Received February 17, 2021, accepted March 2, 2021, date of publication March 8, 2021, date of current version March 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064350

Information Security Monitoring and Management Method Based on Big Data in the Internet of Things Environment

WUCHAO LIANG[1], WENNING LI[2], AND LILI FENG[2]

[1]School of Management Engineering and Business, Hebei University of Engineering, Handan 056038, China
[2]School of Management, Hebei GEO University, Shijiazhuang 050031, China

Corresponding author: Wenning Li (liwenning20201112@163.com)

This work was supported in part by the Hebei Province Department of Education Young Top Talent Project (Research on the Development of Handan Cultural Tourism Industry Based on RMP Analysis) under Grant BJ2019076, in part by the Social Science Fund Project of Hebei Province (Study on Marketing Strategy of Cultural Tourism Industry Based on Idioms and Allusions in Handan) under Grant HB18GL029, in part by the National Social Science Foundation of China (Study on the Coupling Mechanism and Regional Heterogeneity Between Environmental Regulation and Environmental Responsibility Fulfillment of Enterprises) under Grant 18BGL185, and in part by the Hebei Province Universities Hundred Outstanding Innovative Talents Support Program under Grant SLRC2019003.

ABSTRACT As an important part of the new generation of information technology, the Internet of Things (IoT), with its ubiquitous connection and service characteristics, has penetrated into various fields of application and played an important role. In this paper, based on the study of the basic technology of the environmental Internet of Things, combined with the service-oriented technology architecture SOA, J2EE, multi-level system architecture MVC, real-time database and other technologies and project practice experience, summarized and proposed a kind of environmental quality monitoring integrated management platform design and implementation feasibility scheme. Firstly, the background of the era of big data is described in detail, the urgency and necessity of information security monitoring under the background of big data is clarified, and the three elements of information security monitoring mechanism, namely network monitoring personnel, environment and technology, are proposed, and the three elements as the starting point to establish the information security monitoring mechanism; Starting from the relevant monitoring strategies and safety monitoring technologies, this paper explains the basic principles of constructing the evaluation index system, and establishes the evaluation index system according to the key influencing factors of enterprise information security level in the environment of big data. AHP fuzzy comprehensive evaluation method is chosen on the basis of analyzing various comprehensive evaluation methods, and the weight of each evaluation index is determined and the comprehensive evaluation model is constructed. The establishment of information security monitoring and evaluation system, the use of information security monitoring and evaluation system, for information security monitoring work to provide reference standards. Finally, on the basis of the foregoing, relevant strategies for information security monitoring are proposed, and necessary suggestions are provided for information security work.

INDEX TERMS Information security, big data, evaluation model, monitoring mechanism, Internet of Things.

I. INTRODUCTION

Environment of the Internet of things through comprehensive application of various kinds of equipment and technology, such as sensors, infrared detection, radio frequency identification, video monitoring, global positioning system (GPS), satellite remote sensing, etc.), real-time acquisition of various kinds of information (such as pollution, environmental quality and ecological information), to build a multi-level, all-round, the whole ecological environment monitoring network; Through the construction of mass data resource center and unified service support platform, it supports the whole-process intelligence of pollution source monitoring, environmental quality monitoring, supervision, law

The associate editor coordinating the review of this manuscript and approving it for publication was Md Zakirul Alam Bhuiyan.

enforcement and management decision-making of environmental business, so as to promote pollution reduction and environmental risk prevention, and promote the construction of ecological civilization. The purpose of cultivating new environmental strategic industries and scientific development of environmental undertakings [1]., through various types of network environment of things to achieve the following functions: one is the environment of information processing, for all kinds of environmental information for continuous acquisition, storage, analysis, according to the need to automatically generate a variety of environmental assessment report, help management department, a comprehensive grasp area environment and according to the change of the environment will start the corresponding contingency plans, timely inform the relevant departments in a timely manner to deal with, effective control of environmental change, maintain the stability of regional environment. The second is the remote control ability. The environmental Internet of Things has a strong control ability. Through the remote control, the information control center can cut off the discharge of any pollution source in time according to the need, so as to avoid environmental pollution and damage and realize the control of the regional environment.

In view of the information security problems in the context of big data, put forward corresponding solutions and measures from different aspects and perspectives. However, there are few researches on the information security control mechanism in the context of big data, and there are also relatively few researches on the information security evaluation system in the context of big data.

In this paper, the environmental IoT application of in-depth research and analysis, on the Internet of things technology, service-oriented technology architecture SOA, J2EE and MVC framework and other advanced technology to do a comprehensive research, is intended to establish a unified, stable, reliable, open, extension, reasonable and economic, norms, maintainable, comprehensive environmental quality monitoring platform, through the unified data platform and foundation support system, for online mass of real-time data acquisition network and provide data support real-time analysis, provides guarantee for the integration of various business systems. The relevant background of the era of big data is described in detail, and the importance and necessity of information security control under the background of big data is clarified. Starting from the information security control mechanism, the evaluation system of information security control is established, and based on this, the corresponding strategies for information security control under the background of big data are put forward.

II. RELATED WORK

The current environmental monitoring system based on Internet of things in a certain extent, can realize the function of environmental quality monitoring, but also has many problems, mainly reflected in the following several aspects: one is the dispersion system, independent application system construction, the lack of overall planning in terms of data sharing and business collaboration, lead to repeat construction, the ‘‘information island’’ phenomenon common [2], [3]. Second, the monitoring content of the system is limited. The environmental IoT can detect pollution levels and monitor illegal emissions through the pollution source monitoring system, but some environmental elements that have not been included in the monitoring scope have not been monitored, such as heavy metals, radioactive pollution, soil pollution, noise pollution, etc. Third, the practicability of the system function is not strong, so it cannot give full play to its supervisory role to improve the supervision ability of administrative efficiency. There is a big gap between the quality and quantity of talents and the construction and application requirements of the environmental Internet of Things [4], [5]. At present, almost all environmental departments at all levels have problems such as lack of complex information leaders and insufficient number of technical personnel, which is contradictory to the large-scale construction and large-scale application of the environmental Internet of Things. This situation will inevitably lead to unclear needs, incomplete research, not in-depth understanding, unreasonable design. The square, extensibility and stability of system design are important indexes to evaluate the quality of a system. Only by supporting extended applications and integration of heterogeneous systems can the isolated situation of pollution source monitoring network be broken [6], [7]. With ‘‘the service humanity, development platform, interface open, tools, practical’’ as the principle, to the system management data integration [8], [9]. Environment is a fusion of various environmental factors, only will have a unified operational environmental information construction and login unified platform, unified platform, unified construction standards, gradually realize cross-industry, cross-regional, cross-sectoral information linkage and resource sharing, promote each department business collaboration, data sharing, information exchange and data [10], [11] comprehensive utilization ability, environmental regulation can grow together. The goal of this system through the scientific, reasonable and feasible advanced system planning and design, integrated pollution sources monitoring, environmental quality monitoring and computer network information resources, including resources, environment online monitoring business information system construction ‘‘five one’’ goal [12], data collection and transmission ‘‘a net’’, information query present ‘‘picture’’, support system ‘‘one platform’’, ‘‘one center’’ data resource management and information release interaction ‘‘a portal’’. Establish a good foundation and framework for further building an environmental monitoring command information platform of ‘‘monitoring, monitoring and emergency response integration’’ [13], [14].

In the research on the status quo of information security under the background of big data, scholars have fully absorbed and learned from the advantages of research theories, and combined with the basic national conditions, and made a lot of achievements. Under the background of big data, as a result of the new characteristics of big data information security problem faces many new challenges, one of the main reasons for increasing along with huge amounts of data and focus/15 and 16th, computer virus will appear constantly, and quickly update the evolution, and under the background of big data have the characteristics of the nonlinear growth, the growth of the amount of data has a strong uncertainty, this also increased much difficulty to the information security work. Under the background of big data, the threat of information security mainly comes from the aspects of information content, storage carrier, information management and intelligent terminal. By summarizing and sorting out the current situation of enterprise data security of enterprises in the financial and communication industries [17]–[19]. There are threats to the information security of enterprises in these industries and their security needs are relatively prominent. The Internet industry, telecommunications industry, financial industry, medical industry and government organizations have different requirements and different degrees of information security needs [20], [21]. Starting from the protection of privacy information in the context of big data, it is proposed that there are many security risks in the collection, storage and use of big data at present, especially the privacy leakage caused by big data, which brings serious troubles to Internet users [22], [23]. It can be seen from the above research that scholars have a wide coverage of research on information security under the background of big data. They have conducted diversified explorations [24] from the perspectives of industry, individual and government, technology and application, etc., and put forward multi-faceted and multi-level information security issues.

In the aspect of information security strategy research under the background of big data, the necessity of building a national competitive intelligence system based on information security is discussed [25], [26], and the construction measures of the national competitive intelligence system based on information security are proposed. Intelligence literacy should be regarded as the core element of information security theory, and the solution of information security theory under the background of big data is explored [27], [28]. Due to the complexity of information security, it is impossible to completely solve the problem of information security, either theoretically or technically. Therefore, information security prevention technology should be combined with other technologies, based on the existing historical data [29], [30], to improve the pertinence, timeliness and effectiveness of information security prevention technology; From the perspective of ‘‘Prism Gate’’ incident, the problems faced by information security are analyzed, and the viewpoint of constructing information security strategy from the perspective of the rule of law is proposed [31], [32]. Based on the analysis of the importance of information security in the era of big data, the paper proposes that information security must be elevated to the height of national security strategy, the top-level design of network security work should be uniformly deployed, and the whole society should be mobilized to put information security work into practice [33], [34], so as to ensure the practical advancement of information security work. This paper analyzes the possible information security risks under the background of big data from nine perspectives, such as infrastructure and data processing, builds a big data information security risk framework and puts forward corresponding solutions. In contrast with the analysis of the information security governance mechanism in the United States, scholar proposed that network information behavior should be restricted by strict laws and standards [35], [36]. Can be seen from the above research, under the background of big data information security problem [37], [38], scholars from different aspects and angles puts forward the corresponding strategies and measures, but in view of the information security control mechanism under the background of big data analysis research is less, in view of the large data under the background of the research of information security evaluation system is relatively small. The overall level of environmental information at the national level is also developing constantly. Summarizes the development of environmental information, "twelfth five-year" period, the country overall improve the level of environmental information [39], [40], in terms of infrastructure, automatic monitoring ability, laid a certain foundation, but because of the lack of top-level design, there is a large amount of data, information integrity is low, and the problem of information security lack of consideration, information associated with the business support also is very good [41]–[44]. The difficulty in sharing existing data is the most serious problem restricting the development of environmental big data. It is proposed to build a sharing analysis platform to realize the integration of environmental big data, collect and collect various data such as pollution sources, environmental quality and emergency management, and realize application analysis through artificial intelligence [45]–[49]. This paper studies the overall development of environmental informatization, and concludes that at the present stage of the development of environmental informatization, firstly, an environmental monitoring and monitoring system should be established as the basis for environmental data collection. And form an effective integrated environmental management system to carry out various environmental business; at the same time, the data value is transformed through decision support and service.

III. OVERALL SCHEME OF INFORMATION SECURITY MONITORING BASED ON BIG DATA IN THE INTERNET OF THINGS ENVIRONMENT

Not access networked environment quality automatic monitoring station need access to design reasonable plan, to realize automatic monitoring data into a unified data platform, can video monitoring, the environment pollution into video monitoring system platform, industry integration platform for the integrated application of management, and to support further expansion of the business system. The system should adopt a multi-layer architecture and modularized development mode.

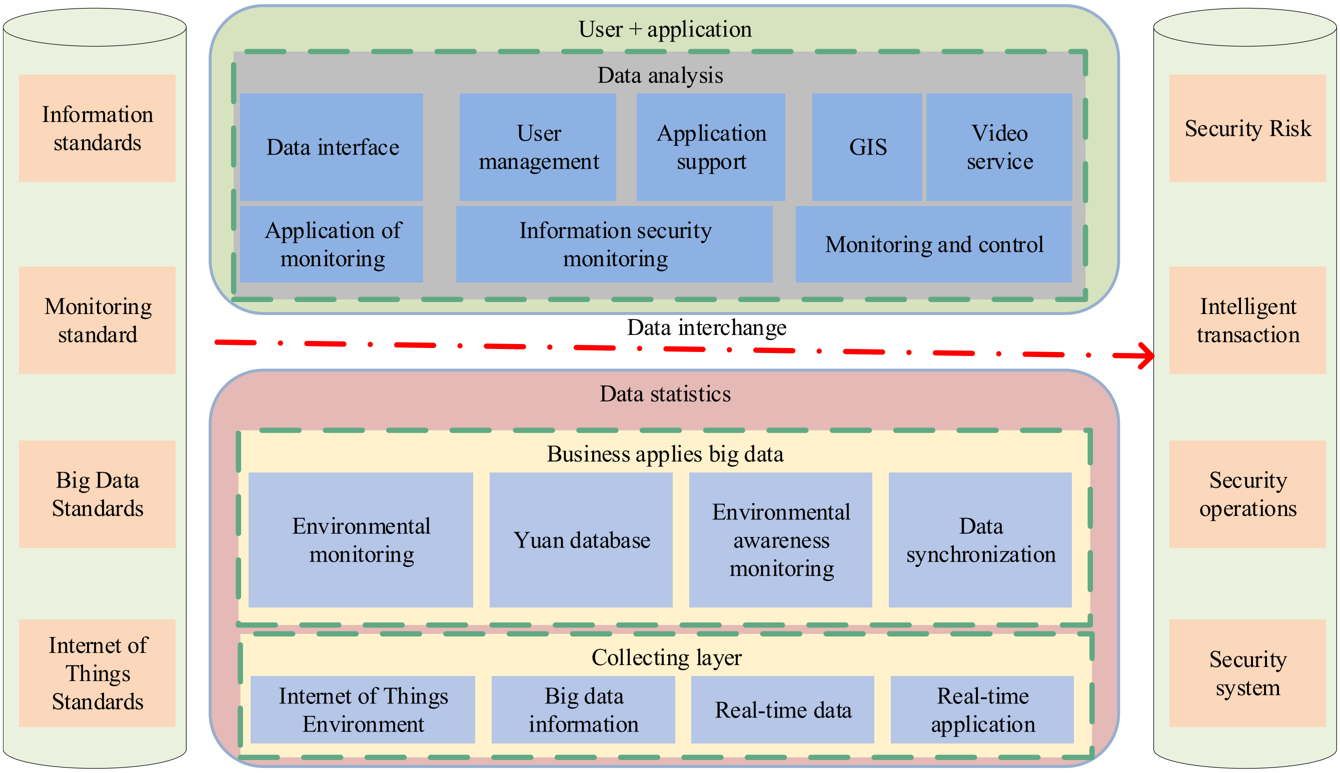

FIGURE 1. General Architecture of Information Security Monitoring For Big Data In The Internet Of Things Environment.

The acquisition layer, data layer, platform layer, business support layer and application layer should be separated. Each module is independent of each other, and its interface is open and clear. Allows system administrators to set up system application modules that users can use through permission management.

The overall architecture is designed and implemented in accordance with the idea of layering. The hierarchical architecture can decompose the construction tasks better, so that the construction tasks of the whole system can be built in parallel on the basis of clear interface definition, so as to shorten the overall construction cycle. At the same time, under the premise that the interface remains unchanged, the layered system architecture can also ensure that the system has a good adaptability to the development of the basic technology of each layer, and better reflects the data acquisition and integration as the core. The following is the overall architecture, which describes the technical components and logical relationships of the scheme, as shown in Figure 1:

A. ACQUISITION LAYER

The main data sources are surface water automatic station, air automatic station and pollution source site end. All kinds of real-time environmental monitoring data collected through front-end collection and monitoring equipment are collected and summarized by the background business system in a unified way, providing basic support for business application.

B. DATA LAYER

The data layer includes real-time data and business application data. The business data of this project can be divided into pollution source database, automatic environmental quality monitoring database, routine environmental quality monitoring database, environmental meta-database and GIS database.

C. PLATFORM LAYER

The platform layer mainly includes data synchronization, data statistics, data exchange, data analysis and data interface.

D. APPLICATION SUPPORT LAYER

Application support layer includes a unified user management, GIS services, video services, real-time data services and application services five independent modules, each module to provide access to service interface, the term through the integration of basic service layer, the formation of the corresponding system for building on running the application system to provide all kinds of generic function.

E. APPLICATION LAYER

Environmental quality monitoring platform is made up of ‘‘environmental quality automatic monitoring system’’, ‘‘pollution source monitoring system’’, ‘‘environmental quality monitoring data management system’’, ‘‘environmental video monitoring management system’’, ‘‘integrated application of GIS platform’’, ‘‘comprehensive application management platform’’, ‘‘administrative efficiency supervision system'' and ''information release and interactive platform'' multiple business application subsystems, common on a uniform application support environment.

F. SOFTWARE LAYERED ARCHITECTURE

The hierarchical software architecture is shown in Figure 2:

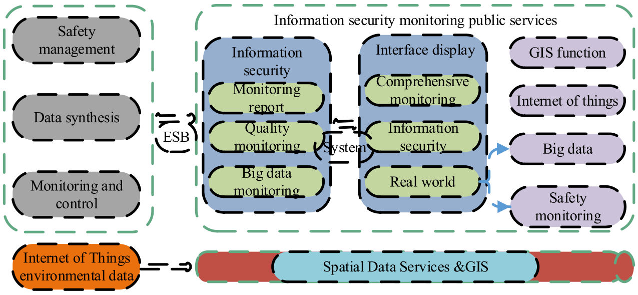

FIGURE 2. **Software layered architecture.**

The software is divided into four parts: interface display layer, interface service layer, business service layer and public service layer.

(1) The main function of the interface layer is to complete data and function interaction with users, and the interface layer is the centralized presentation of system functions. In the system, all the functional modules of the interface layer are provided in the form of plug-ins, and the operation is driven by the environment integrated business service integration framework.

Application interfaces for different users and application scenarios can be customized quickly through different combinations of plug-ins in the interface layer. Functions also facilitates the rapid development and deployment of new functional modules. The interface service layer includes environment integrated business service, report service, GIS service, video service and so on.

Through the combination of interface function plug-ins, different thematic management systems can be customized quickly on the environmental protection comprehensive application management platform.

(2) The interface service layer is the support for the data display and functional interaction of the interface layer, which completes the user operation control and the management of the data presented on the interface. The interface service layer realizes the separation of user interface presentation from business data and business logic and can quickly adapt to the change of user interface requirements.

(3) The business services layer provides business support to the interface services layer through service interfaces published on the ESB. Business services layer by calling the data center data interface and environment spatial data sharing service platform of GIS interface respectively read data between environmental data and loophole, the data result through service interfaces, each business service layer interface is usually an independent business functions of the original services, complex can be achieved through the combination of the interface between the business logic.

(4) The public service layer mainly includes the data interface service of the environmental data center and the GIS interface service of the environmental spatial data sharing service platform.

Application support platform is a common operating environment system framework in environmental business implementation environment. It is a logical platform located between network system, operating system and business application system. It is composed of many specialized service components and middleware, which is the basic structure of application system construction and plays a role of connecting the preceding and the following. Application support platform to provide the most basic components, such as the application server middleware and message middleware, is responsible for data transfer and resource allocation, with the underlying integration services to provide application system interface component, application integration service components, shared business services based service components, components and support application system development and integration. At the same time, the data integration service component is provided to realize the unified access and management of data in the data center. The portal service component enables all business application systems to be integrated in the same environment and provides a single entry, unified user interface, unified user management and authority management.

The application support platform can meet the requirements of providing business data, real-time data, GIS and video services to the third-party system platform. All services must be secure and reliable and need to be registered and managed on the platform.

G. INFORMATION SECURITY MONITORING OF BIG DATA IN THE INTERNET OF THINGS ENVIRONMENT

Monitoring data requires certain bandwidth support when transmitting data from the front-end storage unit to the monitoring center. Data transmission is based on TCP or UDP protocol, and the original data needs to be packaged and compressed. Networked data transmission uses the existing environmental protection network, which needs to meet the requirements of the existing network bandwidth. The data of each central station is transmitted through the backbone of the overall design of the data acquisition network project of the automatic station of the provincial environmental protection department, the local area networks at all levels, the monitoring sub-stations, and the special networks of the communication and monitoring center of the company. Through ADSL/CDMA/GPRS and other network connection. The overall structure is divided into surface water monitoring station data according to the collection source. Data from each sub-station will be transmitted to the provincial department network center platform in real time. The center network platform realizes the reverse control function of the front-end acquisition system through software and hardware.

1) INFORMATION SECURITY AUTOMATIC STATION MONITORING NETWORK

According to the bandwidth required by the front end and the field environment, the information security automatic station chooses wireless 3G and wired mode for transmission. The wired mode is preferred for uploading data at the sub-station networking. When the sub-station is remote and wired construction is difficult, wireless 3G networking is considered. The video monitoring data of the sub-station is transmitted to the operator's video monitoring platform through the private network, and the monitoring data is transmitted through Internet VPN and private network. See Figure 3.

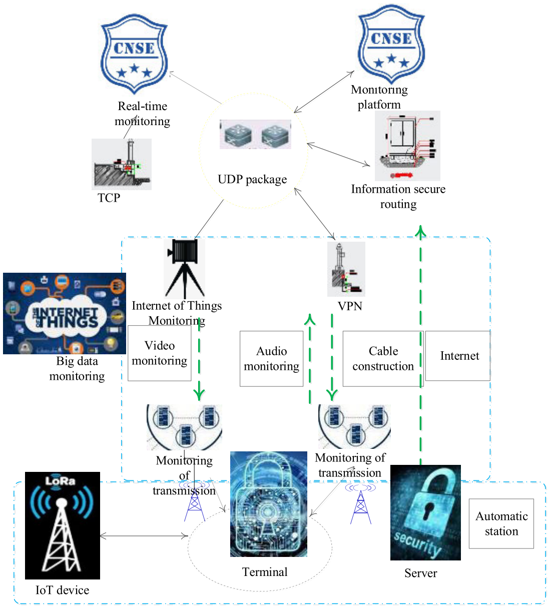

FIGURE 3. **Transmission mode of information security automatic station.**

2) REVIEW DATA UPLOADING

After the original monitoring data of sub-stations is uploaded to the central station (city station or county station), it shall be verified and sent to the provincial department. According to the current data networking scheme, the monitoring data of ground surface water substation is uploaded to the private network adopted by the central station for transmission, and the data receiving server can be directly connected to the private network of the central station to realize the reporting of audit data. However, the monitoring data of air substation is uploaded to the central station by Internet VPN transmission, and the central station needs to add VPN equipment to connect with it. In order to ensure the upload of audit data, the VPN equipment and the ring unified private network need to communicate with each other, and it is suggested to connect through the firewall in the middle.

According to the scientific principle, the host server is divided into six parts, which are real-time data server, business application data server, GIS engine /Web server, application platform server, data business support server, and information release server.

3) REAL-TIME DATA SERVER

Real-time database server is used to receive automatic pollution sources monitoring and environmental quality of real-time data, a large number of real-time data needs to be stored in the database server, but also bear the application platform of real-time data, to be obtained in the design adopts double machine configuration operation, ensure the normal operation of real-time data collection and stable.

4) BUSINESS APPLICATION DATA SERVER

The business application data server undertakes all the data required by each application system, which requires strong processing ability and high stable operation ability. Therefore, the database server is designed to run in a dual-machine configuration. Deploy the database management software on the server, where each node can be used individually and load balanced by the application, with the ability to switch online. If the hair

Outside the business, such as the failure of a node, the node failure switch can be realized to ensure the high availability of the database 7 × 24, for the realization of the stability of environmental data.

5) GIS ENGINE/WEB SERVER

Web services and GIS engine services are uniformly deployed on the GIS engine /Web server platform, and the database is configured on the business application data server platform. This configuration is especially suitable for sites with large databases. A single database can provide data services for multiple servers and provide powerful GIS operation support for applications.

6) APPLICATION PLATFORM SERVER

In order to achieve the project goals, integration of unified data platform construction, business support platform, environment quality automatic monitoring system, automatic pollution source monitoring system, environment quality monitoring data management system, video monitoring management system, integrated application of GIS platform, integrated application of management platform, design all the business application server, to the business platform in order to be able to make the system stable platform run normally, the design of double machine configuration operation.

7) DATA BUSINESS SUPPORT SERVER

The service support server carries the statistics, synchronization and analysis of all data with high real-time performance. Meanwhile, it also provides data interfaces related to the business layer to support the stable operation of the business platform. In order to ensure the stable and normal operation of the system platform, the two-machine configuration operation is designed.

8) INFORMATION PUBLISHING SERVER

This server is deployed on the external network, mainly to provide the release of business data, and the platform can support the maintenance of enterprise information and operation and maintenance information. Relatively speaking, the information release server carries a small load, real-time requirements are not high, so equipped with a server.

IV. CONSTRUCTION OF INFORMATION SECURITY MONITORING MECHANISM UNDER THE BACKGROUND OF BIG DATA IN THE INTERNET OF THINGS ENVIRONMENT

A. ANALYSIS OF INFORMATION SECURITY CONTROL ELEMENTS

In the context of big data, the establishment of information security control mechanism is very important for the development of information security work. The establishment of information security control mechanism should revolve around the elements of control function. Control functions of components including the controller, the control object and control means and tools, will be summarized and constituent elements of the control function extension processing, controller will be open for ''network control personnel'', its extension, including connotation of network security management object and network security management, control object is summarized as ''environment'', the extended connotation includes network facilities, network culture and policies and regulations; The means and tools of control are summarized as ''technology'', and their extended connotation includes four aspects: ''prevention, secrecy, control and examination''.

1) ''PREVENTION'' ONE FIREWALL TECHNOLOGY

''Firewall'' is a network security system located between the internal network and the external network. It is an access control executed when the two networks communicate. It belongs to the category of network communication monitoring system. ''Firewall'' is built on the network boundary, has the function of guaranteeing the security of computer network, which can be reflected in software products, and can be made or embedded in some hardware products. Usually a firewall is a group of software systems and hardware devices that build a secure barrier between the internal network and the external network. Based on the logical perspective of fire prevention, its function is reflected in the separation and restriction and analysis; In terms of the composition of network security policy, the firewall can effectively manage network security by controlling and monitoring the information exchange and access behavior between networks. In the implementation of protection, the firewall is in the core position. The firewall is the only way through which all intranets and extranets are connected. Checking and connecting take place here, only through authorized communications. Based on certain conditions, the firewall has the function of isolating the internal network from the external network, and it can prevent the illegal intrusion and the illegal use of system resources.

2) ''SECRET'' - DATA ENCRYPTION TECHNOLOGY

Under the background of continuous development and innovation of science and technology, only by updating and improving encryption technology can the current information security needs be met. Symmetric encryption and asymmetric encryption are two types of encryption technology. Symmetric encryption is to encrypt and decrypt with the same key. At present, it is the most widely used encryption technology. The typical sessionkey is the Data Encryption Standard (DES) used by the United States government. On the contrary, asymmetric encryption (public or private key) technology is to use different keys in encryption and decryption, in which the public key can be published to the public, and the private key is held by the private key, so the security of data is guaranteed. In order to secure the transmitted data, encryption and decryption of data are essential. Encryption is to convert plaintext data into a specific cryptographic algorithm, so that it is not easy to recognize the degree of a certain plaintext can rely on different keys and the same algorithm for encryption, the formation of different ciphertext. Decryption is to transform ciphertext data into plaintext data by key.

3) ''CONTROL'' - INTRUSION DETECTION TECHNOLOGY AND NETWORK MONITORING TECHNOLOGY

Intrusion detection system is a system to identify and deal with malicious use of computer and network resources. External intrusion of system behavior and unauthorized internal user behavior is the main content of its processing. Intrusion detection system is a technology that can detect and report the unauthorized phenomena in the system in time. Its purpose is to provide guarantee for the security of computer system. Intrusion detection system includes intrusion detection software and hardware. Network monitoring is to monitor and control the computer in the local area network. In the context of big data, the use of the Internet is becoming more and more common, and the use of network monitoring technology is becoming more and more frequent. Monitoring software and monitoring hardware are the main types of network monitoring products.

4) ''AUDIT'' - SECURITY AUDIT TECHNOLOGY

Computer network security audit is at a certain security policy as the guide, to record the information such as the system activity as the backing, environment of events and activities for inspection and examination and inspection operation, to identify system vulnerabilities and intrusion behavior, improve the system performance of technology, is also to review system security risk assessment and corresponding measures process, is an important means to improve the system security.

B. INFORMATION SECURITY MONITORING AND CONTROL MECHANISM MODEL

In the information security control mechanism, people are divided into network controllers and network security managers. As one of the network controllers, network users should set up the correct awareness of information security in the network activities, under the information security-related education and guidance, implement self-management, standardize their own network behavior. Network user's

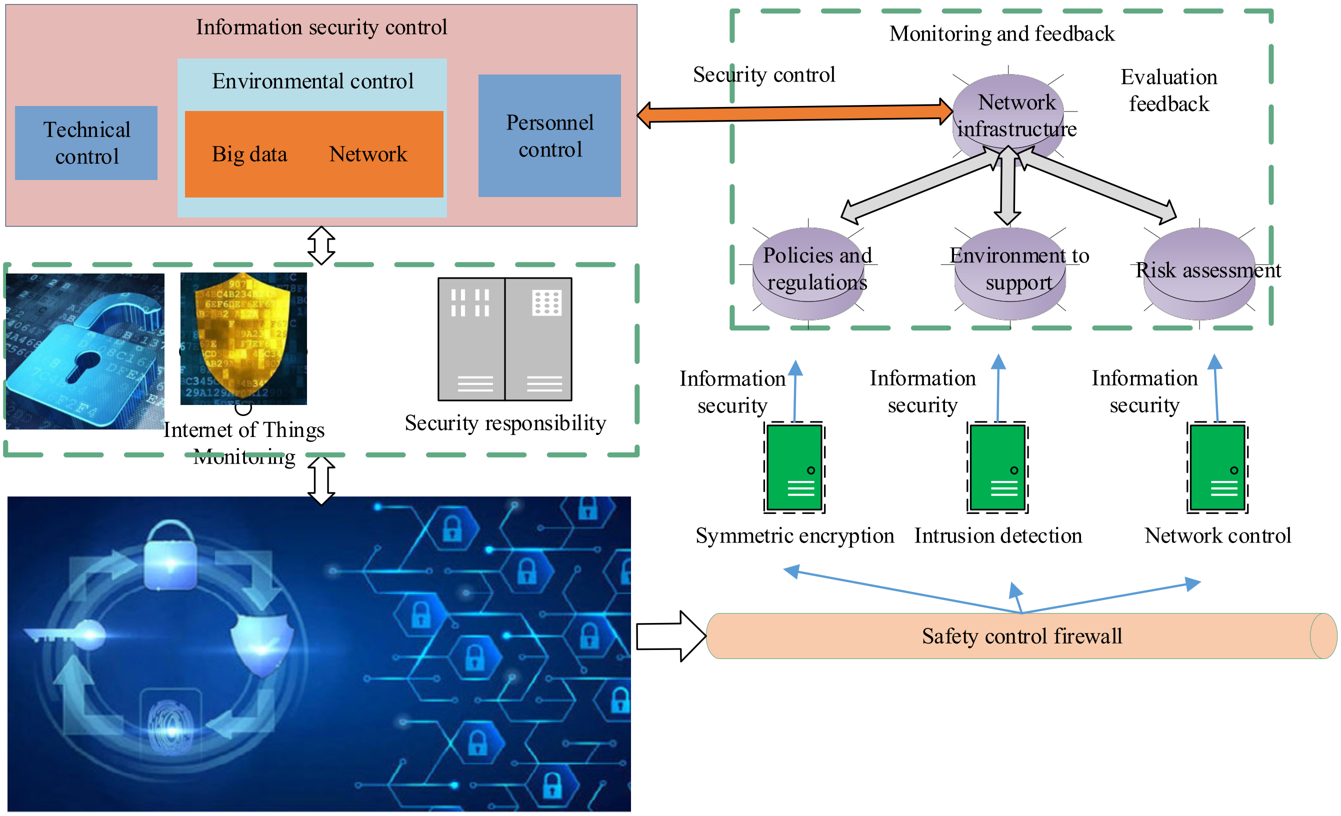

FIGURE 4. Network information security control mechanism model.

information security awareness is particularly important, information security is neglected, largely due to the lack of safety consciousness, the improvement of network users' information security awareness for the implementation of the information security management work of great importance, can fundamentally build information security thoughts ''firewall'', from the source to reduce information security problems. During the operation of the information security control mechanism, network users can install anti-virus software consciously, update the system or patch the system in time, do not download and install software from unknown sources easily, be alert to the links sent by strangers, and disclose personal privacy information cautiously. Moreover, as network users, should consciously abide by the relevant provisions, on the basis of improving their own awareness of information security and self-management, standardize their own network behavior, do not harm the behavior of information security. The mechanism model is shown in Figure 4.

As another object of network information security management, network information service provider plays an important role in network information security control mechanism. As the provider and holder of data and information, the network information service provider has a great initiative in the network information processing, so it also bears the important responsibility of network information security. Therefore, network information service providers should accept the supervision and management of network information security managers, clarify their own responsibility for information security, follow relevant laws and regulations on network information security, standardize their own network behavior, and rationally develop and use data and information on the basis of protecting the legitimate rights and interests of network users.

The construction of network information security control mechanism under the background of big data requires the government to systematically and comprehensively construct the system of laws and regulations to realize the rule of law of network information security protection. The role of legislation in protecting the security of network information lies in that it puts the security of network information under the protection of law, and creates an orderly network environment by establishing the bottom line of the rule of law for the virtual network world. Protective mechanism on the one hand, laws and regulations in the form of the legal government, intermediary organizations, enterprise organization in the network information security responsibility, the law itself has a mandatory behavior for rib, the network information security, such as hacking, rumors spread viruses and can largely deterrence and constraints. On the other hand, laws and regulations through the establishment of the corresponding punishment measures, can be in the network information security accident as an effective way to crack down on network security crimes, so as to promote the network information security protection work in a timely and effective manner.

TABLE 1. Evaluation index system of network information security control mechanism.

Personnel	Web users	Network user safety education
		Network user security awareness
		Web users manage themselves
	Network information service provider	Provider's Security Responsibility
		Provider security behavior
	Management personnel	Technical ability of management personnel
		Safety literacy for managerial positions
		Professional management personnel
Environment	Network infrastructure	Carrier capacity of network facilities
		Data processing capability of network facilities
	Network culture	Cultivation of network culture
		Purification of Internet Culture
	Policies and Regulations	Network information security implementation standard
		Code of conduct for network information security
		Network information security legislation
Technology	Firewall Technology	Network user access rights
		User access authentication
		Protect against denial of service attacks
		Anti-malware
	Encryption technology	Storage encryption technology
		Communication Encryption Technology
	Safety monitoring technology	Application system access control
		Database system access control
		Operating system access control
	Security audit technique	Application system log auditing
		Database system log audit
		Operating system log auditing
		Intrusion detection control audit
		Antivirus upgrade audit

C. NETWORK INFORMATION SECURITY CONTROL EVALUATION SYSTEM UNDER THE BACKGROUND OF BIG DATA IN THE INTERNET OF THINGS ENVIRONMENT

From the perspectives of personnel, environment and technology, a multi-level and multi-index information security control evaluation index is designed and constructed, as shown in Table 1.

The simplified operation of the feature vector is used to calculate the weight of each index, check the questionnaire, and take the average value according to the valid questionnaire, construct the judgment matrix, and use the vector.

The calculation method used in this paper is the sum product method, and the specific steps are as follows:

(1) Normalize each column of elements of the judgment matrix, and the general terms of the elements are as follows:

$$c_{ij} = \frac{c_{ij}}{\sum c_{ij}}, \quad i, j = 1, 2 \ldots . \tag{1}$$

(2) Add the normalized judgment matrix of each column according to rows

$$\omega_{\mathrm{ij}} = \sum_{c_{ij}} c_{ij}, \quad i, j = 1, 2, 3 \ldots . \tag{2}$$

TABLE 2. Average random consistency index R.

N	1	2	3	4	5	6	7	8	9
R.I.	0.1	0.13	0.54	0.92	1.15	1.13	1.34	1.42	1.48

(3) The vector w is the approximate solution of the eigenvector.

(4) Calculate the maximum eigenroot of the judgment matrix

(5) The consistency index of judgment matrix C.I. was calculated by using the maximum eigenroot.

The larger the value of consistency index C.I. is, the greater the degree of deviation of judgment matrix from complete consistency is. The smaller the value of is, the closer the judgment matrix is to complete consistency. For the multi-order judgment matrix, the average random consistency index R.I is introduced. Table 2 gives the average random consistency index obtained from 1000 calculations of positive reciprocal matrices of order 1-9:

Attention should be paid to the construction and maintenance of network facilities, we should use all kinds of security technology means to protect network information system and database, make full use of the security mechanism of database system, application system and network system, and build and maintain network information security system comprehensively and professionally. In addition to strengthening the construction of external hardware facilities, the internal network and database should be effectively managed to ensure the security of stored information. Moreover, we should have the security consciousness of taking precautions, build the disaster recovery backup system, and provide information security guarantee from the network information security system architecture. Set up a distributed data storage system, conduct decentralized data management, build a local backup system, ensure the security of key data, and ensure the stable and reliable operation of the data center. Meanwhile, in addition to ensuring that data centers are protected from attacks, they can also avoid data loss due to earthquakes, fires, or other natural or man-made disasters.

There are three monitoring schemes for bad information: the export flow of each IDC room is fully monitored; Full-volume or sampling monitoring is carried out on the traffic of IDC aggregation layer; Climb IDC managed content through crawler.

According to the unified requirements of the Ministry of Industry and Information Technology, operators all adopt the way of full monitoring of IDC traffic to monitor bad information. In order to compensate for HTTPS encrypted traffic cannot be monitored, a crawler system is added to carry out keyword crawling on HTTPS websites.

The construction of IDC/ISP information security management system began in 2013 according to the unified planning requirements of the Ministry of Industry and Information Technology. The system and traffic related functions mainly have two points: record source/destination IP address, source/destination port, access to ask, belong to the HTTP protocol needs to retain URL; A plugging order can be issued. Blocking rules are set according to IP address, domain name, URL address, keywords and other conditions, and TCP RESET message is sent to block.

In the course of actual use, you can get two very useful types of data. One is by setting the keyword library, so that the system white action matching traffic data in the content and keywords whether hit, and output hit URL and text content. The other is to obtain the URL, separate the domain name, output the active domain name after reduplication, and provide the data source for the subsequent monitoring of the unrecorded domain name.

(1) Data input of unrecorded domain name consists of three parts. The first is the unrecorded domain names in the DNS traffic, the second is the unrecorded domain names output by the CU unit, and the third is the unrecorded domain names in the stock due to the cancellation of the record number.

(2) Monitor whether the unrecorded website can be opened. If it can be opened, it needs to enter the plugging process and make it offline; if not, it should enter the monitoring queue and continuously monitor its online situation.

(3) Follow the principle of blocking before notification for the unrecorded domain name, and make the unrecorded domain name website inaccessible by means of IP domain name blocking. After notifying the user to put on record in time, the user will initiate the application for IP domain name to be unsealed and the website will resume online.

Suspected bad information found in the monitoring link of bad information shall be processed on the disposal platform.

First of all, through intelligent analysis of text semantics and manual combination, it is confirmed that the suspected bad information in the keyword hit webpage does contain bad information. Usually less than 1% of the data is ultimately identified as bad information.

Secondly, the responsible unit of the user is identified through IP comparison, and the responsible unit notifies the user to deal with bad information. Finally, the user feeds back the processing results, and the disposal platform puts the webpage with bad information into the daily tracking and monitoring queue, and the process ends.

Log monitoring should cover all information network assets, and combined with the existing security protection system and the actual operating environment, the integrated monitoring access mode of combining local log and network log should be used.

1) Local log: log generated by network security equipment, platform software and application system's own security functions. Advantages are able to make full use of the existing safety protection ability, more comprehensive record related safety incidents; The disadvantage is that some systems open the security log needs to occupy a lot of system resources (such as database system).

2) Network log: it analyzes and records the operation behaviors of accessing all kinds of devices and applying network resources by mirroring. The advantages are that it does not occupy the resources of the monitored system, does not need to transform the existing system, and is flexible in deployment. The disadvantage is that it cannot record the local operation behavior and cannot analyze and audit the encrypted data stream (e.g., SSH, HTTPS). In the specific application, network security equipment, platform software and application system log functions should be rationally configured to adapt to log monitoring in different systems and networks, so as to avoid function overlap and resource waste. For example, the user operation information of SSH, HTTPS and non-standard applications can be obtained through the local log. At the same time, the database operation information can be obtained through the network log in order to avoid the performance degradation of the database system.

The security log of the equipment and system can only identify the security events that have occurred, and could not monitor the vulnerability of its own. Once its vulnerability is used by the attacker, the consequences are serious. Because of the great harm of security vulnerabilities, it should be found and repaired in time before the vulnerability is used. Loopholes in construction should be compatible with the world's largest public library (Common Vulnerabilities and Exposures, CVE) vulnerability scanning system, according to the characteristics of the network and information system, give full consideration to the source of the leak, availability and other factors, formulate scientific strategy of vulnerability scanning for the export of all kinds of network information assets vulnerability monitoring, monitoring results and will scan for access.

The internal factors mainly refer to the threat posed by the human operation inside the enterprise to the host information security. When it comes to network security, people will unconsciously associate with network boundary security, but in fact, most of the security risks in the network are generated in the internal. For example, in daily work, employees intentionally invade the internal server system of the company through illegal means to steal the important information of the company and endanger the security of the company. Among them, the non-standard operation or subjective operation error of the company's network managers and operators is also one of the important factors that endanger the security of the host network information. Other reasons for internal information leakage include imperfect rules and regulations of the enterprise, staff ignoring the rules and regulations, leakage in the carrier handover process, improper internal network management, etc. According to a survey of 484 companies conducted by the FBI in the United States, 85% of security losses were caused by internal reasons, as shown in Table 3.

For the behavior of endangering the host information security within the enterprise, the first can be protected by the way of internal and external network isolation. The common method of internal and external network isolation is physical isolation. Enterprises build different networks to protect the information security of the host, but this way also has certain disadvantages. Some Intranet users may set up VPNs privately in violation of the rules and regulations of the enterprise, or access the external network by secretly dialing

TABLE 3. FBI security scanning survey results of 486 companies.

Serial number	Security incidents	Possession ratio %
1	Internal security threat	86
2	Internal unauthorized storage	13
3	Patent information was stolen	15
4	Financial fraud by insiders	11
5	Data or networks are compromised	11

up or wireless network. This provides an opportunity for the hacker to establish a connection by dialing, etc. As people pay more and more attention to the information security of the host, according to the technical requirements of computer information secrecy involving national secrets, enterprises with high density involved should also build their own confidential information system to carry out security monitoring of the host information, and establish a three-level protection mechanism beforehand, during and after the event. Among them, the extrance mechanism means to control the classified computers, the in-process mechanism means to monitor the use of the classified computers, and the ex post mechanism means to monitor and audit the classified computers. And the confidential information system server is built in the company, completely isolated from the external network, through a specific IP host for access, and the use of unified confidential media to transmit data, is the most important measure to monitor the security of the host information within the enterprise.

The flow of big data Internet of Things information security monitoring algorithm:

Step 1: Initialize a group of particles (population size m), including random position and velocity;

Step2: evaluate the fitness of each particle;

Step3: For each particle, compare its fitness value with the best position PBest that it passes through. If the OK, make it the current best position pbest;

Step4: For each particle, compare its fitness value with GBest, the best position it passes through. If the OK, make it the current best position gbest;

Step5: Adjust the speed and position of the particles;

Step6: If the ending condition is not met, go to Step2.

Iteration termination condition is generally selected as the maximum number of iterations Gk or (and) the optimal position searched by the particle swarm so far satisfies the predetermined minimum adaptation value according to the specific problem.

The main work of data preprocessing is to analyze and normalize the massive historical data, and the analytic hierarchy process is adopted here. This model in the application of analytic hierarchy process the main idea is based on your own history network security events can be divided into network attack, information broken, malicious software, information content security four categories, and combining the actual logging and classification of IDS is subdivided into 72 classes of network events, thus design a model includes four levels of awareness, get each time calculated by using hierarchical analysis method integrated monitoring of a single value, using a single situational values to describe the system security situation of the current point in time. The training samples and prediction samples are constructed, and parameters such as population, iteration times and termination conditions are set. The big data information security monitoring algorithm in the Internet of Things environment is used to find the best parameters C and G of SVM. When the maximum number of iterations is reached or the termination conditions are met, the program ends, the prediction process is shown in Figure 5.

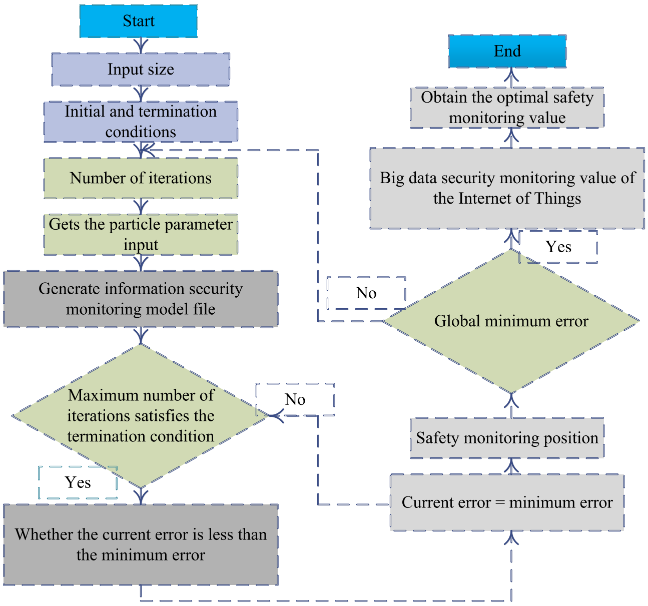
Start
Input size
Initial and termination conditions
Number of iterations
Gets the particle parameter input
Generate information security monitoring model file
Maximum number of iterations satisfies the termination condition
No
Yes
Whether the current error is less than the minimum error
End
Obtain the optimal safety monitoring value
Big data security monitoring value of the Internet of Things
Yes
No
Global minimum error
Safety monitoring position
Current error = minimum error

FIGURE 5. Information security prediction process.

V. EXPERIMENTAL VERIFICATION

This section carries out simulation verification of service classification. Based on the Naive Bayes algorithm and using Matlab 2016b as the simulation software, we firstly divide the security level of services into 4 categories, which are I, II, III and IV, respectively. Among them, the services of class I and class IV belong to the security zone of wireless public network intervention. The algorithm was trained with 1000 pieces of data and tested with 50 pieces of data.

Visualization results of four training data extraction are shown in Figure 6:

Each pie chart represents 1 input for the corresponding business. Here, four input data are selected. The proportion of the four colors represents the probability that it belongs to this business. It can be seen that the four kinds of services can reach the maximum under the corresponding probability to be correctly classified.

Machine learning algorithm is a fitting process based on big data, so the amount of data directly affects the classification accuracy. Figure 7 shows the relationship between data volume and classification readiness rate. The accuracy rate was 97 percent with 1000 more training data.

Six test data were input into the classifier to calculate In(Pa /Pb), and the results were shown In Figure 8:

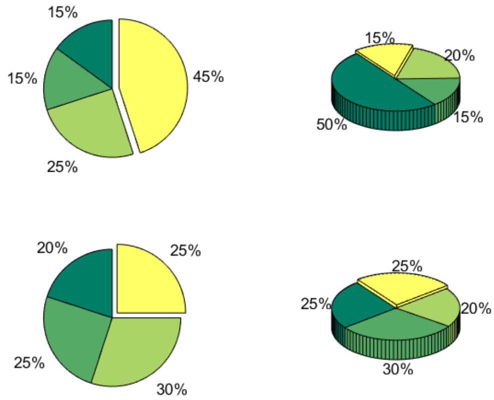

FIGURE 6. Simulation results of Bayesian service classification.

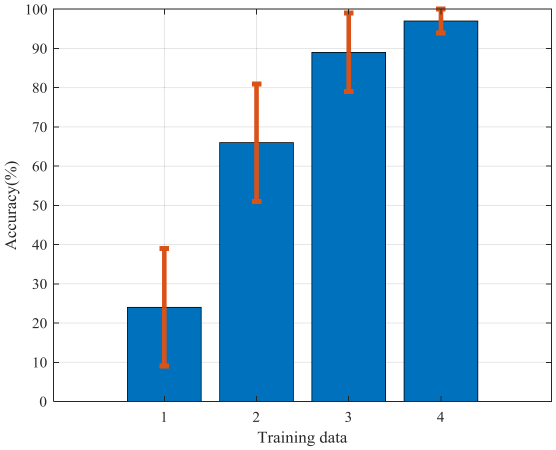

FIGURE 7. Influence of training data amount on accuracy.

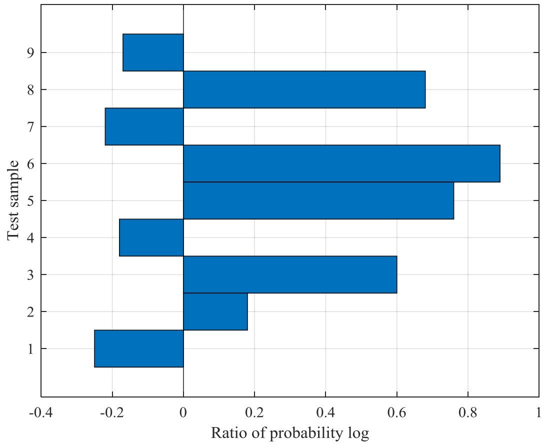

FIGURE 8. Simulation results of Bayesian anomaly detection.

It can be seen that after E is used to replace 0 as the decision boundary, not only abnormal samples are successfully judged, but also the correct sample 2 is avoided to be judged as abnormal.

Provide comparative analysis of historical data and central trend data analysis. The system provides comparative analysis of historical data mainly including single factor single site, single factor multi-site and multi-factor single site historical data comparison functions.

(a) Users can choose time period, time granularity and monitoring factors according to their needs to compare and analyze the data of two time periods of a site.

(b) Users can compare and analyze the monitoring data of the same monitoring factor from multiple sites according to their needs, in which time granularity is optional. Data granularity includes: minutes (gas station data), hours, days, weeks, months, seasons and years.

Factor (c) more than single site history data analysis is mainly used for the same site factor, compares the monitoring value of multiple monitoring, in order to find out the correlation of the monitoring project monitoring value trend, at the same time to choose monitoring value of data granularity, granularity of data include: minutes, hour, day, week, month, season, year. The page effect is shown in Figure 9:

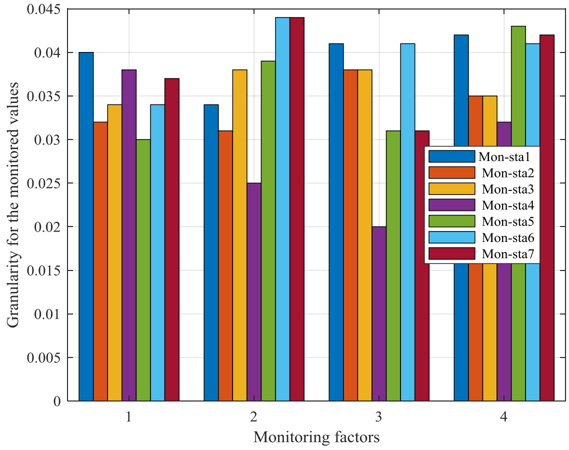

FIGURE 9. Comparative analysis of historical data.

The system provides trend analysis of single point and multi-point center data. The trend analysis of single point center data is to carry out trend analysis of central data on the monitoring data of a certain station and the same period, mainly including arithmetic mean, geometric mean, median, percentile, standard deviation, range and mode, etc. The multi-point central trend can be analyzed according to the station situation of a river.

There are three main types of real-time data presented. Monitor real-time data, equipment online situation, monitoring equipment online situation including online and communication interruption, the system will be different colors to distinguish different states; Data status, divided into normal, alarm and missing data. For different states are also expressed in different colors, so that users can be clear at a glance. The system supports custom query conditions, you can set the focus site for targeted query. Real-time curve shows real-time data to users in the form of curve graph, which is convenient for users to understand the change trend of real-time data of each monitoring project and make corresponding decisions in time. Real-time curve is a trend curve that shows the current monitoring data at the monitoring point.

Figure 10 is the effect diagram of real-time change trend of information security.

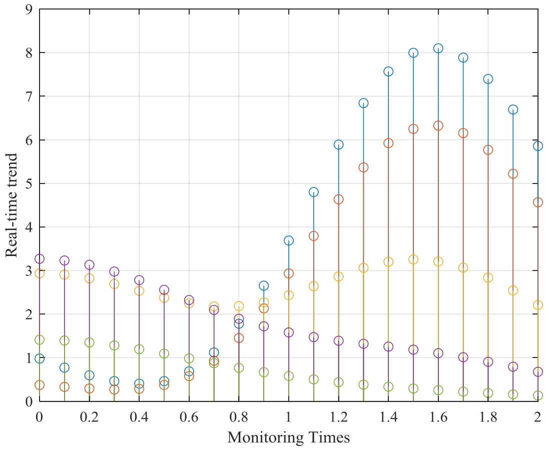

FIGURE 10. Rendering diagram of real-time change curve of information security.

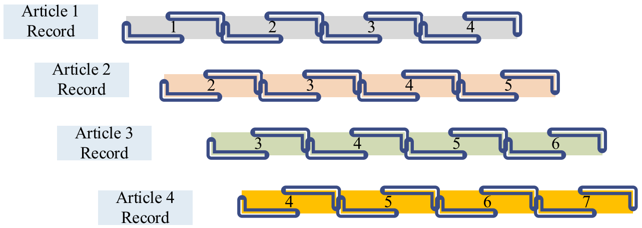

FIGURE 11. Sliding window method.

TABLE 4. Network communication test results.

	Use the number of days	Broken network number	Connection status	Packet loss rate
Terminal 1	185	6	Disconnect	0%
Terminal 2	185	6	Connection	0%

The network communication test is mainly conducted in two aspects. One is the packet loss rate, which is an important indicator to measure the reliability of communication equipment. The packet loss is mostly caused by the network itself or network communication equipment, such as insufficient network bandwidth, slow processing speed of switch or router, etc. The other is the stability of the network connection, that is, the effectiveness of the reconnection mechanism, whether it can automatically re-establish the network connection in the event of a network failure. Two terminals were set for comparative test. Terminal 1 did not enable the network disconnection reconnection mechanism, while Terminal 2 did. The test results are shown in Table 4.

It can be seen from Table 4 that the packet loss rate of both terminals is 0, because the data amount transmitted each time is only dozens of bytes, and the network congestion will not be caused by insufficient bandwidth. During 185 days of testing, the server detected 6 network outages. Terminal 1 did not reconnect after each outage, and Terminal 2 was able to reconnect automatically.

Finally, the time series of situation values corresponding to the monitoring time points are obtained, which need to be divided into training samples and test samples. Because the obtained time series is too large, it is impossible and unnecessary to input all the training samples as well. Meanwhile, in order to realize a faster safety warning, the concept of sliding window is used in the selection of training samples in this model. The specific implementation is to select a fixed time interval (such as 4 days) as the initial window to make training prediction; then the window slides back for a period of time (such as 1 day) to make training prediction. So the Windows slide alternately. See Figure 11 for the detailed process.

TABLE 5. Model training input parameters.

Parameter	Set the value
Particle swarm size	35
Particle space dimension	5
Inertia weight	(0.9,0.2)
Inertial factor	3
(C, G range)	(0.1,35000),(0.1,10)
Particle velocity range	(0, 30), (0, 0.005)
Maximum number of iterations (k)	300
Nuclear methods	Gaussian random
Inertia weight function	w1-((wl-w2)/k)

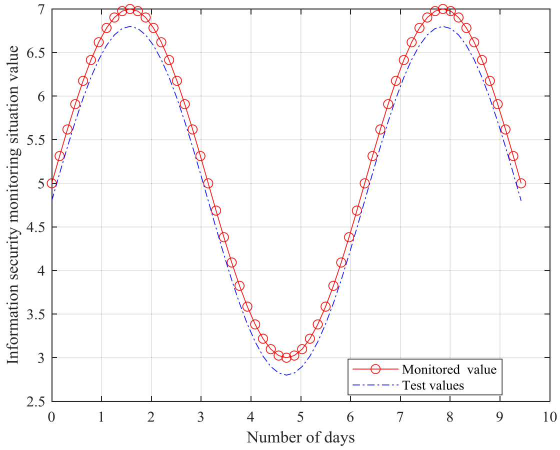

FIGURE 12. Function curve.

Using sliding window to construct training samples can make the originally completely discrete data set into partial linear correlation, that is, a time series with self-covariance coefficients between (0.25-0.75) is constructed.

The training parameters of the common big data information security monitoring model in the Internet of Things environment are shown in Table 5.

As shown in Figure 12, according to the historical data analysis, the curve of the monitoring information security situational values fluctuate quite gentle, and the theoretical results fit well with the test function curve, so from now on function according to different worth to the corresponding function X Y value to construct the situational predictors of training sample, test sample and forecast sample testing, where X is rounded represents the number of days, the corresponding function values Y to approximate the information security of the monitoring values.

The optimal parameters C and G found by information security monitoring are 22462.59 and 4.08 respectively, and the minimum error of prediction is 3.99%. The comparison results between the predicted results and the real value are shown in Figure. 13.

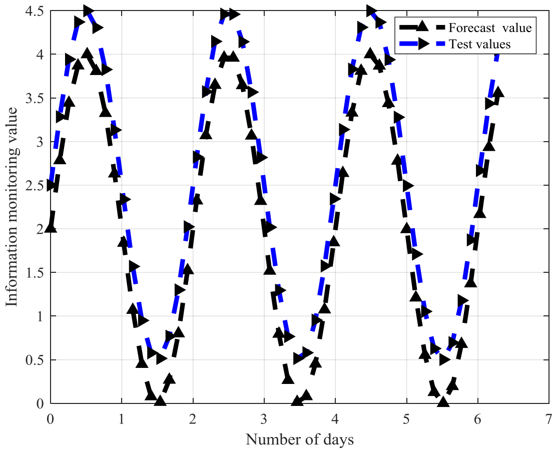

FIGURE 13. Comparison of predicted results with real results.

VI. CONCLUSION

Improving environment of information development in our country, but the network security business is developing at an early stage, the state bureau of technical supervision and other departments, under the guidance of our country and international standards of information security and network security technology and product standards developed, it shows that the process of our products have been into the standardization of information security. In this situation, the network information security monitoring system shows the necessity and practical significance in the network dynamic security protection. This paper describes the design and implementation of the network information security monitoring system in detail. Through the integration of information security monitoring and early warning and scheduling command platform construction, information security status can be timely grasp the global level, greatly improve the efficiency of information security incidents emergency disposal, is the senior information security guarantee system, establish and improve the implementation of ''active intelligent security protection, centralized and unified information control'' the concrete practice of the security policy.

Around the Internet of things environment big diameter data first scene of the network information security system of the third line, set up the network information security control mechanism model of triple dimensions from network control personnel, environment, technology to support each other, work together to build up the Internet of things environment under the background of big data combined with the mechanism of prevention and control of network information security system, for the Internet of things environment under the background of big data network information security work provides a theoretical guidance. Through the construction of network information security control model, and through the questionnaire about the way of empirical research, using structural equation model to verify the three elements of the network information security control effect of the network information security, and on this basis, through the methods of expert interview score, build up the Internet of things environment under the background of big data control network information security evaluation model, and the weight given by scientific computing evaluation system, to enhance the practicability of evaluation system, for the Internet of things environment under the background of big data network information security provides a practical guide.

REFERENCES

[1] S. Liu, L. Guo, H. Webb, X. Ya, and X. Chang, ''Internet of Things monitoring system of modern eco-agriculture based on cloud computing,'' *IEEE Access*, vol. 7, pp. 37050–37058, Mar. 2019.

[2] M. L. Han, J. Lee, and A. R. Kang, ''A statistical-based anomaly detection method for connected cars in Internet of Things environment,'' in *Proc. Int. Conf. Internet Vehicles*, vol. 9502, Nov. 2015, pp. 89–97.

[3] C. Yin, J. Xi, R. Sun, J. Xi, R. Sun, and J. Wang, ''Location privacy protection based on differential privacy strategy for big data in industrial Internet-of-Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 9–23, Nov. 2017.

[4] R. E. Samuel and D. Connolly, ''Internet Of Things-based health monitoring and management domain-specific architecture pattern,'' *Issues Inf. Syst.*, vol. 3, pp. 1345–1356, Dec. 2015.

[5] F. Zhang and Y. Zhang, ''A big data mining and blockchain-enabled security approach for agricultural based on Internet of Things,'' *Wireless Commun. Mobile Comput.*, vol. 2020, no. 1, pp. 21–28, Nov. 2020.

[6] T. Malche, P. Maheshwary, and R. Kumar, ''Environmental monitoring system for smart city based on secure Internet of Things (IoT) architecture,'' *Wireless Pers. Commun.*, vol. 107, no. 4, pp. 2143–2172, Apr. 2019.

[7] C. Shi, J. Fei, and X. Zhang, ''Continuous trust evaluation of power equipment and users based on risk measurement,'' *Sci. Program.*, vol. 2020, no. 4, pp. 2111–2116, Dec. 2020.

[8] L. Huang, X. Yuan, and J. Zhang, ''Research on Internet of Things technology and its application in building smart communities,'' *J. Phys. Conf. Ser.*, vol. 1550, no. 2, pp. 22029–22033, Mar. 2020.

[9] Y. Liu and S. Zhang, ''Information security and storage of Internet of Things based on block chains,'' *Future Gener. Comput. Syst.*, vol. 106, pp. 296–303, May 2020.

[10] J. Xiao, Y. Situ, and W. Yuan, ''Parameter identification method based on mixed-integer quadratic programming and edge computing in power Internet of Things,'' *Math. Problems Eng.*, vol. 2020, Sep. 2020, Art. no. 4053825.

[11] J. Chen and Q. Zhu, ''Interdependent strategic security risk management with bounded rationality in the Internet of Things,'' *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2911112–2911123, Nov. 2019.

[12] A. Ferdowsi and W. Saad, ''Deep learning for signal authentication and security in massive Internet of Things systems,'' *IEEE Trans. Commun.*, vol. 13, pp. 2878025–2878039, Feb. 2018.

[13] R. Ando, S. Shima, and T. Takemura, ''Analysis of privacy and security affecting the intention of use in personal data collection in an IoT environment,'' *IEICE Trans. Inf. Syst.*, vol. E99.D, no. 8, pp. 1974–1981, 2016.

[14] Q. Zhang, Y. Li, and R. Wang, ''Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things,'' *Int. J. Intell. Syst.*, vol. 36, no. 7, pp. 22293–22302, Oct. 2020.

[15] K. Gundars and S. Janet, ''Development of Internet of Things-related monitoring policies,'' *J. Inf. Privacy Secur.*, vol. 16, pp. 282–295, Jan. 2018.

[16] T. Fossati, ''This document defines a DTLS 1.2 profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.,'' *Int. J. Commun. Antenna Propag.*, vol. 5, no. 3, pp. 283–295, Dec. 2015.

[17] H. Yang, R. Zeng, F. Wang, G. Xu, and J. Zhang, ''An unsupervised learning-based network threat situation assessment model for Internet of Things,'' *Secur. Commun. Netw.*, vol. 2020, no. 9, pp. 1–11, Nov. 2020.

[18] Y. Li, Y. Tu, and J. Lu, ''Multi-point collaborative authentication method based on user image intelligent collection in the Internet of Things,'' *Electronics*, vol. 8, no. 9, pp. 978–989, Sep. 2019.

[19] H. Ma and Z. Zhang, ''A new private information encryption method in Internet of Things under cloud computing environment,'' *Wireless Commun. Mobile Comput.*, vol. 2020, no. 6, pp. 21–29, Sep. 2020.

[20] A. Ali and S. Alshmrany, ''Health monitoring and management system by using wireless sensor network and Internet of Things (IoT),'' *Int. J. Comput. Netw. Inf. Secur.*, vol. 19, no. 12, pp. 179–184, Dec. 2019.

[21] Y. Zhao and Y. Zhan, "Research on the application of value creation of big data in smart tourism," *Int. J. Emerg. Trends Social Sci.*, vol. 6, pp. 18–32, Jan. 2019.

[22] Y. Xiao and J. Dai, "Application and analysis on geological hazard monitoring and early warning system based on Internet of Things," *J. Phys. Conf. Ser.*, vol. 1601, no. 3, pp. 32015–32021, May 2020.

[23] H. Cheng, N. Wu, and J. Lian, "The management and monitor system of tunnel construction based on Internet of Things," *Lect. Notes Electr. Eng.*, vol. 334, pp. 1019–1026, Aug. 2015.

[24] X. Yi, "Framework analysis of privacy protection and information security enhancement model based on Internet of Things," *Int. J. Eng. Model.*, vol. 31, no. 1, pp. 302–308, Jan. 2018.

[25] X. Liu, T. Zhang, N. Hu, P. Zhang, and Y. Zhang, "The method of Internet of Things access and network communication based on MQTT," *Comput. Commun.*, vol. 153, pp. 169–176, Mar. 2020.

[26] F. Jamil, S. Ahmad, and N. Iqbal, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, pp. 2195–2204, Apr. 2020.

[27] P. R. Kumar, A. T. Wan, and W. S. H. Suhaili, "Exploring data security and privacy issues in Internet of Things based on five-layer architecture," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 1, pp. 108–121, Apr. 2020.

[28] A. Parlina, K. Ramli, and H. Murfi, "Theme mapping and bibliometrics analysis of one decade of big data research in the scopus database," *Information*, vol. 11, no. 2, pp. 69–82, Jan. 2020.

[29] A. Humeau-Heurtier, S.-Y. Lee, Y.-H. Liu, M. Milanova, and L. E. V. Silva, "Guest editorial special issue on cardiovascular system monitoring and therapy: Innovative technologies and Internet of Things," *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 4, pp. 725–728, Aug. 2018.

[30] L. Xie, Y. Ding, and H. Yang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 99, pp. 2913682–2913693, Apr. 2019.

[31] N. Liang, "Security transmission and storage of Internet of Things information based on blockchain," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 750, no. 1, pp. 12164–12170, Mar. 2020.

[32] T. G. Stavropoulos, G. Koutitas, D. Vrakas, E. Kontopoulos, and I. Vlahavas, "A smart University platform for building energy monitoring and savings," *J. Ambient Intell. Smart Environ.*, vol. 8, no. 3, pp. 301–323, Apr. 2016.

[33] I. Khoufi, P. Minet, and A. Laouiti, "Survey of deployment algorithms in wireless sensor networks: Coverage and connectivity issues and challenges," *Int. J. Autonomous Adapt. Commun. Syst.*, vol. 1, no. 4, pp. 341–390, Dec. 2017.

[34] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, Nov. 2018.

[35] D. S. Lavrova and Y. S. Vasil'ev, "An ontological model of the domain of applications for the Internet of Things in analyzing information security," *Autom. Control Comput. Sci.*, vol. 51, no. 8, pp. 817–823, Dec. 2017.

[36] P. Blazek, O. Krejcar, D. Jun, and K. Kuca, "Device security implementation model based on Internet of Things for a laboratory environment," *IFAC-PapersOnLine*, vol. 49, no. 25, pp. 419–424, 2016.

[37] Q. Zhang and D. Xu, "Security authentication technology based on dynamic Bayesian network in Internet of Things," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 573–580, Feb. 2020.

[38] S. F. Khan and M. Y. Ismail, "An investigation into the challenges and opportunities associated with the application of Internet of Things (IoT) in the agricultural sector—A review," *J. Comput. Sci.*, vol. 14, no. 2, pp. 132–143, Feb. 2018.

[39] S. Hong, S. Park, L. W. Park, M. Jeon, and H. Chang, "An analysis of security systems for electronic information for establishing secure Internet of Things environments: Focusing on research trends in the security field in South Korea," *Future Gener. Comput. Syst.*, vol. 82, pp. 769–782, May 2018.

[40] Y. A. Mendoza, T. J. L. Gomez, and M. A. L. Páez, "Risks and security solutions existing in the Internet of Things (IoT) in relation to big data," *Ingenierìa y Competitividad*, vol. 23, no. 1, p. e9484, Sep. 2020.

[41] S. Fatima, N. A. Aslam, and I. Tariq, "Home security and automation based on Internet of Things: A comprehensive review," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 899, pp. 12011–12023, Oct. 2020.

[42] M. Chen, S. Lu, and Q. Liu, "Uniqueness of weak solutions to a Keller-Segel-Navier-Stokes model with a logistic source," *Appl. Math.*, pp. 1–9, Feb. 2021, doi: 10.21136/AM.2021.0069-20.

[43] I. Ha, "Security and usability improvement on a digital door lock system based on Internet of Things," *Int. J. Secur. Its Appl.*, vol. 9, no. 8, pp. 45–54, Aug. 2015.

[44] W. Wang, Z. Gong, J. Ren, F. Xia, Z. Lv, and W. Wei, "Venue topic model–enhanced joint graph modelling for citation recommendation in scholarly big data," *ACM Trans. Asian Low-Resource Lang. Inf. Process.*, vol. 20, no. 1, pp. 1–15, Feb. 2021.

[45] W. Wei, M. Guizani, S. H. Ahmed, and C. Zhu, "Guest editorial: Special section on integration of big data and artificial intelligence for Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2562–2565, Apr. 2020.

[46] L. Cai, Y. Qi, W. Wei, J. Wu, and J. Li, "MrMoulder: A recommendation-based adaptive parameter tuning approach for big data processing platform," *Future Gener. Comput. Syst.*, vol. 93, pp. 570–582, Apr. 2019.

[47] H. Hu, B. Tang, X. Gong, W. Wei, and H. Wang, "Intelligent fault diagnosis of the high-speed train with big data based on deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 2106–2116, Aug. 2017.

[48] W. Wang, N. Kumar, J. Chen, Z. Gong, X. Kong, W. Wei, and H. Gao, "Realizing the potential of Internet of Things for smart tourism with 5G and AI," *IEEE Netw.*, vol. 34, no. 6, pp. 295–301, Nov. 2020.

[49] 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, Aug. 2015.

WUCHAO LIANG was born in Handan, China, in 1984. He received the bachelor's degree from the Shijiazhuang University of Economics, in 2008, and the master's and Ph.D. degrees from the Kunming University of Science and Technology, in 2009 and 2013, respectively. He currently works with the Hebei University of Engineering. He have been published home and abroad more than ten papers. His research interests include marketing management and strategic management.

WENNING LI was born in Hebei, China, in 1976. She received the bachelor's degree from Harbin Science and Technology University, in 1999, the master's degree from the Capital University of Economics and Business, in 2005, and the Ph.D. degree from Wonkwang University, South Korea, in 2020. From 1999 to 2002, she worked with the Shijiazhuang University of Economics. From 2005 to 2017, she worked as a Vice Professor with Hebei GEO University. She currently works with Hebei GEO University. She have been published home and abroad more than ten articles. Her research interests include accounting theory and practice, accounting informatization, financial risk, and early warning systems.

LILI FENG was born in Hebei, China, in 1977. She received the bachelor's and master's degrees from the Huazhong University of Science and Technology, in 2000 and 2005, respectively, and the Ph.D. degree from the Zhongnan University of Economics and Law, in 2013. From 2000 to 2002, she worked with Guangdong Fudi Company Ltd. From 2005 to 2010, she worked with the Shijiazhuang University of Economics. From 2013 to 2018, she worked as a Vice Professor with Hebei GEO University. Since 2018, she has been working as a Professor with Hebei GEO University. She have been published home and abroad more than ten articles, two of which has been indexed by SCI and SSCI. Her research interests include corporate governance and corporate social responsibility.