Hindawi
Mobile Information Systems
Volume 2022, Article ID 1195137, 12 pages
https://doi.org/10.1155/2022/1195137

*Research Article*

# Constructing a Security System for Classified Computer Information Using Distributed Parallel Computing

**Leng Wang[1] and Li Yang[2,3]**

[1]*Department of College of Information Engineering, Jilin Engineering Vocational College, Siping, Jilin 136000, China*
[2]*Department of College of Artificial Intelligence, Tangshan University, Tangshan, Hebei 063000, China*
[3]*Key Lab of Intelligent Equipment Digital Design and Process Simulation, Tangshan University, Tangshan, Hebei 063000, China*

Correspondence should be addressed to Li Yang; yangli@tsc.edu.cn

Received 4 April 2022; Revised 8 May 2022; Accepted 19 May 2022; Published 31 May 2022

Academic Editor: Mian Ahmad Jan



Information security can ensure an efficient application of classified computers. At present, in some classified computers, there exist problems and deficiencies in the field of information security management. It is not conducive to the control of information security. A network parallel computing system is a network-based system that has a high potential to resolve these issues. In recent years, with the development of cost-effective CPU and high-speed network technology, this system has gradually attracted the attention of people. Based on the research on distributed parallel computing, this paper abstractly analyzes the network parallel computing environment. It also discusses how a security protection system solution based on a distributed enterprise network environment helps rectify this problem. After research and analysis of classified computer information systems, this paper uses distributed parallel computing for building an advanced security system. Experimental results show that this method can improve the security status of the system to a much higher extent compared to the existing network security technologies. It has strong practicality and good social and economic value. The purpose of this paper is to provide information management tools for enterprises to improve the secrecy of management-level enterprises.

## 1. Introduction

In the contemporary information society, with the maturity of global information, the extensive establishment of large-scale distributed information systems, and the rapid development of social information applications, the application form of computers has gradually risen to the network form [1]. From the initial auxiliary tool, the role of the computer is increasingly dependent on economic, cultural, military, and social life [2]. At present, the application scope of computer networks in government departments, enterprises, and institutions is gradually expanding. A large number of information systems based on various network structures have emerged. However, the information involved is highly extensive [3]. With the construction and application of computer information systems, information security and confidentiality have increasingly become an important issue. It is also affecting the efficiency of informatization [4]. In the classified computer information system used to process and transmit state secret information, if the security and confidentiality are not well guarded, this will endanger the national security and interests. Additionally, due to the open architecture of the network, the security control system and network management mechanism have become weak and vulnerable to external attacks and unauthorized access. All kinds of computer information are exposed to such attacks. The security of computer systems has become one of the important issues that people pay attention to in the information age [5]. Information is an important strategic resource related to the national economy and livelihood of people. While classified computer information system has always been the key protection field of confidentiality work, we need to take comprehensive measures to ensure the stability and safety operation of classified

computer information systems [6]. At present, in network and distributed information systems, information security can no longer be considered from a single security function, security mechanism, and security range. It must be comprehensively and systematically studied from the architecture [7]. However, there is still a lack of a standardized theoretical system in the field of information system security architecture research and other issues of the security architecture that has not been systematically studied. It is conductive to ensure the overall security development and use of information systems.

Information in classified computers is always confidential. Once it is leaked, it will cause serious consequences. The computer network is the foundation of the information society. It has entered every corner of society [8]. With the development of computer networks, many government organizations have begun the use of classified computer information systems for their work, where the state confidential information will enter the computer classified information system. It is urgent to ensure the security of the computer information system [9]. In recent years, the security risks of classified computer information systems had emerged one after another. Technicians need to pay more attention to the security maintenance of classified computer information systems. Relevant personnel should pay attention to the management and control of information security in specific management fields. They must reasonably design the management system related to information security [10]. We should implement it in our daily work, give full play to the advantages of the information security management system, and provide certain basic guarantees for the information security of classified computers [11]. With the development of computer technology, parallel computing with distributed clusters composed of low-grade workstations or PCs connected by high-speed local area networks has gradually replaced the functions of some large parallel computers and taken the lead in the field of high-performance computing. Network parallel computing technology is a branch of distributed processing technology [12]. This technology is a network-based parallel computing technology. Based on distributed parallel computing, this paper proposes a security system for classified computer information systems. The innovations are as follows:

(1) This paper constructs the security systems of classified computer information system from the innovative perspective of "distributed parallel computing." It abstractly analyzes the network parallel computing. It gives an example of the task flow model of parallel computing. This model provides a powerful tool for understanding, analyzing, and evaluating an actual network parallel computing system.

(2) After combining the key contents of information security management of classified computers, this paper puts forward suggestions on the design and implementation of information security management systems and clarifies the technical measures and key points. Based on the intranet, this system realizes the automatic flow of confidential business processes, online registration, and approval of confidential business documents. At the same time, statistics and analysis are made on the process data generated by the confidential management business, as well as other various forms such as data and documents that are used to help confidential enterprises to carry out their confidential management. Information security of classified computers can be better maintained through the application of an information security management system.

This paper is arranged as follows: Firstly, this paper discusses the research background, the significance of centralized management, the control system of classified information security, and the development status of related technologies in Section 2. Section 3 presents the commonly used security application technologies, products and services, and a three-dimensional solution for the security of classified computer information systems based on distributed parallel computing. Moreover, Section 4 demonstrates the proposed methodology and results in this paper. It shows that the proposed system in this paper has a good performance that can improve the management level of enterprise secrecy and realize the standardization and information management of secrecy management. Finally, the paper is concluded in Section 5.

## 2. Related Work

The information security of confidential computers is an important part of the current confidential information security of enterprises and institutions. Once the hidden security risks of classified computer information systems are discovered, they may become the target of theft and piracy. Therefore, to maintain the security of computer information systems and ensure the safe operation of secret-related computer information systems, it is necessary to strengthen the research on the security maintenance of secret-related information systems. Ding et al. proposed the design purpose and work objectives of the information security management system for classified computers. They proposed design and implementation suggestions, aiming to provide certain support for related information security management and control [13]. Anand and Singh believe that the centralized management and control system for classified information security is a solution for the information security management of classified enterprises. It can strengthen the management of secret-related information, improve the management process, standardize the management of secret-related information, improve the level of security management of secret-related information, and reduce the occurrence of management loopholes and leaks [14]. Ramalingam et al. deeply analyzed the common requirements of various secret-related enterprises for the security management of secret-related information and made a general design of the software to form commercial

software products suitable for various enterprises [15]. Hodeish et al. constructed a complete, safe, reliable, and controllable confidentiality security protection system for classified information systems according to the needs of security protection requirements of classified information systems [16]. Van Horn et al. pointed out that computer firewall technology can effectively reduce the risk of information leakage. To effectively defend against computer viruses, firewall technology adopts various possible ways to reduce the risk of virus infection of confidential information systems [17]. Dewey and Shaffer fully analyzed the enterprise information security confidentiality management process and development model, as well as the demand for development tools in the process of confidentiality management combined with advanced development technology. They designed and implemented a centralized management and control system based on confidential information security [18]. Howser and McMillin regarded the network security of an enterprise as a systematic project and started from the theoretical exploration of enterprise network security. They proposed a design scheme of a step-by-step protection system based on the information security nervous system [19]. Tan et al. studied the security system framework of a certain computer network information system industry from two aspects of technical safeguard measures and management strategies. They formed an operational technology and management specification that is instructive for the security construction of a certain industry's computer network information system [20]. Akram et al. analyzed a large number of security management measures for classified computer information systems. They hoped to further ensure the security of classified computer information systems [21]. Ni et al. introduced the design goals and design principles of classified information systems. Based on the results of risk analysis, they formulated a security control plan [22]. Hamid et al. pointed out that the development of information security technology has evolved from the initial local security mode such as single-host security and network security to an overall security system that integrates a series of security modes such as host security, network security, and data security [23].

Based on the previous research on distributed parallel computing and the security of classified computer information systems, this paper innovatively combines all of them. It puts forward a method of constructing the security system of classified computer information systems based on distributed parallel computing. It also deeply analyzes the key technologies involved in the development of this system and the security management measures of classified computer information systems. The security risks of a classified information system are analyzed from the physical layer, network layer, and data link layer. According to the analysis results of security risks, three levels of security control measures are designed and implemented. They are preventive, detectable, and corrective. A complete set of security management mechanisms are designed and established, and advanced network security devices such as firewalls and intrusion detection systems are deployed in the implementation of security projects. To maximally eliminate the existing security risks and loopholes in classified information systems, the confidentiality, integrity, and availability of classified data and information in computer information systems can be reliably protected.

## 3. Methodology

This section presents the distributed parallel computing and construction of confidential computer information security system to carefully explain the proposed methodology that is used in this research. The explanation is as follows.

*3.1. Distributed Parallel Computing.* With the development of computer networks, parallel computing technology has gradually matured and has been widely used. It has become economical and mature to use parallel computing in various applications. This makes it possible to use distributed parallel computing in the security of classified computer information systems [24]. Network parallel computing needs a portable network computing environment. It enables the users to design programs on a common platform. However, the parallelism needs to be as transparent as possible to the users. Previously, in the field of parallel computing technology, the mainframe computer was the mainstay. Among them, CPU coupling is accomplished through the high-speed bus, while the network parallel computing connects working nodes through the network. CPU coupling is accomplished through network data transmission. It shows that the network parallel computing inherits the advantages of superior performance and stability of the mainframe central processing mode. At the same time, it absorbs the advantages of network and computer combination in distributed processing technology. Parallel computing technology replaces the expensive multi-CPU technology with cheap high-speed network communication technology along with high performance. Here, good scalability and flexibility are obtained. All these factors make the network parallel computing technology attract much attention in the field of high-performance computing.

In a distributed environment, each parallel part of application software runs on many different types of machines. They have different object code formats and may also use different debuggers. Each execution is also not repeatable. In the architecture of network parallel computing mode, there is a central management system similar to the mainframe. It forms a network parallel computing system [25]. It is responsible for dividing a program into multiple program segments. They are run on different working hosts, respectively. While obtaining high processing performance, all working hosts can also be managed in a unified way. The management system is connected with the working host and each working host is connected through the network. They communicate with each other through the network. Due to the parallel computing and management modal of the

central management system, the performance, computing efficiency, reliability, and resource utilization of the whole system are improved. Moreover, as all working hosts are interconnected by a network, the system has good scalability and strong flexibility. The performance-price ratio of the working host in this mode is far more attractive than a single CPU in a mainframe. At the same time, there is no limitation on the selection of the working host in this mode. This makes it highly portable. With the development of parallel computers, to improve the parallel granularity, the matrix block technology is currently adopted. Multiple columns of the matrix are operated simultaneously at a time. As a result, the parallel granularity is increased. This can also achieve healthy results. Suppose that

$$A = [A_0, A_1, \ldots, A_{n-1}]. \tag{1}$$

In the formula, $A_i$ is the $m \times \overline{m}$ array, where

$$m = \overline{m} \times n. \tag{2}$$

$A_i$ is stored in $P_{i \bmod p}$. The algorithm principle is

$$A = \begin{bmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{bmatrix} = \begin{bmatrix} L_{00} & 0 \\ L_{10} & I \end{bmatrix} \begin{bmatrix} U_{00} & U_{01} \\ 0 & U_{11} \end{bmatrix}. \tag{3}$$

When $A_0$ is partially decomposed, $L_{00}$, $L_{10}$, $U_{00}$ can be obtained at the same time. Based on this, the following can be calculated:

$$\begin{aligned} U_{01} &= L_{00}^{-1} A_{01}, \\ U_{11} &= A_{11} - L_{10} U_{01}. \end{aligned} \tag{4}$$

Mapping in parallel processing refers to the assignment of subtasks to parallel processes. In a parallel simulation, the whole simulation task is decomposed into a large number of logical processes. The assignment explains the mapping in parallel simulation [26]. There are many mapping strategies in the field of parallel computing. It can be divided into two categories: one type of strategy can get the optimal solution, and the other kind can get the approximate solution. Network parallel virtual machine refers to a series of CPU groups with memory that can provide users with computing power. Users do not need to know the characteristics of these nodes, such as hardware or operating system. These are transparent to users. The system shields the heterogeneity of the operating system and host hardware in the heterogeneous model. The parallel program adopts a node programming model. Program design should reduce communication as much as possible and increase the granularity of the algorithm to improve the efficiency of the parallel algorithm. The foundation of the whole computing environment is the underlying structure composed of the local area networks and operating system. Here, the one local area network can be composed of various current local area network technologies. To improve the performance of the network parallel computing system, high-speed LAN technology must be preferred [27]. To make the i860 processing chip play its due role, great attention should be paid to the use of library functions; otherwise, its calculation speed will become very low. The numerical calculation results made on Dawning 1000 use its efficient mathematical function library. It truly reflects the calculation speed. For regular problems such as matrix calculation, it is particularly important to use library functions. For parallel programs with regular interaction patterns, a kind of mapping method based on array allocation can effectively realize load balancing and minimize communication interaction between processes. The distributed computing platform is shown in Figure 1.

A heterogeneous application can be decomposed into multiple subtasks according to the calculation type and its run on different machines in the network. This involves the identification of code parallel types, the division and mapping of parallel tasks, and scheduling [28]. Ideally, a dynamic adaptive scheduling algorithm should be adopted to maintain the load balance of the system. Another entity in the network that parallels the virtual machine model is the virtual network. It is a general transmission medium for the users to provide data transmission services. Users do not need to care about the specific network implementation. It shields the heterogeneity of the network layer. These two entities constitute a network parallel virtual machine model. The configuration and management of a virtual machine is the first function that the parallel programming environment provides to the users [29]. The user only needs to specify the node name of the machine to join. The parallel programming environment automatically configures each node machine as a virtual machine. In this, the computer that the user started at the beginning is the master node and the rest are the slave node machines. The parallel programming environment registers the state information of all node machines in the virtual machine.

The operating system can be any multitasking operating system. It says that the underlying structure of the network parallel computing environment should be an application of various LAN technologies. The upper layer of the underlying structure is the network parallel computing system. It is the core of the whole computing environment. It endows the environment with parallel computing capability. The function of the system is to shield the related details of the underlying platform and provide parallel computing services to the user parallel programs at the upper level. In all parallel processing, data must be exchanged between the cooperative tasks. The messaging model has become an alternative example in terms of the number and types of multiprocessors that support it, as well as the applications, languages, and software systems that use it.

*3.2. Construction of Confidential Computer Information Security System.* Classified computer information system refers to the combination of equipment, technology, and management that use a computer, communication, network, and other technologies to collect, process, store, and transmit information related to state secrets and work secrets of the party and government organizations.

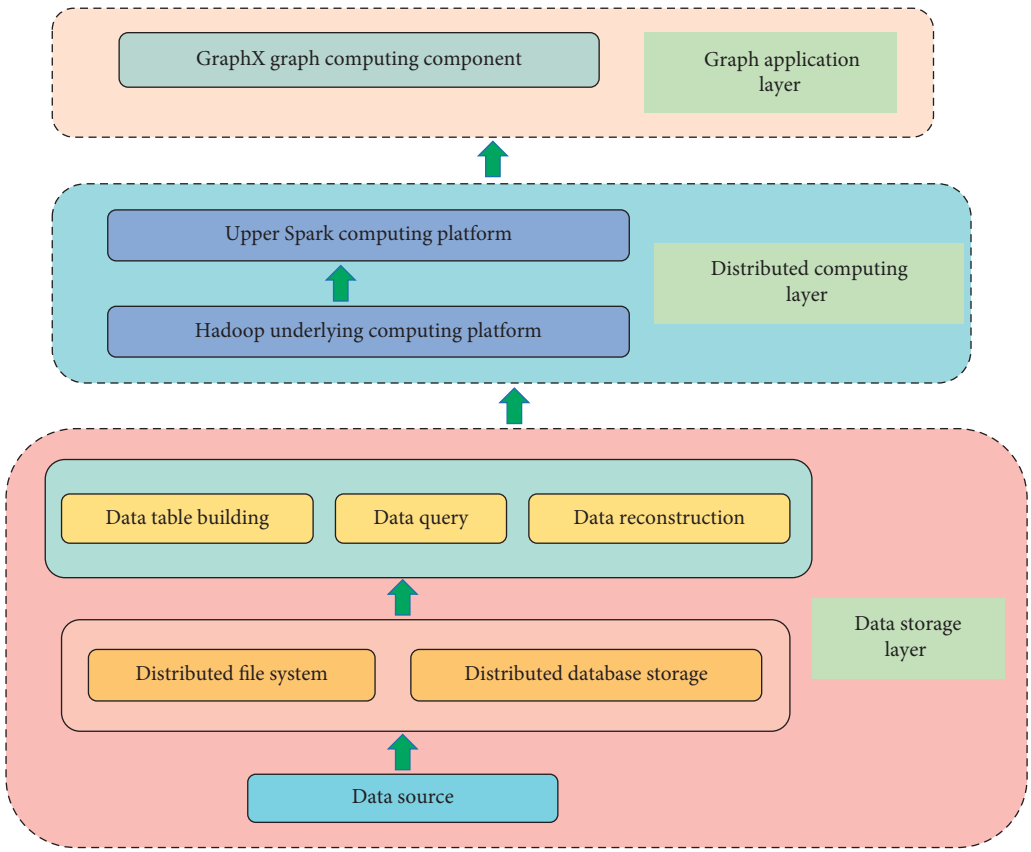


Figure 1: Distributed parallel computing platform.

Information security is to provide security protection for the transmission, storage, and access of the information in a distributed computing environment to prevent it from being stolen, tampered with, and illegally operated. The formulation of information security policies needs different types of information security policies according to the actual situation of each department in an organization. This provides management guidance and support for information security. To ensure the good application of security management system in information security protection of related classified computers, we should focus on designing relevant technical measures, integrating technical elements and means, and enhancing the security of various information and contents of classified computers with the help and support of advanced technologies [30]. The component-oriented and SOA- (Service Oriented Architecture-) integrated middleware technology has a reasonable hierarchical structure. It makes the system maintain good scalability. The application can be independently upgraded through the upgrade interface reserved by the system. The components can be quickly assembled according to the different needs of users. The main hardware configuration performance indicators of the system are shown in Table 1.

Generally, the understanding of computer information security is to ensure the confidentiality, integrity, controllability, availability, and nonrepudiation of information in the computer information system. The construction of an information security management system should be overall planned according to the guiding ideology of "standardizing confidentiality, quasi-determining level, according to standards, simultaneous construction, highlighting key points, ensuring core, clarifying responsibilities, and strengthening supervision." During the design of the management system, the confidentiality system and the actual situation should be interrelated. Relevant security management software should be designed in the terminal security system and user security system. The security management measures of the server should be used to improve the security of all information. According to the actual situation of enterprises, this software system needs to interact and integrate information with other existing application systems during normal operation. The main application systems include an information portal, log management, human resource management, fixed assets management, and domain server integration. The network security audit system is mainly used to monitor user activities from inside and outside the network, detect existing and potential threats in the system, identify, record, store, and analyze information related to security-related activities, and give an alarm and response to emergencies. The software architecture diagram is shown in Figure 2.

The network layer of a classified information system mainly provides logical channels for data exchange and transmission. The products involved include Layer 2 and Layer 3 switches. Considering the application cost and the

Table 1: Main hardware configuration performance indicators.

| Package | Physical equipment | Quantity | Operating system | RAM | CPU | Hard disc |
|---|---|---|---|---|---|---|
| Server | Dedicated server | 2 | Win Server 2010 | 16 G | 4 | ≥800 GB |
| Storage device | Dedicated storage device | 1 | — | — | 4 | 1 T |
| Intranet working machine | Ordinary business desktop | On-demand configuration | Windows 8 | 4 G | 2 | 128 G |

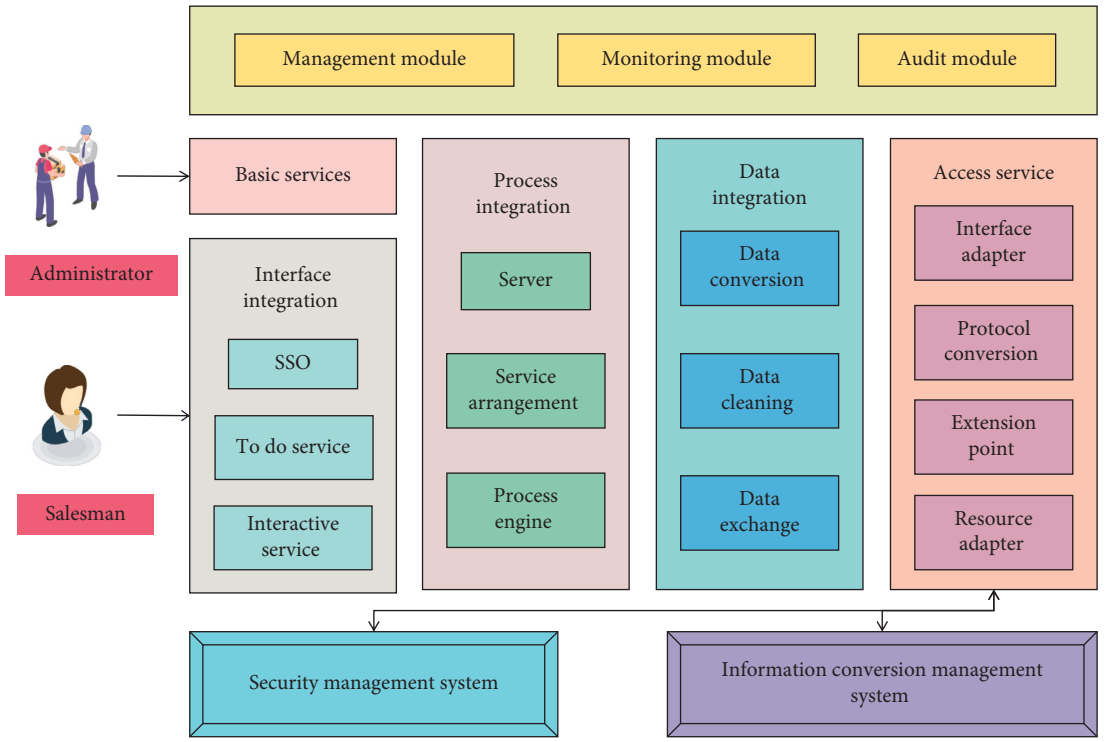


Figure 2: Software architecture diagram.

convenience of security management, distributed protection should be changed into centralized protection. Important classified databases and information system servers of various departments should be centrally placed in the data center computer room. In addition, large-scale UPS equipment and a special air conditioner for the precision machine room must be installed in the machine room to control the temperature and humidity of the power supply and environment. The security management department of the information system shall, according to the management principle and the confidentiality of the data processed by the system, formulate a corresponding management system, use a video jammer for display, use an antielectromagnetic leakage power socket for power access, and use shielded twisted pair or optical fiber for data lines to prevent electromagnetic leakage. Lock or affix a seal on the equipment to prevent unauthorized assembly and disassembly of the equipment. Any disassembly and assembly of the equipment must be applied for approval. It shall be executed by a special person, and the application record and operation record shall be maintained and kept.

The terminal security management system fixed network settings and port shielding. For illegal outreach, the terminal security management system links with the network switch to search for illegal users in real time. Once it is detected that the client without terminal security management software is trying to connect to the network, it blocks the illegal access to the machine on the switch port. As the carrier of data transmission, the security of the network layer is an important link to ensure the security of classified information. A large number of security incidents are implemented by penetrating the network layer. In order to reduce the risk of external penetration of the classified network and meet the requirements of the state for the construction of the classified network, it is physically isolated from the external network to ensure the security of the classified information system. In this design, it is planned to use the tape drive to periodically carry out an offline backup of the system. Hot backup refers to an "online" backup in which the downloaded backup data is still in the whole computer system and network. It is only transferred to a nonworking partition or another non-real-time processing business system for storage.

The forward operator represents the influence of the previous state at time $t$, and its derivation can be divided into two parts: initialization and iteration. Initially calculate the forward operator value of the first time slice ($t = 1$), and the iterative process provides a general delivery method of the operator. The forward operator initializes ($t = 1$):

$$\alpha_1(c) = P(X_1 = c|Y_1) = \frac{P(X_1 = c, Y_1)}{P(Y_1)} = \frac{P(X_1 = c_1) \cdot P(Y_1|X_1 = c)}{\sum_{d=1}^{v} P(X_1 = d) \cdot P(Y_1|X_1 = d)}$$
$$= \eta_1^{\alpha} \cdot P(X_1 = c) \cdot \prod_{Y}^{W,H,HD,CD} \left( \sum_{k \infty Y} P\left(Y_1 = y^k | X_1 = c\right) \cdot E\left(Y_1 = y_1^k\right) \right). \tag{5}$$

In the above formula, $\eta_1^{\alpha}$ is the value of the normalization factor $\eta_t^{\alpha}$ of the forward operator at $t = 1$, as shown in the following formula:

$$\eta_1^{\alpha} = \frac{1}{\sum_{d=1}^{v} P(X_1 = d) \cdot \prod_{Y}^{W,H,HD,CD} \left( \sum_{k \infty Y} P\left(Y_1 = y^k | X_1 = d\right) \cdot E\left(Y_1 = y_1^k\right) \right)}. \tag{6}$$

$$\eta_t^{\alpha} = \frac{1}{\sum_{d=1}^{v} P(X_t = d) \cdot \prod_{Y}^{W,H,HD,CD} \left( \sum_{k \infty Y} P\left(Y_t = y^k | X_t = d\right) \cdot E\left(Y_t = y_t^k\right) \right)}. \tag{7}$$

Similarly, $\eta_t^{\alpha}$ is only related to time $t$. It has nothing to do with the state of the load node at this time. The sum of the probabilities in each state is 1. Therefore, no calculation is required in the actual derivation. It is used as a probability normalization.

To truly realize intranet security, we must reduce the security domain to every network terminal. Firewalls are used to realize fine-grained access control and intrusion prevention on each terminal. Firewalls are set up in important server areas and are used to complete access control of the application layer, shield unnecessary access areas and ports, and increase the security access control ability of key areas. The distributed firewall is responsible for the security protection between network boundaries, subnets, and nodes within the network. It is purely a complete system. On the core switch, the data packets forwarded by each port are mirrored to the intrusion detection system. The intrusion detection and firewall equipment are linked together to produce the effect of automatically blocking the identified attacks and blocking them in real time, resultantly realizing the detection of hacker attacks in each network segment and blocking attacks in important server areas in time. The main feature of the cloth firewall is that it adopts the host resident mode. One of its important components is called the "host firewall." The important feature of the host firewall is that it resides on the protected host. The network outside the host is untrusted whether it is inside or outside the enterprise network. Therefore, a highly targeted security policy can be set for specific applications running on this host and services provided to the outside world. Relative error, root mean square error, and average absolute percentage error are selected as the basis for judging the algorithm effect. The formula is as follows:

$$RE = \frac{|P_i - P_i|}{P_i},$$
$$\text{MAPE} = \frac{\left[\sum_{i=1}^{N} \left(|P_i - P_i|/P_i\right)\right]}{N} \times 100\%, \tag{8}$$
$$\text{RMSE} = \sqrt{\frac{1}{N} \sum_{i=1}^{N} \left|\frac{P_i - P_i}{P_i}\right|^2}$$

For the virus protection of the local area network, we should deploy the network version virus protection system under centralized control. The virus killing strategy is uniformly set on the server, and antivirus software and system patches are automatically and regularly updated on each client through the server to achieve the best protection effect. After completing the security management system of classified computer information, to ensure that the related security management purposes can be achieved at work, the comprehensive ability of system application should be emphasized. The system manages the classified information, carriers, and equipment through user and authority verification, process approval, information flow encryption, closed-loop management of classified information from generation to filing, secret vector, equipment borrowing and returning management, and centralized information processing and control.

## 4. Result Analysis and Discussion

According to the test requirements of the configuration items, it is necessary to check the compatibility of design documents, static analysis of program code, and code walkthrough. The system performance index might meet the

design requirements, an inspection of internal and external interfaces, interface friendliness, system security, and logic rationality. According to the demand for data recovery, this paper realizes the online secondary backup strategy of sensitive data, a full backup of data every Sunday, and incremental backup of data every Monday to Saturday. This not only ensures data security but also reduces the backup load of data. According to the requirements of confidentiality management, the rules and regulations are established, and the system provides information entry management functions of legal representative responsibility, leadership responsibility in charge of confidentiality, project leader responsibility, and confidential personnel responsibility. It also includes the addition, deletion, and modification of responsibilities. The contents of responsibilities include responsibility category, responsibility description, activity record, registration time, registrant, and other information. The system environment is shown in Table 2.

The viewpoint in the field of information security is that the highest level of security is not about the products or services but the overall management. Without effective management ideas, a strict management system, responsible managers, and well-implemented management procedures, there is no real information security. Confidentiality management is the core business of information security management. It is responsible for the overall management of classified items of enterprises, classified personnel, secret vector, and information equipment. This includes classified management of scientific research items, information management of classified personnel, and account management of information equipment dealing with classified items. The encryption technology of computer systems mainly ensures the security of information system data. By setting a certain security secret key for data information, the security and accuracy of data can be protected. This is to ensure further guarantee for the security of computer system. At the same time, the overall management of enterprise classified personnel is carried out. It includes the application of classified personnel, confidentiality education, and training, as well as carrying classified information for office control. Training employees for safety awareness and improving their protection ability are one of the important foundations for building a network security system for the organization. When overall security awareness of the employees is improved, intrusion attacks can be effectively reduced. It is also more conducive to the smooth realization of the network security system. To verify the performance of this algorithm, we compare it with the algorithms in [16, 18]. The root mean square errors of the three algorithms are shown in Figure 3. The average absolute percentage errors are shown in Figure 4.

According to Figures 3 and 4, the error of this algorithm is lower and the accuracy is higher compared to the other two algorithms. From this experiment, it is concluded that the algorithm in this paper has a certain accuracy.

When the confidential personnel, carrying information and the equipment, leave the office, they must fill out the application for carrying confidential information first. After being approved by the department head and the business leader in charge, the information equipment management personnel will remove the relevant protection for the information equipment in accordance with the application. The core problem of security incident handling is to eliminate the current threats. It mainly refers to eliminating the causes of security incidents. If the security incident is a computer virus, antivirus software is used to eliminate it. When the hardware such as the hard disk of the classified computer is disassembled or the operating system and software installed on the classified computer are upgraded, updated, or scrapped and depreciated, the classified computer must be treated by security technology. Close the distributed security management to centralization, protect the whole security domain hierarchically, and divide the important server areas with fine granularity. Multilayer division of the security domain not only meets the work requirements but also highlights the key points, saves the investment of manpower and material resources, and fully reflects efficiency and rationality. We do the test again, and the comparison of the recall rates of the algorithms is shown in Figure 5.

The security policy of the core of the system, the formulation of the management system, the network construction, and the deployment of security products are the main dynamic process. The level of each part is also in a dynamic cycle. This process of continuous circulation can effectively discover the current security problems of the organization and revise the parts that do not meet the requirements of the organization after evaluation. In this way, the revised contents at each level can better meet the security requirements of the organization. Network intrusion detection system uses bypass monitoring to analyze and monitor data packets flowing through the network. The deployment of an intrusion detection system will not affect the network performance. However, the premise of its effective work is to ensure that the intrusion detection system can capture all data packets of the monitored network. It is embodied in the configuration of the switch monitoring port in an enterprise network. To verify the reliability of the system in this paper, we tested the safety of the system in Literature [16], Literature [18], and this system, respectively, and obtained the results as shown in Figure 6.

The security handling process of the system for handling events needs tools, services, and specialized processes. These processes include copying, monitoring, tracking, alarm, notification, dialogue, elimination, recovery, and other processes. In daily work, strengthening attack, defense drills, and the emergency plan for attack and defense drills must include superior plan, organization, monitoring, early warning, graded response, information management, investigation, and evaluation. If a secret-related incident is found, the safety construction and rectification should be strengthened in time. In the process of handling system security incidents, including all personnel encountering security incidents, they should first report the corresponding incidents to the security center or system manager at the corresponding administrative level for handling. The corresponding specialized technicians shall resolve the problem or submit the problem to the higher-level security center for

Table 2: System software environment.

| Kind | Operating system | Use |
|---|---|---|
| Runtime environment | Windows 2010 Server | Web server operating system |
| | Windows 10 | Intranet client operating system |
| | Firefox, Google Chrome | Intranet client application environment |
| | Oracle 11.2 G | Database management system |
| | Microsoft Office 2019 | Document editing software |
| Exploitation environment | Microsoft Visual Studio.NET 2010 | Application development tools |
| | Microsoft Office 2010 | Document editing software |

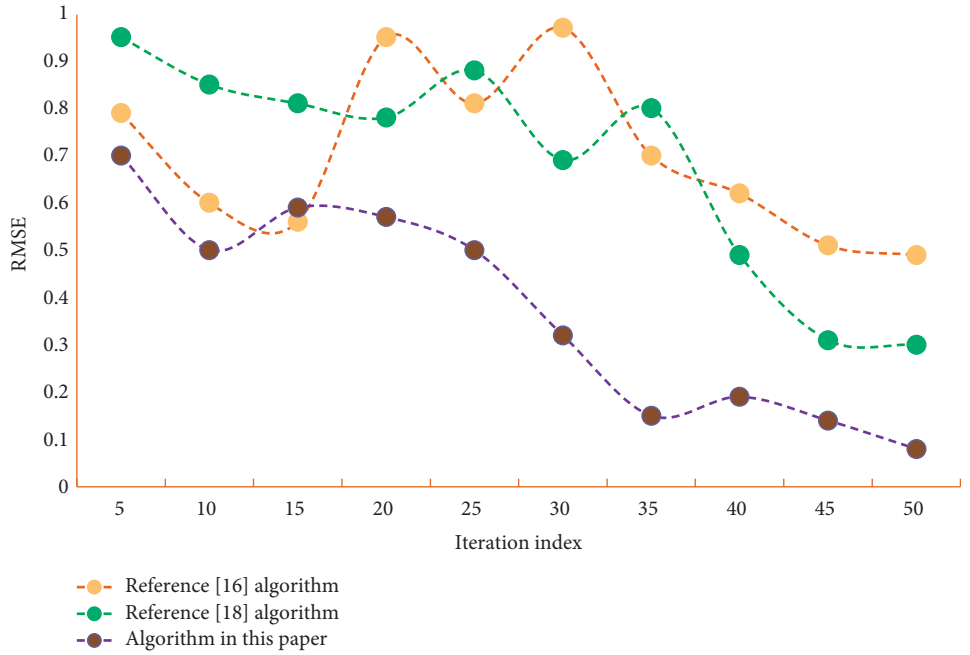


Figure 3: Comparison of root mean square errors of algorithms.

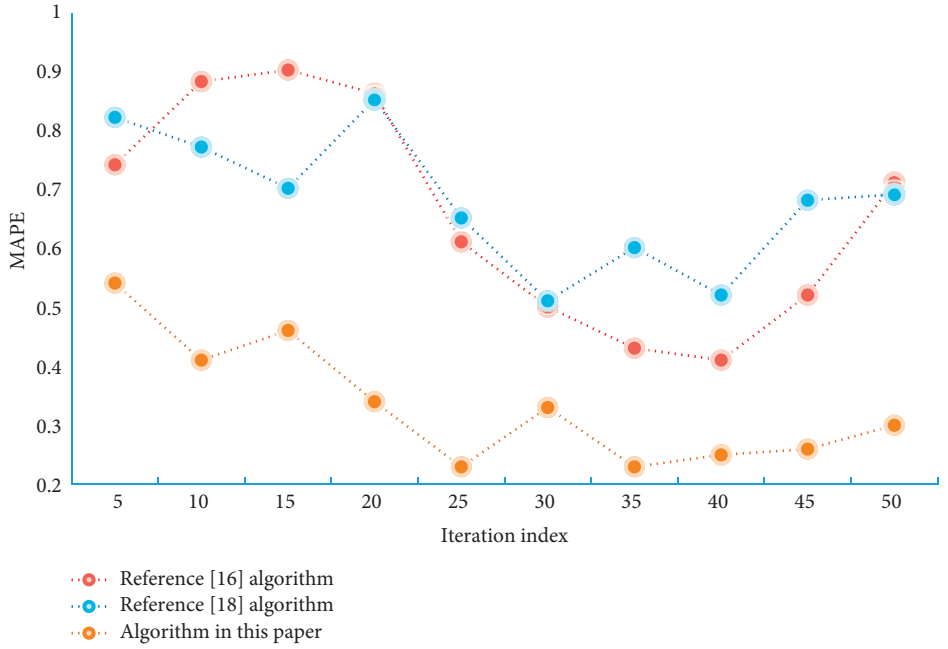


Figure 4: Comparison of average absolute percentage errors of algorithms.

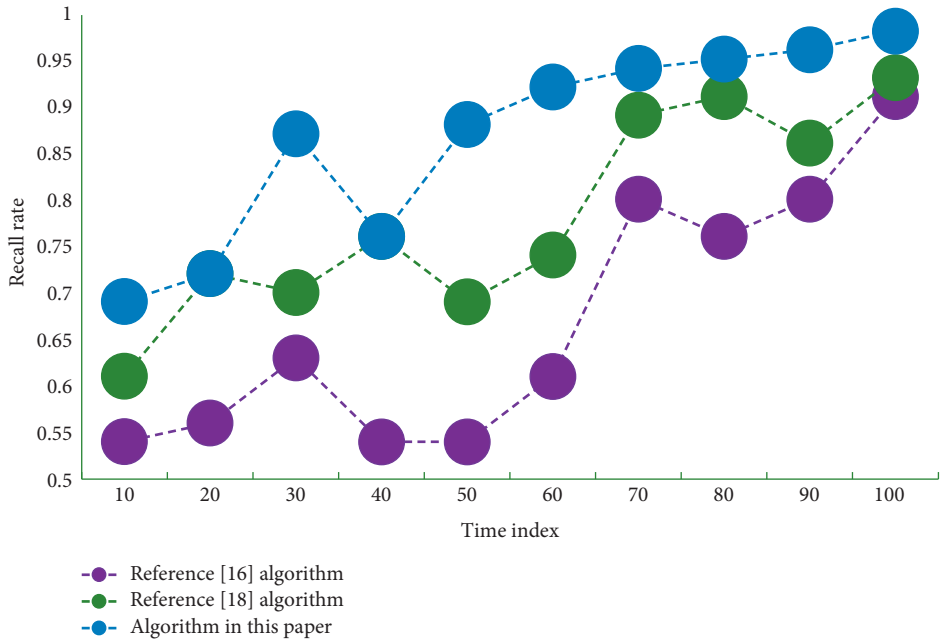


Figure 5: Comparison of recall rates of algorithms.

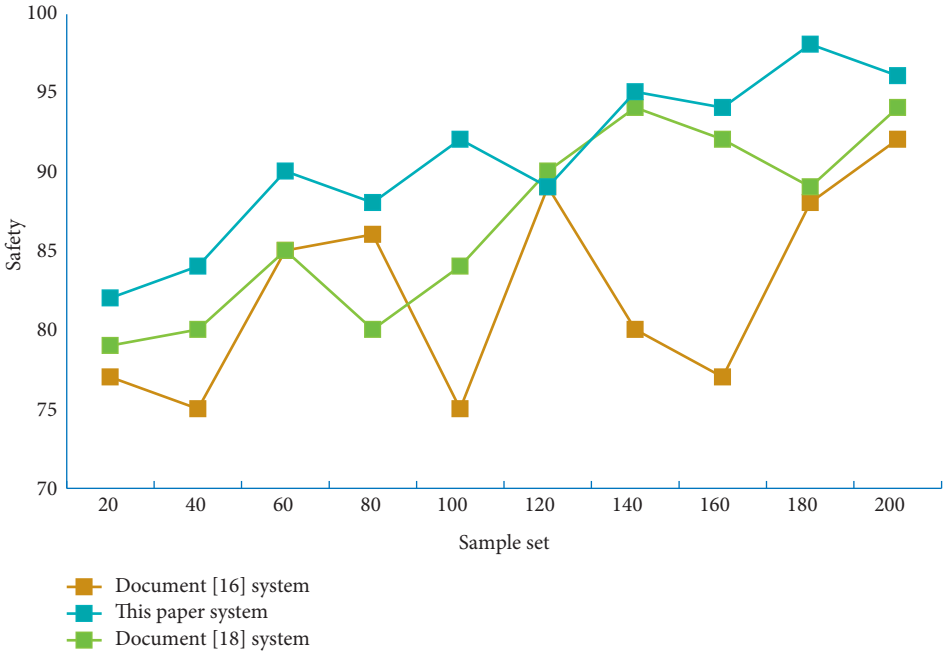


Figure 6: Security test of the system.

handling. Again, the stability tests of different systems are carried out, and the obtained results are drawn into the data chart as shown in Figure 7.

From the test results of the system security and stability, it can be noticed that the system in this paper has high security and stability. It can be applied to the security work of classified computers and has certain practical value.

In the process of actual operation and management, complete security control of the whole classified information system is applied. When dealing with a certain level of security risks, it is possible to implement multiple levels of security control measures. However, at this level, it is impossible to realize the overall security of the classified information system only by limiting the security control measures. The centralized management and control system of confidential information security takes the security and confidentiality management of computers and information systems as the core and the technical requirements of classified protection as the system framework. It meets a series of requirements and standards and deepens

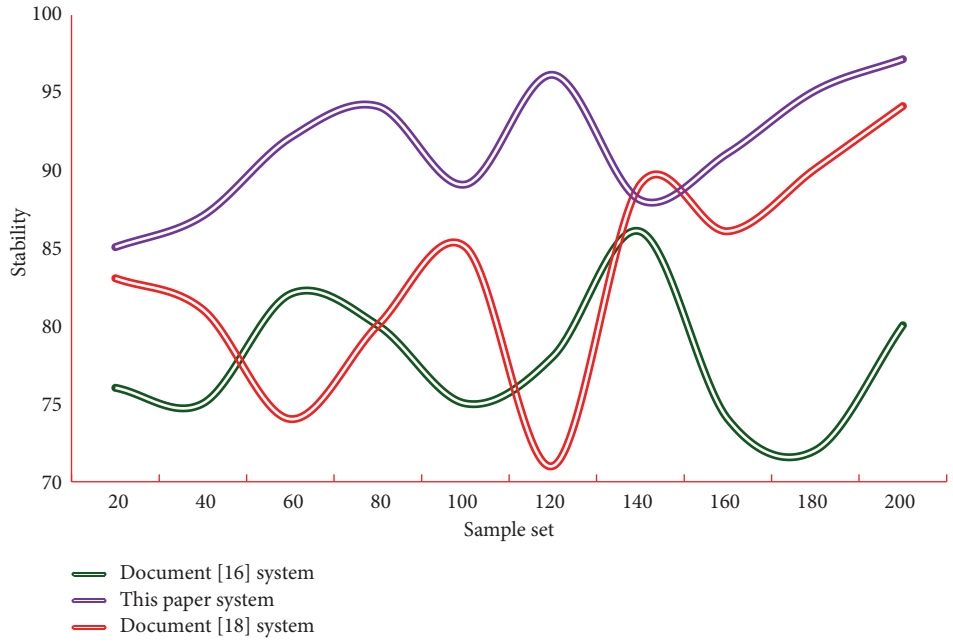


Figure 7: Stability test of the proposed system.

management. It also realizes the registration and approval of confidential business processes and can control the whole process of confidential information conversion and circulation. Adopt the linkage protection working mode, reasonably design the protection system with continuous characteristics, and ensure the linkage of protection work.

This system closely focuses on the work of project confidentiality, confidential personnel, carrier and equipment information management, and confidential information conversion. It also provides practical and confidential information security centralized management tools that meet the confidentiality management regulations. This paper experimentally shows that the security control scheme of classified information systems comprehensively improves the security coefficient of classified computer information, the security test, recovery test, and installation test of the system. It provides a safe and efficient guarantee environment for the in-depth development of business.

## 5. Conclusions

Information security management of classified computers is very important. The technology of contemporary classified computer information systems is in the process of continuous development. Although the classified information system will face great challenges, the maintenance of classified information is of great significance to security. We must pay close attention to the development of security technology and take necessary technical measures for security. In this paper, the related problems of the security system construction of classified computer information systems based on distributed parallel computing are discussed. They are combined with the actual situation of enterprise classified information security management, the system analysis, and design detail. This method can not only ensure information security at all levels but also consider information security. Resultantly, it forms a set of perfect information security management methods. It minimizes the security risks of classified information systems and ensures the security, confidentiality, integrity, availability, and accuracy of sensitive data and information. Part of the experimental test results shows that the functions are consistent with the requirements, and all the functional requirements are fulfilled. Therefore, the system meets the needs of users and achieves the goal of design and development. This system has realized the simplification and standardization of management of confidentiality and improved its management level. However, the hidden dangers of classified computer information security, its prevention, and its solution are long-term and important issues. The relevant departments need to continuously increase the investment level of classified information security maintenance. To actively prevent the leakage of classified information systems and maintain the security of information systems, more measures should be taken to maintain the security of classified computer information systems in China. It is hoped that the research in this paper can further improve the efficiency and security of the confidentiality management business and make some contribution to the development of confidentiality.

## Data Availability

All the data about this research are included for publication of this work.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References


[1] K. A. Salleh and L. Janczewski, "Technological, organizational and environmental security and privacy issues of big data: a literature review," *Procedia Computer Science*, vol. 100, pp. 19–28, 2016.

[2] S. Khandare and U. Shrawankar, "Image bit depth plane digital watermarking for secured classified image data transmission," *Procedia Computer Science*, vol. 78, pp. 698–705, 2016.

[3] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Generation Computer Systems*, vol. 89, pp. 110–125, 2018.

[4] H. Hu, Z. Wang, G. Cheng, and J. Wu, "MNOS: a mimic network operating system for software defined networks," *IET Information Security*, vol. 11, no. 6, pp. 345–355, 2017.

[5] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[6] A. A. Dhumal and S. Jadhav, "Confidentiality-conserving multi-keyword ranked search above encrypted cloud data," *Procedia Computer Science*, vol. 79, pp. 845–851, 2016.

[7] W. Zellinger, V. Wieser, M. Kumar et al., "Beyond federated learning: on confidentiality-critical machine learning applications in industry," *Procedia Computer Science*, vol. 180, pp. 734–743, 2021.

[8] M. Guerine, M. B. Stockinger, I. Rosseti et al., "A provenance-based heuristic for preserving results confidentiality in cloud-based scientific workflows," *Future Generation Computer Systems*, vol. 97, pp. 697–713, 2019.

[9] Q. N. Natsheh, B. Li, and A. G. Gale, "Security of multi-frame DICOM images using XOR encryption approach," *Procedia Computer Science*, vol. 90, pp. 175–181, 2016.

[10] K. Mivule, "Data swapping for private Information Sharing of Web search logs," *Procedia Computer Science*, vol. 114, pp. 149–158, 2017.

[11] J. R. Vacca, *Computer and Information Security Handbook*, Newnes, London, UK, 2012.

[12] A. Boiko and V. Shendryk, "System integration and security of information systems," *Procedia Computer Science*, vol. 104, pp. 35–42, 2017.

[13] L. Ding, Z. Wang, X. Wang, and D. Wu, "Security information transmission algorithms for IoT based on cloud computing," *Computer Communications*, vol. 155, pp. 32–39, 2020.

[14] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, 2020.

[15] D. Ramalingam, S. Arun, and N. Anbazhagan, "A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM," *Procedia Computer Science*, vol. 134, pp. 365–370, 2018.

[16] M. E. Hodeish, L. Bukauskas, and V. T. Humbe, "An optimal (k,n) visual secret sharing scheme for information security," *Procedia Computer Science*, vol. 93, pp. 760–767, 2016.

[17] K. E. Van Horn, A. D. Dominguez-Garcia, and P. W. Sauer, "Measurement-based real-time security-constrained economic dispatch," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3548–3560, 2015.

[18] C. M. Dewey and C. Shaffer, "Advances in information security education," in *Proceedings of the 2016 IEEE International Conference on Electro Information Technology (EIT)*, pp. 0133–0138, IEEE, Forks, ND, USA, May 2016.

[19] G. Howser and B. McMillin, "Using information-flow methods to analyze the security of cyber-physical systems," *Computer*, vol. 50, no. 4, pp. 17–26, 2017.

[20] S. Tan, X. Li, and Q. Dong, "TrustR: an integrated router security framework for protecting computer networks," *IEEE Communications Letters*, vol. 20, no. 2, pp. 376–379, 2015.

[21] R. N. Akram, H. H. Chen, J. Lopez, D. Sauveron, and L. T. Yang, "Security, privacy and trust of user-centric solutions," *Future Generation Computer Systems*, vol. 80, pp. 417–420, 2018.

[22] Z. Ni, Q. Li, and G. Liu, "Game-model-based network security risk control," *Computer*, vol. 51, no. 4, pp. 28–38, 2018.

[23] M. A. Hamid, M. Abdullah-Al-Wadud, M. M. Hassan et al., "A key distribution scheme for secure communication in acoustic sensor networks," *Future Generation Computer Systems*, vol. 86, pp. 1209–1217, 2018.

[24] C. Zuo, "Defense of computer network viruses based on data mining technology," *International Journal on Network Security*, vol. 20, no. 4, pp. 805–810, 2018.

[25] D. Grzonka, A. Jakóbik, J. Kołodziej, and S. Pllana, "Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security," *Future Generation Computer Systems*, vol. 86, pp. 1106–1117, 2018.

[26] M. Zineddine, "Optimizing security and quality of service in a real-time operating system using multi-objective Bat algorithm," *Future Generation Computer Systems*, vol. 87, pp. 102–114, 2018.

[27] C. G. García, D. Meana-Llorián, B. C. P. G-Bustelo, J. M. C. Lovelle, and N. Garcia-Fernandez, "Midgar: detection of people through computer vision in the internet of things scenarios to improve the security in smart cities, smart towns, and smart homes," *Future Generation Computer Systems*, vol. 76, pp. 301–313, 2017.

[28] B. G. Batista, C. H. G. Ferreira, D. C. M. Segura, D. M. Leite Filho, and M. L. M. Peixoto, "A QoS-driven approach for cloud computing addressing attributes of performance and security," *Future Generation Computer Systems*, vol. 68, pp. 260–274, 2017.

[29] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology," *Procedia Computer Science*, vol. 183, pp. 4–13, 2021.

[30] G. Levitin, L. Xing, and Y. Dai, "Optimal data partitioning in cloud computing system with random server assignment," *Future Generation Computer Systems*, vol. 70, pp. 17–25, 2017.