strategies.

With its convenience and economy, data sharing has become an attractive service provided by the Internet of things platform. Jiang et al. solves this challenging problem by proposing a new attribute-based data sharing solution for mobile users with limited resources in the Internet of things. However, in terms of data owners, the problem of fine-grained, efficient, and standard data confidentiality shared by the Internet of things has not been resolved [1]. Due to the diversity of IoT providers, it is a very important challenge for organizations to choose the right IoT services to meet their needs. Abdel-Basset et al. introduced how to provide a multicriteria decision analysis (nmcda) method to evaluate the quality of IoT services, thereby helping decision makers evaluate different IoT services. However, his article is not comprehensive enough and there are still some problems to be solved [2].

The innovations of this paper are as follows: (1) combining theoretical analysis and empirical research, fully apply the Internet of things technology to the research of digital art museums. This article not only theoretically but also through a large number of practical investigations discusses the computer network information security problems faced by digital art museums under the Internet of things environment from the practical level and gives some solutions to play a role of theoretical guidance and practice [3]. (2) The design and development of a hybrid firewall can not only prevent cyberattacks but also quickly respond to new cyber threats. (3) Combining the specific design plan of the digital art museum, based on practical experience, summarizes and analyzes the computers faced by the digital art museum in the Internet of things environment, an effective way of network information security protection. The network BP algorithm is used to analyze and organize the data of the Internet of things model construction and various aspects of the related content, which is a meticulous end-to-end secure structure network. Analyze the security protection cost of computer network security protection and the nature of information security hazards.

2. Research Methods of Computer Network Security Protection in Digital Art Museum

2.1. Internet of Things Technology. The Internet of things (IoT) [4, 5] technology, that is, the Internet of everything, is developing rapidly, and it has brought unprecedented convenience to life and industry. As an extension of the Internet technology, the Internet of things technology extends the "Internet" from traditional computer networks to various terminal devices that can be seen everywhere, whether it is a computer, handheld device, living industrial facility, or tiny sensor, as long as it can be communicated through some kind of communication method. Basic information exchange with the outside world can be connected to the "Internet of things" recess. The structure of the Internet of things environment mainly includes the perception layer, the network layer, and the application layer, which are responsible for the collection, transmission, processing, and transformation of information into services; as far as digital art museums are concerned, relevant information about a work, such as the author, the work itself, and development information, is entered into a specific Internet information platform and the computer automatically processes and categorizes this information to generate online and offline services. The increasingly open features of the Internet are more reflected in the integration of resources across the entire network. When providing users with public resources, information disclosure, and diversified and personalized services, operators or openers can collect or integrate the required resource services or conduct secondary development through openness.

The convenience service provided by the Internet of things environment to modern society stems from his perception: so, the sensor network technology is an indispensable and even very important part of the entire Internet of things environment. With the development of information and communication technology, sensors and related components have become increasingly robust and inexpensive. The application of sensor networks in life and industrial production has also become more extensive and in depth from the fields of monitoring, tracking, and control. People use sensor networks in a wide range, a large number, and diversity. In the field of sensor networks, the wireless sensor network (WSN) [6] is the most widely used. It is well known that the wireless sensor network is a distributed sensor network and its end is a sensor that can perceive and inspect the external world. The sensors in the WSN communicate wirelessly, so the network settings are flexible, the location of the device can be changed at any time, and it can also be connected to the Internet in wired or wireless mode. Based on its wireless characteristics, its application scenarios are more flexible and network attributes are more complex. The role of the sensor network gateway is also more important. The sensor network here is a generalized sensor network. It is no longer just a conventional sensor network based on a certain protocol, but a network of perception monitoring systems in the perception layer of the Internet of things.

The overall architecture of the IoT environment mainly includes a perception layer, a network layer, and an application layer, as shown in Figure 1. The perception layer [7, 8], the so-called basic network connected by everything, is mainly responsible for the collection of information, including traditional sensor networks and various monitoring systems; in a broad sense, it belongs to the category of sensor networks; the network layer is responsible for the information obtained by the perception layer, reliable transmission, network management, and simple information processing. It is precisely because the structure of wireless sensor networks has great advantages, which also promotes the diversification of its communication media and means. The transmission medium is no longer just a traditional computer network. It may be a mobile phone network, a radio and television network, or a dedicated line or a local area

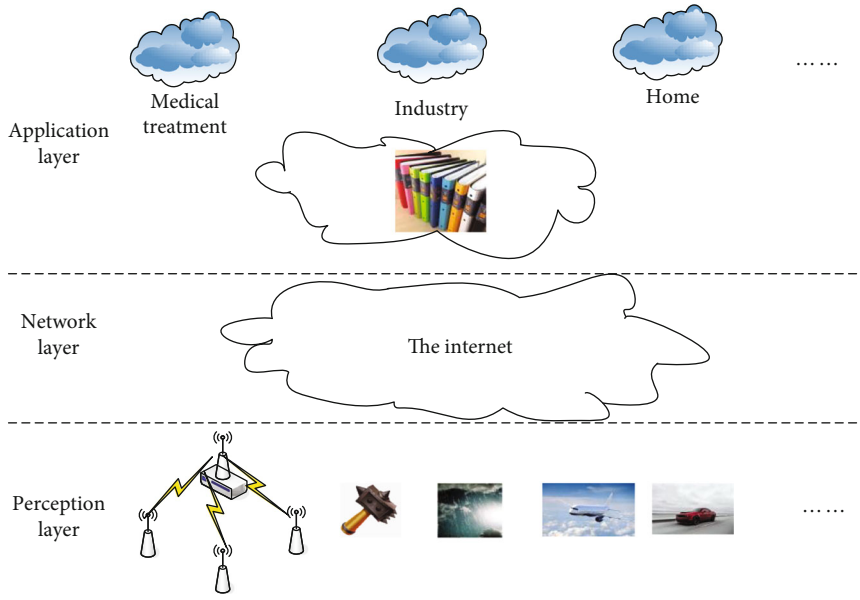

Figure 1: IoT architecture.

network. As long as a unified abstract description of the network that can be used to transmit perception information, the gateway involved is part of the network layer, which is located on the network layer to realize network interconnection and is a complex network interconnection device; the application layer is responsible for the perception of the information. All kinds of intelligent processing are carried out, and information is transformed into data to realize a wide range of intelligence, which is mainly carried out on the cloud platform.

2.2. Characteristics of Information Security in the Internet of Things Environment. The key to solving information security issues is how to implement regulations. From a substantive point of view, the substantive regulation of information security in the Internet of things environment is the application of substantive laws in the field of information security. Therefore, it must follow the general provisions of the law, such as the protection of personal rights, the regulation of public power, the general provisions of the law on infringements, intellectual property rights, property rights, and criminal constitution and punishment. However, information security issues in the Internet of things environment are different from general legal issues after all. According to its own characteristics, corresponding countermeasures need to be taken according to these new characteristics. The end-to-end security structure of the Internet of things is shown in Figure 2.

2.2.1. The Overall and Extensive Nature of the Impact of Information Security. In the Internet age, human-computer dialogue information is input into computers by humans and then processed by computers. Through the intermediary of computers and networks, a great amplification effect is produced. Information security has become a major issue that affects the country, social development, and personal privacy. However, due to the limitation of the influence of the fact that information collection cannot be separated from people, the collection and dissemination of information are subject to certain technical limitations and its scope of influence also has certain limitations. When the collection of information is restricted, it will have a great impact on the information construction of the digital art museum and will also have a certain impact on the information of related works and the data will have errors to some extent. In the context of the Internet of things, the depth and breadth of information are unmatched by the Internet. Through radio frequency identification technology and sensing technology, the Internet of things has surpassed the human-machine dialogue in the Internet era and realized the trinity of human-machine-things. The collection and utilization of information have less dependence on people, and things are information that can be exchanged directly between people and things, which greatly expands the collection of information.

"It is possible to fully and accurately obtain the physical world environment, behavioral state (such as location and stay time), physiological state, etc. of personal life." The amount of information is increasing rapidly, and people's understanding of information is more in depth and convenient. People's lives have a benign impact, but on the other hand, information security is also facing greater pressure. More and more information from the country, society, and individuals is inadvertently collected and disseminated through the Internet, making information confidentiality. Integrity and authenticity are more susceptible to interference from external forces, and information security involves far greater areas than before. Ensure the integrity of the information because although others cannot understand it; it can destroy your information, such as deleting part of the information, so that the legal recipient cannot get the correct information, and the integrity mechanism ensures

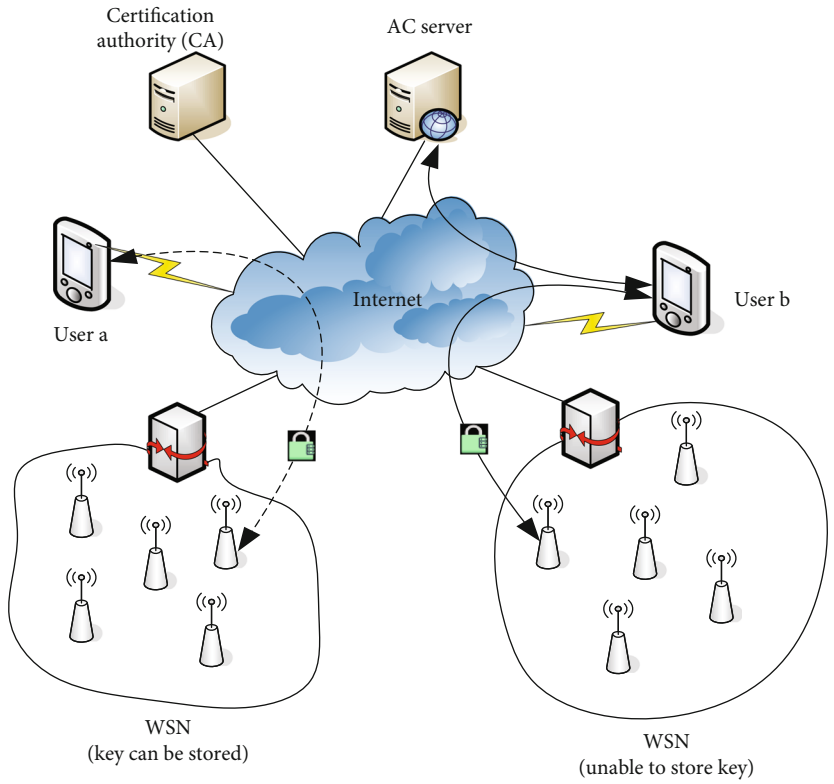

Figure 2: End-to-end security structure diagram.

that the integrity of the information is not destructive and can safely let the recipient get all the data. In addition, because the application of the Internet of things is industry oriented, global, or even cross industry, its ultimate vision is to form a global system, which may affect the entire industry in the world or a region and even the normal operation of several industries, while involving the privacy of the public. Therefore, under the environment of the Internet of things, the impact of information security is unprecedented and it is obviously global and extensive. The overall and extensive nature of the impact of information security determines that information security issues not only affect private interests but also have a wide range of publicity. From a legal perspective, legal regulation of this requires not only personal autonomous private law but also protection of the public law norms of interests.

2.2.2. Vulnerability of Information Security. Due to the technical aspects of the Internet of things, information security is more susceptible to infringements in the Internet of things environment. First of all, because the Internet of things uses radio frequency identification technology, sensor technology, etc. to perceive and process information and the sensing nodes of the Internet of things have simple functions, low processing capabilities, and low energy, they cannot independently realize complete security protection and the number of nodes. The large size is difficult to manage and control, and it is easy to have omissions. It gives attackers an opportunity. This makes the communication information of the node easily eavesdropped or even controlled, resulting in network information leakage; it also allows the attacker to obtain identity and password information through the node. Tamper with software and hardware, and then, capture nodes, pretend to be legitimate users, and conduct attacks such as monitoring user information and publishing false information. Secondly, at the network level, the Internet of things has common security threats on the one hand, including illegal access to the network and eavesdropping on information, virus intrusion, and man-in-the-middle attack. On the other hand, the Internet of things may have information security issues such as heterogeneous network layers and huge network clusters. Thirdly, from the processing level of the Internet of things, the amount of data in the Internet of things is large and needs to be used. In cloud computing technology, if the cloud computing system data protection mechanism is not perfect, it may cause data theft. Finally, from the application level, if the authentication mechanism is not perfect and the access permission setting is not perfect, it may not be able to isolate the intrusion of illegal users, resulting in user information security and personal privacy being violated. To this end, relevant agencies should strengthen the establishment of relevant mechanisms, especially strictly control the security authentication mechanism, supervise the entire process such as access permissions and access records, and strictly control the screening and supervision of users. From a social perspective, information security is also easy to be violated in the Internet of things environment. In the Internet age, information security is an important topic, which must involve the location of each industry's associated area. From the current experience, the

main reason why information security is violated in the Internet era is that the information behind it, the black industry chain driven by commercial interests. In the era of the Internet of things, the Internet of things will be applied more deeply in various industries, as well as national defense, military, and other national core interests. The information disseminated by the Internet of things contains higher commercial and political values. The attacker has a stronger incentive to steal information. In addition to technical improvements, the vulnerability of information security requires an appropriate expansion of the legal scope and density of regulations from a legal perspective, such as increasing the preventive obligations of participants in the Internet of things [5].

2.2.3. The Immediacy and Uncertainty of Information Security Hazards. In the Internet age, the dissemination of information has achieved immediacy, that is, the dissemination of information can reach the audience immediately from the source of the dissemination, but this information still needs a process from being received to being maliciously used to cause real social harm. It can be long or short, but after all, there is room for remedy. In the era of the Internet of things, attackers can directly manipulate things through human-machine-things dialogue and people can directly control things remotely and infringe on things. The harm caused by malicious use of information is instantaneous, giving information security. The time and opportunity for the aggrieved party to remedy are relatively very small. From the perspective of risk science, the immediacy of information security hazards, under the influence of psychological diffusion, can easily give the society the illusion of infinite risks and cause social panic. In addition, there is still considerable uncertainty about the hazards of information security in the Internet of things environment. Due to the huge amount of data, the current information management by the existing network mechanism cannot truly measure and clean up in some cases. Specifically, the huge number of nodes and huge amount of data in the Internet of things give information security attackers a great opportunity to invade the network. The aggressor has an absolute dominant position, and once it invades the Internet of things, it can often effectively realize its own intentions, while the victim is in a completely passive state, and it often does not know who committed the infringement and for what purpose, what purpose is achieved, when it will come, and what opportunity is there to remedy. It is the immediacy and uncertainty of this kind of hazard that make it extremely difficult for information security governance entities to manage and prevent it. The eyes of legal norms are simply lingering on the hazard results, and it is difficult to rely solely on traditional consequential legal logic [9, 10]. To solve the problem, the attention of the law must be moved forward.

2.2.4. The High Cost of Information Security Assurance. In the Internet environment, the protection of information security has shown the characteristics of high cost. Many acts that endanger personal privacy, trade secrets, and even national information security cannot be dealt with due to technical reasons, which indirectly contributes to the infringement of information. Security behaviors have caused a large number of information security infringements and criminal acts. In the environment of the Internet of things, due to the technical characteristics of the Internet of things itself, information security is a big problem that hinders the development of the Internet of things. Security issues will be faced in every link of information from perception to transmission to application. If the main focus of the solution is on postevent relief, the cost of guaranteeing information security will be very high, which is not conducive to the sustainable development of the Internet of things and is an inefficient solution. In addition, in the Internet of things environment, the most important thing is the ambiguity of the identity of the information security infringement subject and the high difficulty of determining the causal relationship between the infringement and the result of the infringement, which makes the investigation of the responsibility for the information security infringing costly. Because in the Internet of things, although there is an identity authentication mechanism and a password management mechanism, the technology can never be absolutely complete, it may always be broken and unauthorized manipulation may cause information security to be compromised. But who is implementing it? Unauthorized operation is in a state of vagueness. The costs of litigation and the benefits of litigation are obviously asymmetrical; the mechanisms of administrative law enforcement and criminal law enforcement are also difficult to investigate and collecting evidence is difficult as well, and the causal relationship between the infringement and the result of the infringement is difficult to identify in the traditional way. As a result, the cost of law enforcement is too high. All in all, it is very costly to solve information security problems in the Internet of things environment in accordance with the current legal framework and legal means. Because of this, it is necessary to design laws governing information security in the Internet of things environment based on the cost-benefit principle to ensure that the basic rights of citizens can be maintained and the cost of law application can be reduced.

2.3. Methods of Computer Network Security Protection. The network itself has a complete network security system, and the controlled functions include list connection restrictions, maximum list permissions, administrator permissions, and file functions [11]. All these functions can improve data security. In order to prevent or limit network viruses, this article proposes the following countermeasures:

(1) Diskless workstations need to have a system server in the network; the server contains the required operating system and additional workstations to run the operating system. The essence of a diskless workstation is to separate the hard disk from the host and only perform operations without storage. Adopt a diskless workstation. Workstations without disks can only read but cannot write to users. In this way, the possibility of virus implantation is greatly reduced [12]. But if there is only one diskless server,

if this server encounters a problem and fails, it will result in the entire disk being paralyzed. To find a way to solve this problem, one more server is used as a diversion. When one is broken, the division is diverted, just on top. Only in this way can the operating speed of the diskless workstations in the diskless network be guaranteed, and it will play a role in the diversion

(2) Restrict user access rights. It is best not to use a super user to log in to the system. Ordinary users are only allowed to access their own lists and files, and usually, multiple users are not allowed to access the same lists or files to prevent cross contamination of network viruses [13]. If necessary, users can be notified not to upload executable files to the group list and the group list can only store data resources

(3) Strengthen system management. The files in the shared list are generally set as read only, so that they will not be arbitrarily deleted or modified [14]. Because the system program list does not have editing permissions, the virus will not pollute system files nor will it spread to other users

(4) Strengthen workstation management. The workstation is the entrance of the network. If antivirus materials and chips are installed on the workstation, the required path for screening and filtering can be strengthened to achieve the effect of intercepting viruses in advance [15, 16]

2.4. Solutions of Digital Art Museum. Digital virtual display adopts virtual reality cultural relics, the construction of digital multimedia, and network technology to implement the communication and convenient virtual display. On the basis of the existing exhibition mode of the museum [17], the expansion of the digital heritage information and interactive experience of the museum is increased and the exhibition of the museum is felt close to let us easily acquire exhibition and historical knowledge; this is an important concept of digital museum research. The virtual display system mainly includes streaming media and interactive 3D video technology [18]. The combined application of the interactivity and immersion of virtual technology is an image of a digital art gallery simulated with the help of Internet technology. The image contains many sections according to the different divisions of works inside the museum, virtual space reconstruction, interactive virtual studio, and multimedia guide. A digital art museum is a combination of humanities and science and technology in the era of product information. The new appreciation, which was born after it, is rooted in the soil of traditional and modern technology museums and is a new form of museum under the new network environment, so it is different from the concept pursuit and practice of traditional museums. Therefore, in the implementation of digital art museums, the paper puts forward the following suggestions to promote the construction of a digital museum [19, 20].

First, the plan of digital art museum is drawn up and the practical solution is implemented in combination with the overall development plan of the actual digital museum.

Second is data collection: according to the order of cultural relics, the understanding of a digital museum is sorted out one by one and the theory is full of and rich in potential connotation of works and the existing value and necessity in the design are discussed and solid basic work is insisted [21].

Third is the way of display and display: from the digital display mode, the museum exhibits can be viewed 360 degrees in the web design.

2.5. Comprehensive Evaluation Method of Computer Network Information Security. In order to better and more directly evaluate the computer network information security situation, this paper uses some methods, for example, set a indicators to comprehensively evaluate m things:

$$X' = \left(x'_{ij}\right)_{m\times a}, \quad i = 1, 2, \cdots, m\,; j = 1, 2, \cdots, a. \tag{1}$$

The comprehensive evaluation of distance needs the following steps:

(1) Index codirection

If there is an inverse index or an appropriate index in a indicators, it will be transformed into a positive index and the data matrix after transformation will be recorded as

$$X = \left(x_{ij}\right)_{m\times a}, \quad i = 1, 2, \cdots, m\,; j = 1, 2, \cdots, a. \tag{2}$$

(2) Dimensionless

Choose an appropriate method to make the data dimensionless, and the data matrix after transformation is denoted as

$$Y' = \left(y'_{ij}\right)_{m\times a}, \quad i = 1, 2, \cdots, m\,; j = 1, 2, \cdots, a. \tag{3}$$

First, clarify the value of a certain cultural relic, including all aspects of physical attributes. Through the combination of itself and various utilization values, the optimal arrangement is realized.

(3) Determine the reference sample (virtual sample)

Usually, the best sample y^+ and the worst sample y^- are used as reference samples. Because the indicator is positive, the maximum value of each indicator in all samples can be used to form the best sample; the minimum value of each indicator can be used to form the worst sample, denoted

by Y^+ and Y^- as follows:

$$Y^+ = (y_1^+, y_2^+, \cdots, y_a^+)^T,$$
$$Y^- = (y_1^-, y_2^-, \cdots, y_a^-)^T. \quad (4)$$

(4) Calculate the distance

The relevant literature adopts the following forms:

(a) D_i^+ means distance from the sample point to the optimal sample point:

$$D_i^+ = \sqrt{\sum_{j=1}^{a} \left(y_m - y_j^+\right)^2} \quad (5)$$

(b) Based on equation (5), D_i^- means distance from the sample point to the optimal sample point:

$$D_i^- = \sqrt{\sum_{j=1}^{a} \left(y_m - y_j^-\right)^2} \quad (6)$$

3. Research Experiment on Computer Network Information Security Based on the Internet of Things

The digital art museum is a system that provides online services for the protection and display of human cultural and natural heritage. It processes and processes information resources through digital technology, thus playing a role in spreading civilization. However, due to the diversity of connections, the uneven distribution of terminals, and the open sharing of computer networks, the Internet of things is vulnerable to attacks by external hackers, malicious software, and other means. Therefore, the security and confidentiality of network information are very important issues and it is urgent to resolve these threats.

Therefore, we need strong enough security measures to protect network security and improve firewall technology based on various devices and technologies of the Internet of things to solve network security problems.

3.1. Design and Implementation of a Hybrid Firewall System Based on the Internet of Things. A "firewall" refers to the system that uses control strategy between two networks, and it is also a network monitoring system to ensure the security of a computer network. As a kind of control technology with the function of separation, restriction, and analysis, a firewall is usually a combination of the software system and hardware equipment, which is used to establish a security barrier between internal and external networks. The general structure is shown in Figure 3.

However, there are several serious problems in traditional firewalls: (1) unregistered network attacks cannot be stopped and resolved, and the network connection performance is relatively poor. (2) It is impossible to share resources with each other, nor can it realize automatic adjustment functions. (3) There are fewer countermeasures against attacks, and the operating efficiency of the network is relatively low.

Aiming at these problems of traditional firewall, this paper designs a hybrid firewall system, which can solve some problems and improve the scope and efficiency of protection.

3.2. The Composition of a Hybrid Firewall Architecture Based on the Internet of Things. The hybrid firewall adopts a combined structure, which is mainly composed of an internal firewall, external firewall, fortress host, and base station host server, as shown in Figure 4.

3.3. Main Composition and Function Description of a Hybrid Firewall Based on the Internet of Things. The internal and external firewalls can perform different filtering levels. The shielded subnet can only access the authenticated Internet host and internal subnet and access the base station host. All other traffics to bypass will be blocked, so that the security factor can be constantly strengthened.

4. Analysis and Comparison of the Situation Faced by Digital Art Museums in the Cloud Computing Environment

4.1. Research Background of Digital Art Museums. With the development of museums and the advancement of science and technology, as well as the spiritual pursuit and aesthetic awareness of the audience, there are more and more museums in China with rich types and diverse subjects. At the same time, the total number of museums in China has jumped to the top five in the world, namely, the United States, Germany, Japan, China, and Russia. The following is the number of museums and the flow of people from 2014 to 2019, as shown in Table 1.

However, due to the impact of COVID-19, museums across the country were closed in 2020 in accordance with the requirements for epidemic prevention and control. During this period, the museum system has launched digital art museums. Actually, digital art museums move physical museums online through technical means. The emergence of the Internet is a kind of convenience for people. It can observe and experience the breath of history in restaurants and museums anytime, anywhere. When the digital art museums went online, they were warmly welcomed by everyone.

4.2. Research and Analysis of Computer Network Information Security Protection in the Cloud Computing Environment. In order to better understand cloud computing and its advantages, this paper makes the following comparative analysis with fog computing and edge computing, as shown in Table 2.

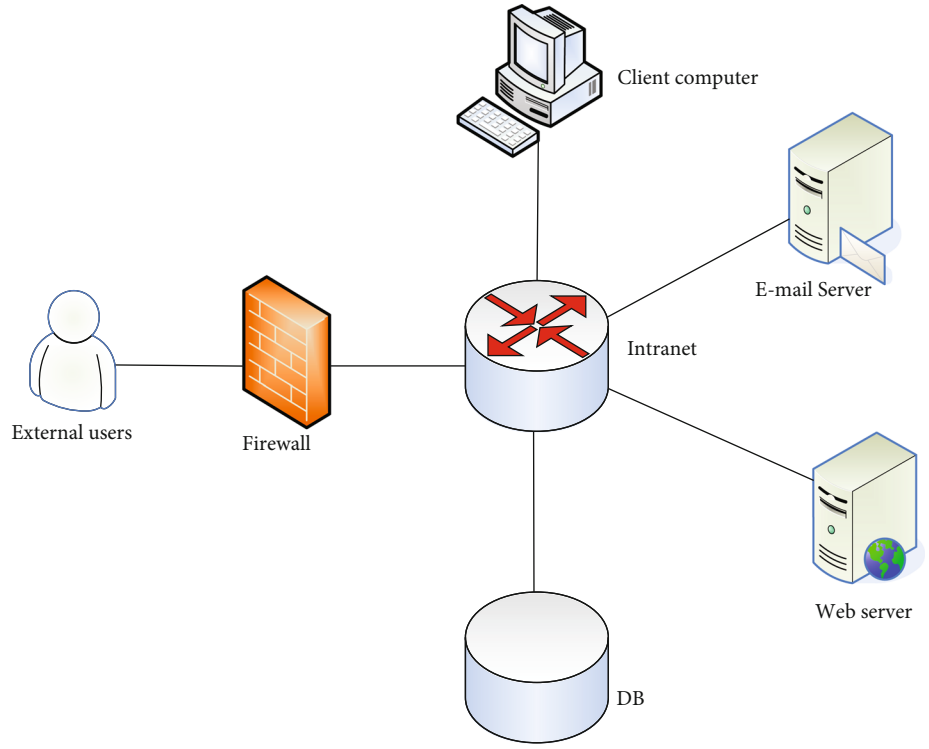

Figure 3: General structure diagram of the firewall.

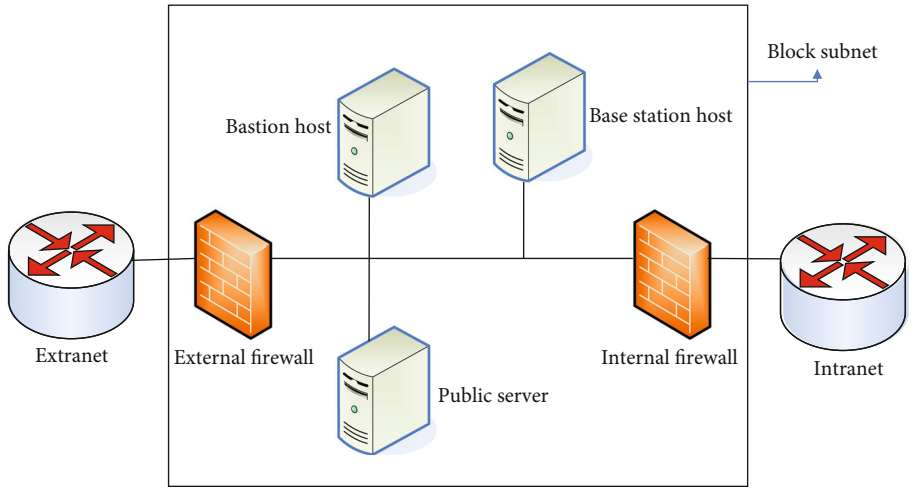

Figure 4: Structure of the hybrid firewall system.

Table 1: Museum status.

	2014	2015	2016	2017	2018	2019
Number of museums	4510	4692	4873	5136	5354	5535
Human traffic	71800	78100	85100	97200	112600	122700

In cloud computing services (CCS), consumers are more concerned about moving their more private data and applications from their own private computing environment to an online cloud environment, which is shared by different users and can usually be accessed through public networks. A survey conducted by the International Data Corporation

Table 2: Performances.

	Data processing speed	Processing time	Service quality	Extended performance
Cloud computing	High	Short	High	Strong
Fog computing	Medium	Long	Good	Medium
Edge computing	Average	Medium	Average	Average

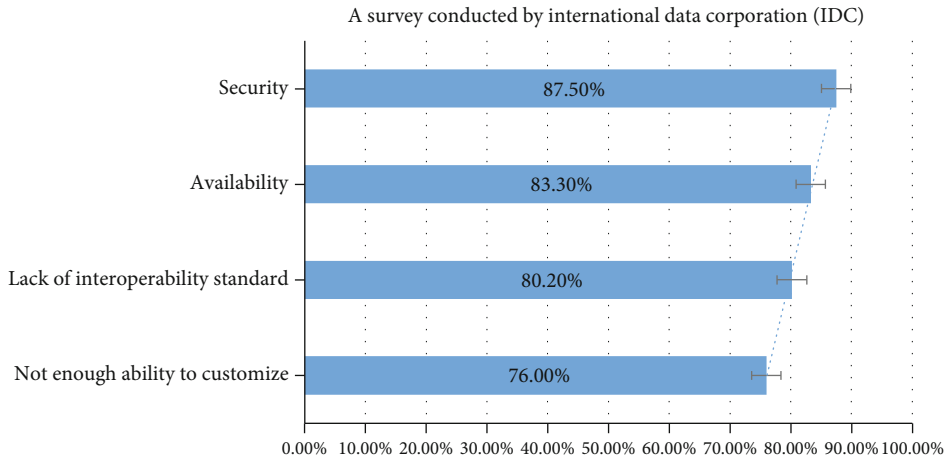

Figure 5: Issues ranked by cloud computing costumers.

(IDC) in September 2020 revealed some issues related to cloud computing clients, as shown in Figure 5. Security has become the most concerned issue.

5. Conclusions

This article starts with definitions and questions and roughly proposes the concepts of cloud computing and digital art museums and analyzes their characteristics. From the perspective of the combination of the two, it discovers the computer network information security problems faced. In order to better solve these problems and make users no longer worry about the security of cloud computing technology, this paper designs a hybrid firewall. This kind of firewall can greatly enhance network security and countermeasures and upgrade and improve information security technology. However, due to the limitations of my professional knowledge and the need for more time and experimentation to protect computer network information security, there are still many areas for improvement in this design. We need to continue to research and explore not only for the healthy operation of digital art museums in the cloud computing environment but also for the development of our country's computer network information security.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] D. Jiang, L. Shi, P. Zhang, and X. Ge, "QoS constraints-based energy-efficient model in cloud computing networks for multimedia clinical issues," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14307–14328, 2016.

[2] M. Abdel-Basset, M. Mohamed, and V. Chang, "NMCDA: a framework for evaluating cloud computing services," *Future Generation Computer Systems-The International Journal of Escience*, vol. 86, pp. 12–29, 2018.

[3] S. Li, L. D. Xu, and S. Zhao, "The Internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[5] A. al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[6] S. M. Sensor, "Mania! Sensor mania! The Internet of things, wearable computing, objective metrics, and the quantified self 2.0," *Networks*, vol. 1, no. 3, pp. 217–253, 2012.

[7] B. Wang, "Review on Internet of things," *Journal of Electronic Measurement & Instrument*, vol. 23, no. 12, pp. 1–7, 2009.

[8] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[9] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[10] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer Law & Security Review the*

International Journal of Technology & Practice, vol. 26, no. 1, pp. 23–30, 2010.

[11] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the SOA-based Internet of things: discovery, query, selection, and on-demand provisioning of web services," *IEEE Transactions on Services Computing*, vol. 3, no. 3, pp. 223–235, 2010.

[12] M. M. Dhanvijay and S. C. Patil, "Internet of things: a survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, pp. 113–131, 2019.

[13] Y. Wang, "Food information management and security strategy of computer network," *Advance Journal of Food Science & Technology*, vol. 11, no. 12, pp. 792–794, 2016.

[14] X. Z. Wang and Q. Li, "E-commerce supply chain security and influencing factors of logistics industry development based on VAR model," *International Journal of Security and its Applications*, vol. 10, no. 9, pp. 129–140, 2016.

[15] K. Shi, "Research on the network information security evaluation model and algorithm based on grey relational clustering analysis," *Revista de la Facultad de Ingenieria*, vol. 14, no. 1, pp. 69–73, 2017.

[16] D. Dang-Pham, S. Pittayachawan, and V. Bruno, "Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace," *Information & Management*, vol. 54, no. 5, pp. 625–637, 2017.

[17] K. Herland, H. Hämmäinen, and P. Kekolahti, "Information security risk assessment of smartphones using Bayesian networks," *Journal of Cyber Security & Mobility*, vol. 4, no. 2, pp. 65–86, 2016.

[18] Y. W. Abdalaziz and A. Hamarsheh, "Analyzing the IPv6 deployment process in Palestine," *International Journal of Computer Network and Information Security*, vol. 12, no. 5, pp. 31–45, 2020.

[19] M. M. Hassan, "Centralized relay selection and optical filtering based system design for reliable free space optical communication over atmospheric turbulence," *International Journal of Computer Network and Information Security*, vol. 12, no. 1, pp. 27–42, 2020.

[20] O. Barabash, A. Musienko, S. Hohoniants et al., "Comprehensive methods of evaluation of efficiency of distance learning system functioning," *International Journal of Computer Network and Information Security*, vol. 13, no. 1, pp. 16–28, 2021.

[21] A. F. Rasheed and A. E. Abdelkareem, "Performance evaluation of MAC protocols with multi-sink for mobile UWSNs," *International Journal of Computer Network and Information Security*, vol. 11, no. 7, pp. 1–7, 2019.