Hindawi
Advances in Multimedia
Volume 2023, Article ID 9793158, 1 page
https://doi.org/10.1155/2023/9793158

Retraction

Retracted: Computer Multimedia Security Protection System Based on the Network Security Active Defense Model

Advances in Multimedia

Received 15 August 2023; Accepted 15 August 2023; Published 16 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Shang and J. Zhang, "Computer Multimedia Security Protection System Based on the Network Security Active Defense Model," *Advances in Multimedia*, vol. 2021, Article ID 8792105, 9 pages, 2021.

Hindawi
Advances in Multimedia
Volume 2021, Article ID 8792105, 9 pages
https://doi.org/10.1155/2021/8792105

Research Article

Computer Multimedia Security Protection System Based on the Network Security Active Defense Model

Yanhong Shang[1] and Jing Zhang[2]

[1]*Computer Science Department of Tangshan Normal University, Tangshan, Hebei 063000, China*
[2]*Dean's Office of TangShan Normal University, TangShan, HeBei 063000, China*

Correspondence should be addressed to Jing Zhang; 2016120252@jou.edu.cn

Received 6 August 2021; Accepted 8 November 2021; Published 13 December 2021

Academic Editor: Zhendong Mu

In response to the continuous development of computer science and multimedia technology, many problems related to computer multimedia security are gradually exposed in the development. Through the existence of hidden dangers of computer multimedia security, a computer is constructed based on the network security active defense model. For a multimedia security protection system, select four modules in the system for design and description. Finally, the experimental results show that the system designed in this study can realize the security protection of computer multimedia, and the system is simple to operate and has strong practicability and meets the expected design effect.

1. Introduction

With the continuous development of computer science and multimedia technology, it has also brought many problems to network security. There have been many network security incidents in different fields at home and abroad. The hidden dangers of computer multimedia security can be summarized into three main areas: computer system and its own security problems, security risks caused by external network attacks, and problems caused by computer system updates, upgrades, and routine maintenance and management [1–3]. Regardless of the type of security hazard, it is necessary to meet the rapidly growing development needs of computer multimedia technology in accordance with computer basic hardware equipment, daily maintenance and management, and related system software upgrades [4]. In the computer operation process because of the system security aspects, the existence of defects makes the computer's entire operating system or data use and sharing process security, confidentiality, integrity, and detection mechanisms have huge security risks. Therefore, the design of the computer multimedia security protection system is very important. Through the development and design of a security protection system that matches the current computer and multimedia technology, the security performance of the computer system can be better improved, and the integrity, confidentiality, and availability of the system and its data application process data can be ensured for better good use.

Computer multimedia security system (CMESS), as an effective and important means of existing network security monitoring, can greatly improve network operation security management and control and network active defense capabilities. Based on the existing network security active defense model, this study fully analyzes the needs of computer multimedia information networks and proposes a computer multimedia security protection system based on

the network security active defense model, which can be followed by the security monitoring and management of computer multimedia information networks.

2. Computer Multimedia Security System Architecture and Defense Model

In daily work and life, computer multimedia security risks are everywhere, mainly including natural factors such as damage to computer connection lines due to changes in the external natural environment, resulting in information loss; hacker attacks such as network hackers steal business secrets to make a living, it poses a huge challenge to the safety of computer multimedia, and in extreme cases, it can also cause loss and destruction of information and data; and computer viruses such as network viruses cause hardware crashes and file damages through system transmission, and in severe cases, computer systems paralyzed and so on. Although people have taken certain measures to enhance security protection during computer use, such as enhancing computer multimedia security awareness, configuring antivirus software for regular detection, network monitoring to suppress virus intrusion, establishing firewalls, and using encryption technology, computer multimedia security protection involves multiple factors, including natural factors and human factors [5–7]. Therefore, we still need to carry out effective computer multimedia security protection system development and practical application. The architecture design of the computer multimedia security protection system mainly includes the application layer, the core layer, and the hardware layer. The system architecture diagram is shown in Figure 1. The framework consists of the application layer, the core layer, and the hardware layer from top to bottom. Each layer has a corresponding composition. Module: Among them, the application layer includes 4 modules such as login permission verification, the core layer includes 5 modules such as dongle verification, and the hardware layer includes 3 modules such as mobile media. In the actual application process, each module performs its own function. There are also strict intervention guidelines. If any module in the architecture system does not meet the requirements for use, it is not allowed to use and intervene. This can effectively avoid the failure of the protection of the overall module due to a failure of a link.

Definition 1. Given F: $R_n \longrightarrow R$, there exists an n-dimensional weight vector related to F, $w_i \in [0,1], 1 \le i \le n$, and $\sum_{i=1}^{n} w_i = 1$, so that

$$F(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} w_i b_i, \tag{1}$$

where b_i is the i^{th} largest factor $(a_1, a_2, \ldots, a_n)$ of the array. Then, F is called the n-dimensional network security active defense model analysis.

The network security active defense model analysis is an analysis between the maximum analysis and the minimum analysis.

When $w = (1, 0, 0, \ldots, 0)$,

$$F(a_1, a_2, \ldots, a_n) = \max(a_1, a_2, \ldots, a_n) = b_1. \tag{2}$$

In the active defense analysis calculation, the network security active defense model analysis is equivalent to the "or" analysis.

When $w = (0, 0, 0, \ldots, 1)$,

$$F(a_1, a_2, \ldots, a_n) = \max(a_1, a_2, \ldots, a_n) = b_n. \tag{3}$$

The analysis of the network security active defense model is equivalent to the "and" analysis in the active defense analysis.

When $w = (1/n, 1/n, 1/n, \ldots, 1/n)$,

$$F(a_1, a_2, \ldots, a_n) = \frac{1}{n}\sum_{i=1}^{n} a_i. \tag{4}$$

The network security active defense model analysis is equivalent to the arithmetic average analysis.

The identification of the weight vector analyzed by the network security active defense model is directly related to the size of the dataset. In order to ensure the fairness and rationality of the evaluation results, this study discretized the Gaussian distribution to clarify the weight vector of the position. In this method, the degree of freedom value is placed in a position with a relatively small weight value, which effectively eliminates the adverse effect of emotional factors on the evaluation process.

The set μ is the mathematical expectation of $w = (1/n, 1/n, \ldots, 1/n)$ assigned to the weight vector $(1, 2, \ldots, n)$; σ is the standard deviation of $(1, 2, \ldots, n)$ in the μ and the weight vector w, so we have

$$\begin{aligned} \mu_n &= \frac{1}{n}\frac{n(n+1)}{2} = \frac{n+1}{2}, \\ \sigma_n &= \sqrt{\frac{1}{n}\sum_{i=1}^{n}(i-\mu_n)^2}, \\ \omega' &= \frac{1}{\sqrt{2\pi\sigma_n}} e^{-(i-\mu_n)^2/2\sigma_n^2}, \\ \omega &= \frac{\omega'}{\sum_{i=1}^{n}\omega'}. \end{aligned} \tag{5}$$

In order to evaluate n information systems, the evaluation group set is $D = (d_1, d_2, \ldots, d_n)$, where $d_k (k = 1, 2, \ldots, m)$ represents the K^{th} evaluator. The subjective judgment is given in the form of evaluation: the utility value is $u^{(k)} = (u_1^k, u_2^k, \ldots, u_n^k)^T$, the language evaluation

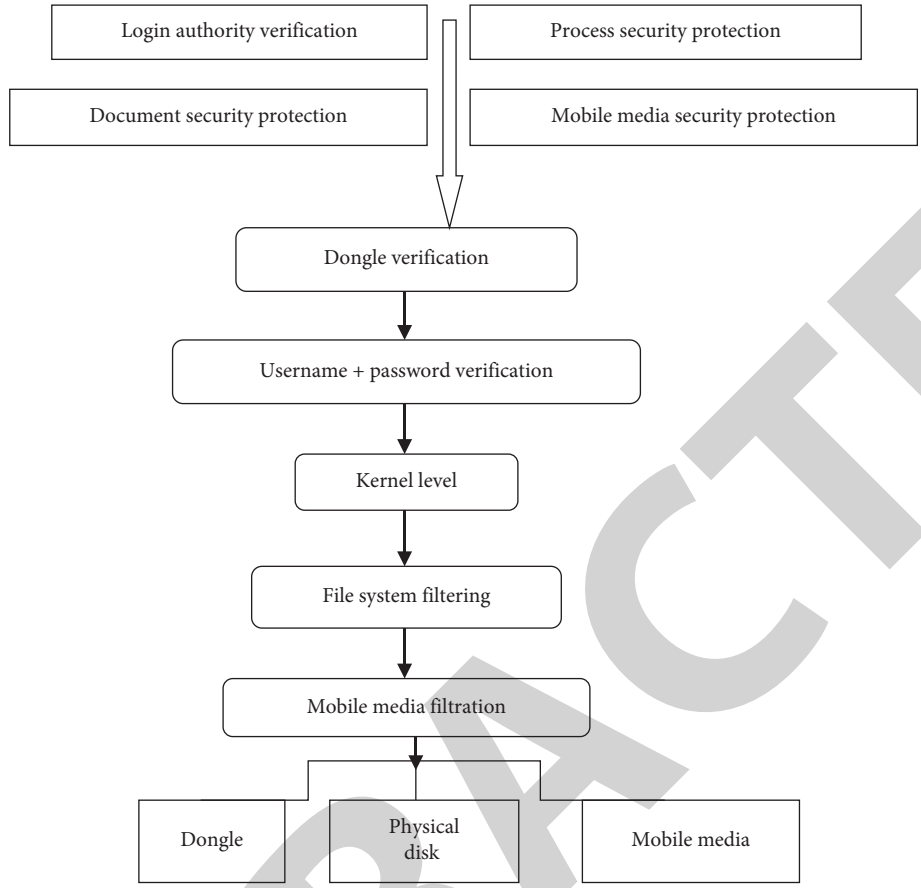

Figure 1: Architecture diagram of the computer multimedia security protection system.

value of active defense analysis is $S = (s_0, s_1, \ldots, s_T)$, and the active defense analysis is complementary. The judgment matrix is $p_{(k)} = (p_{ij}^{(k)})_{n\times n}$, so the information that matches these judgments becomes the utility value.

3. Computer Multimedia Security Protection System Design

It can be seen from Figure 1 of the computer multimedia security protection system architecture that the four modules at the application layer play a very important role. Therefore, the design and development of these four modules are emphasized.

3.1. Login Permission Verification. Figure 2 is a flowchart of the operation of the login authority verification module in the application layer of the computer multimedia security protection system architecture diagram. The main process includes inputting the dongle after the computer is running and then verifying the media. If the conditions are met, the media will be further loaded, and if the media verification is not passed, the program will be forbidden. At this time, the entire system cannot continue to run, and the judgment efficiency is high. After the loading medium is passed, the next step is to verify the certificate file and then verify the user' name and password [8–11]. After these subroutines are verified, the program can be successfully opened, and if any intermediate link fails to pass the verification before starting the program, then the safety protection system will all recognize it as a failure and return to the prohibition of loading the program again. It can be seen that the authentication of login authority plays a vital role in the security protection of the entire computer system, and the security protection level and overall operation efficiency are relatively high.

3.2. Process Security Protection. Process security protection belongs to the application layer of the computer multimedia security protection system. Its existence can control the process of the computer multimedia security protection system to start, terminate, verify external information, exclude untrusted processes, and add trusted processes [12]. Its running process is shown in Figure 3. In the actual running process, when the process security protection module is opened, if it is judged that it is a safe condition at this time, the process will be further created, and if the process security protection module fails to open or the process creation fails, the program will be directly terminated. After the program is created successfully, the computer will further execute the underlying driver and verify the underlying process information after success, open the process after passing it, send the program to the application layer after failure, and use the

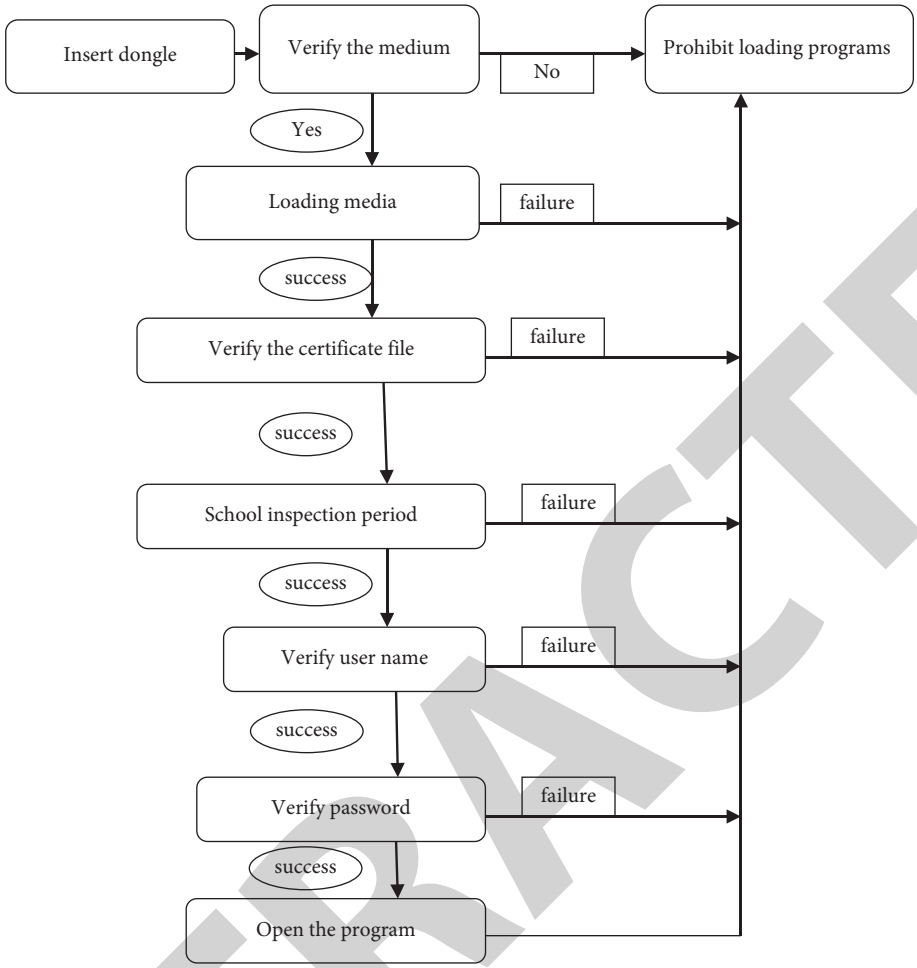

Figure 2: Operation flowchart of login authority verification module.

query open program mode to operate the entire running process. Only the program that trusts the current operation is executed in the open program, and the untrusted operation is added to the blacklist. After the trusted program is successfully run, it can be further added to the trusted program to speed up the efficiency of the next operation [13, 14]. During the entire running process of the security protection module, the entire running program will end whether it is the failure of the underlying driver or the failure of the program to be sent to the program.

3.3. Document Security Protection. Document security protection is also subordinate to the application layer of the computer multimedia security protection system. Its existence can ensure the integrity and confidentiality of data files. During the operation process, it plays a role in starting the program, loading the driver, reading the document, and controlling the document application effect. Since the current computer system generally uses the drive system provided by Windows officially, although this drive system is stronger than the application programming interface in protection and safety, it has greater difficulties in specific technical implementation. Therefore, this study designs a document security protection system based on filter-driven technology. Figure 4 is a flowchart of document security protection operation based on computer multimedia security protection. In the actual computer application process, an authorization process is required after opening the data file (such as Doc and XLS); if it is an unauthorized process, the corresponding ciphertext is required for processing; in the authorization process, a verification process is required for subsequent operations. If there is a ciphertext display, stop the operation. If this is not the case, you can open the document and then perform the underlying I/O driver processing. During this process, you can observe whether the program is running normally and then determine whether to read the key. If the key read is successful, the read-write control operation can be performed, and both write and read are performed in an encrypted operating environment, and if the key read is unsuccessful, the next operation is refused. This self-designed document security protection system based on filter drive technology has stronger protection functions than the traditional application programming interface and the drive system provided by Windows officially. This type of document security protection system can be introduced in the actual computer application process to strengthen the protection of documents with special confidentiality requirements.

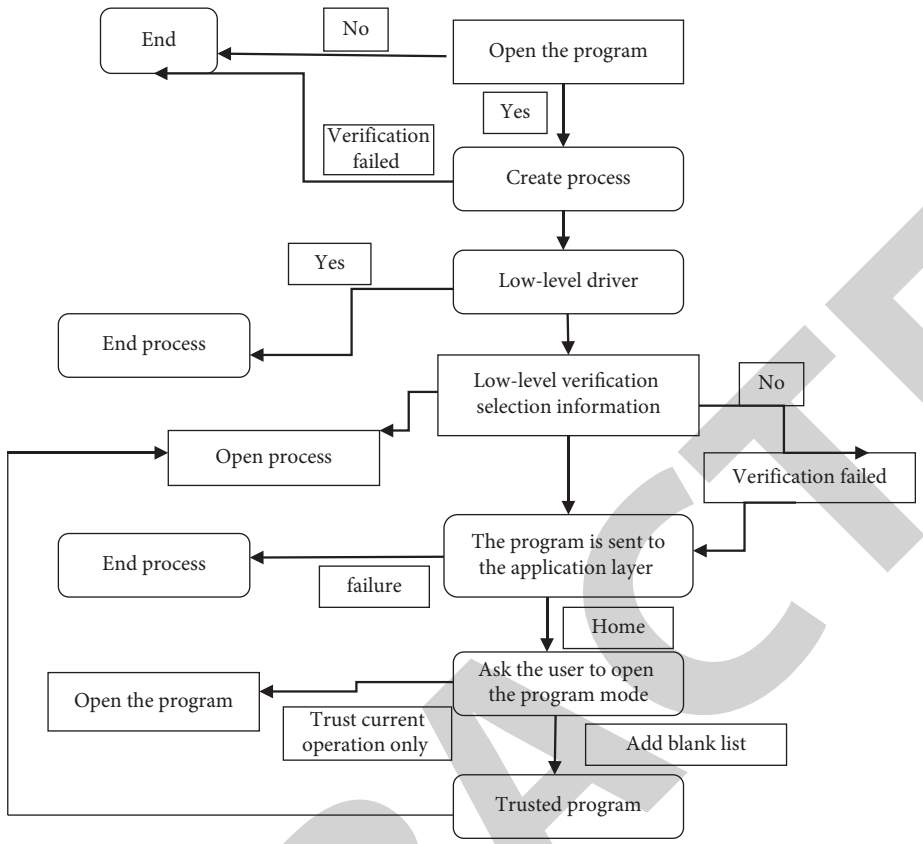

Figure 3: Process security protection operation flowchart.

3.4. Mobile Media Security Protection. The mobile media security protection also belongs to the application layer of the computer multimedia security protection system, and its existence can realize the functions of computer reading and writing control and information transmission. In the process of daily work, life, and study, mobile media are ubiquitous, and the security protection of such mobile media with communication and connection attributes is considered to be a module that needs to be strengthened [15]. From the perspective of past mobile media security protection strategies, the overall structure should be mainly carried out from the steps of monitoring the system before use, preventing during use, and eliminating hidden dangers after use [13].

Figure 5 is a flowchart of mobile media security protection operation based on computer multimedia security protection. During the use of the computer, media verification is required after the removable media are inserted. If the verification is passed, the next step can be loaded. If the media verification is not passed, the loading is directly prohibited. This is an important basis for mobile media protection and media loading. The process is divided into two types: loading success and loading failure. The next step of verifying the algorithm key operation can be carried out if it succeeds. If it fails, the operation is directly prohibited; after the verification algorithm key operation is successful, the verification period is confirmed, and it is successful. You can read and write data. If any step of the above process fails, the operation is prohibited; writing data are more complicated than reading data. After reading, the entire mobile media function is basically completed, and data are written. It is also necessary to perform verification and write protection in the subsequent process, which can be subdivided into two types: readable and unwritable and readable and writable in the open state, according to actual needs.

4. Computer Multimedia Security Protection System Performance Test

Data collection CMESS is deployed in the data source, and in the computer multimedia information network, in order to minimize the pressure of collection on the monitored equipment, the strategy of "collect once, use multiple times" should be adopted as much as possible to avoid alarms, performance, and assets and repetitive collection of data such as security incidents. In terms of information extranets, as the main threats faced are from Internet attacks and penetrations, external website vulnerabilities being attacked, websites being tampered with or planting viruses and Trojan horses, and extranet desktop terminal information being stolen, therefore, collecting CMESS is mainly used in information extranets. The collected content is information extranet and Internet boundary security device logs, Internet egress mirroring traffic information, and desktop terminal management software monitoring information. In terms of the information internal network, the boundary of the information in internal and external networks adopts a strong isolation device for computer multimedia special logic, reducing the threat of attacks from external networks.

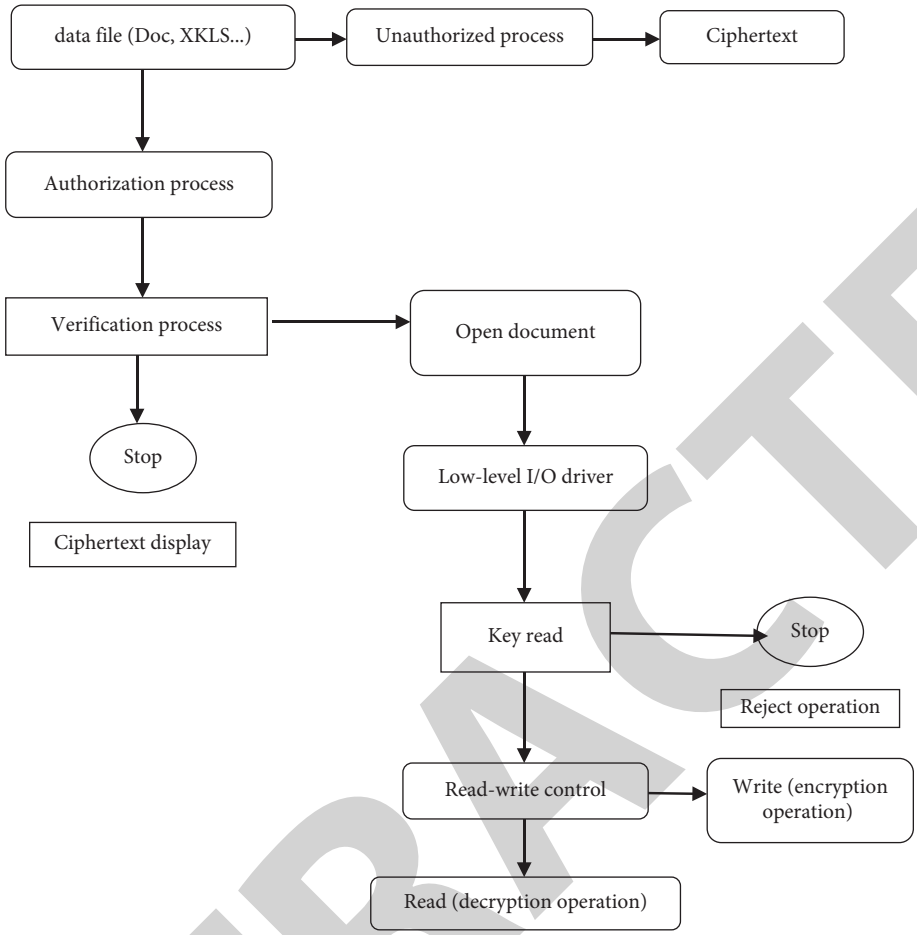

Figure 4: Flowchart of document security protection operation.

However, the main computer multimedia business system deployed in the information intranet is more sensitive to security incidents and threats, and it is necessary to further improve the operation and maintenance capabilities and the level of security monitoring. Therefore, the main collection content of CMESS in the information intranet is network equipment alarm information, network equipment, host (including server, database, and middleware), application performance data, desktop terminal management software data, and asset data. In addition, the data source can also come from the results of risk assessment (including asset identification, category, value, vulnerability, threat, and impact).

As shown in Figure 6, the CMESS management library is responsible for creating, adding, deleting, and configuring data collection CMESS and data processing CMESS. Data collection CMESS performs uniform format conversion of probe data according to the uniformly configured data format. Data processing CMESS merges, categorizes, and filters the standardized and formatted data according to the configured processing rules and stores them in the network information database.

After the computer multimedia security protection system is designed and developed, the system performance needs to be further tested to ensure that the security protection system designed in this article will not affect the normal development of other services and use the system CPU occupancy rate and system memory occupancy rate. The size is an evaluation index. By testing the CPU occupancy rate and memory occupancy after running the system, it can be known that the CPU occupancy rate under the operating environment is less than 20%, and the memory occupancy rate is less than 120M, indicating that the security protection system designed in this study will not affect the normal operation of other computer services. Figure 7 shows the computer's performance index test results after turning on the computer multimedia security protection system and running for 10 hours. Under normal circumstances, the computer's average CPU usage rate is less than 3%, the peak usage rate is less than 12%, the virtual memory usage is 100 MB, and the computer memory usage (working set) is 108 MB. It can be seen that after the security protection system designed in this article is turned on, the computer's normal business operations will not be affected. Beginning in December 2018, the security protection system designed in this article has been deployed, debugged, and used in different occasions. The 6-month trial operation results show that the computer multimedia security protection system designed in this study has achieved computer security protection. The system is easy to operate and has strong

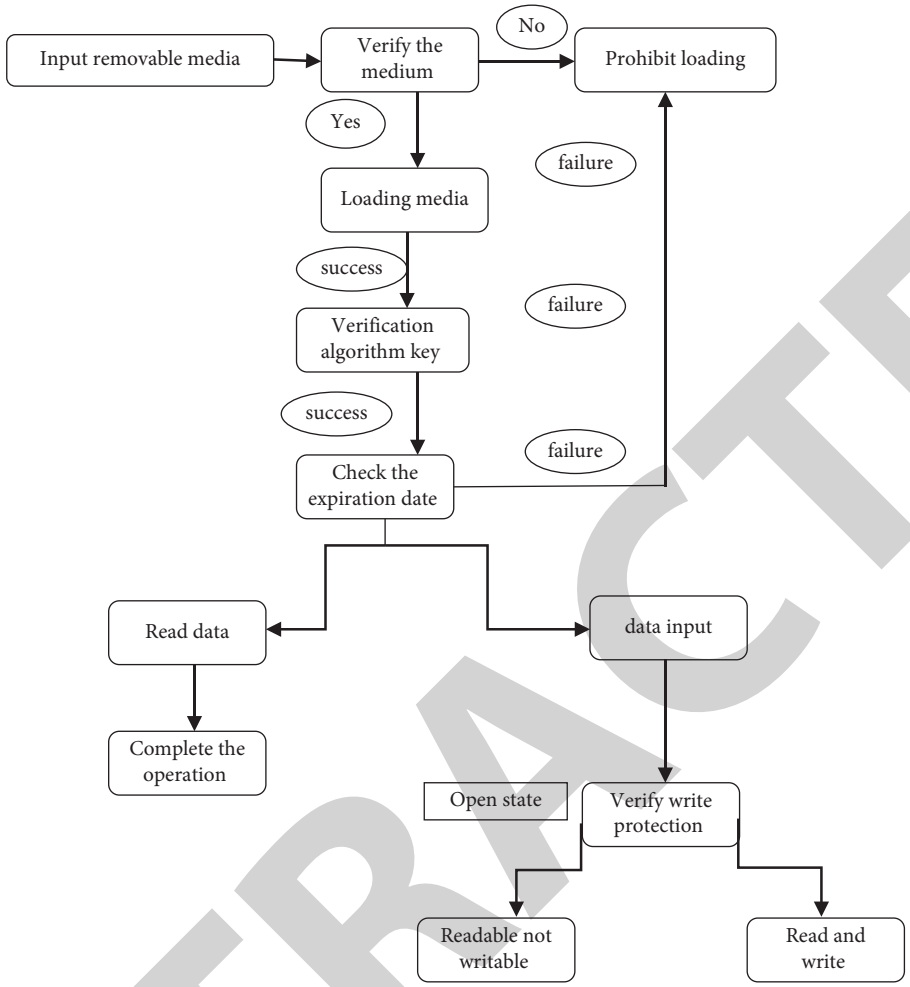

Figure 5: Operation flowchart of mobile media security protection.

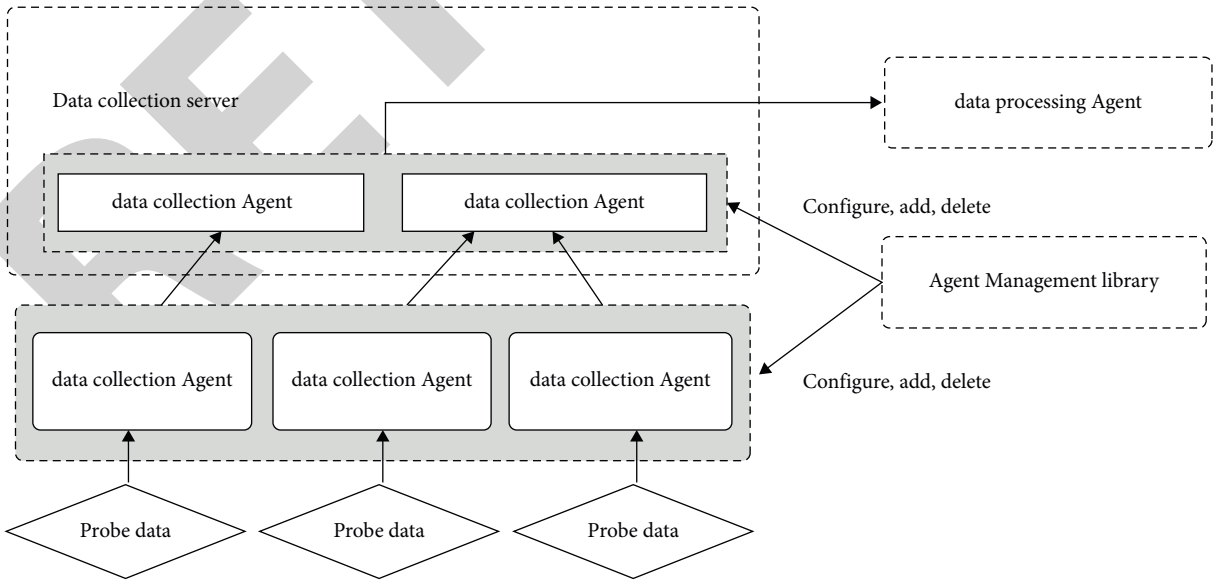

Figure 6: Data collection and processing based on CMESS.

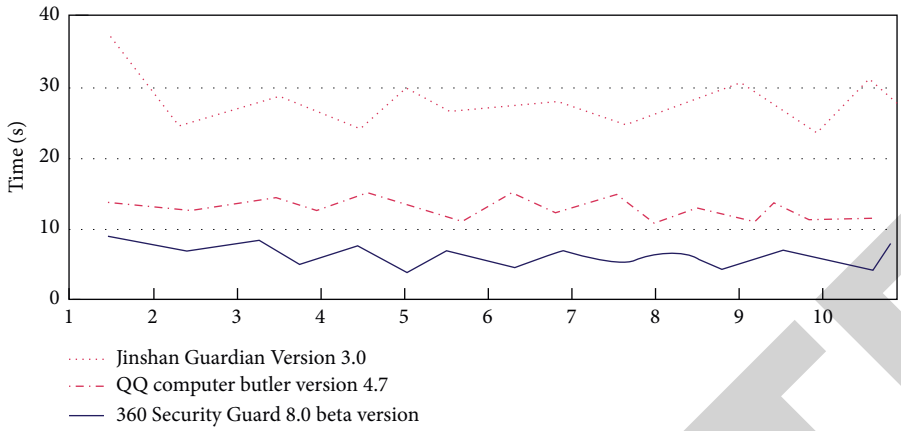

Figure 7: Computer multimedia security protection system performance test results.

practicability. It has achieved the expected effect and can be further promoted and applied.

5. Computer Network Information Security Protection Measures

The continuous development of computer networks and the outbreak of various information data leakage incidents have made computer network users increasingly demanding personal information security. The construction of a computer network information security environment can not only effectively ensure information security but also achieve greater effective protection of information security. This requires that the traditional information security protection measures be used as the basis to continuously increase the construction of information security.

5.1. Users Must Pay Full Attention to Personal Account Security Protection. Proactively strengthening the security protection of network information from the perspective of users is currently the most effective means of maintaining network information security. Therefore, individual users must pay great attention to information security protection, strengthen personal protection measures from the basic starting point of the computer network, actively protect personal related communication accounts, bank accounts, and e-mail accounts, and adopt efficient security management; in the actual application of computer networks, individual users must establish a basic information security awareness and effectively avoid the risk of password leakage by complicating the handling of personal accounts, increasing the difficulty of cracking account passwords, and regularly changing security passwords.

5.2. Strengthen the Level of Computer Information Network Firewall. Firewall security technology is a security technology that effectively controls network access in a computer system. It takes effective security protection strategies from the inside of the computer. The computer network firewall mainly sets different security levels to prevent some illegal users from intruding into the computer in the external network environment. The network system is a very effective protection technology, which can fully guarantee the internal information security of the computer network and play a very important role. During the operation of the firewall, the noncompliant information is filtered by presets of different levels, the illegal data transmission process is effectively blocked, and some dangerous information and operations are filtered to effectively ensure the safe operation of user network information.

5.3. Reasonable Use of Antivirus Software. In the big data environment, the user's computer network system must not only have its own security protection but also is necessary to use third-party software to protect the computer network information. In the process of computer network operation, the extremely strong protection technology and other related equipment cannot fully guarantee the user's information security, and the emergence of antivirus software has made up for this security gap. Antivirus software can be more professional and targeted for purification. The network environment of computer network users can remove system viruses in time. Therefore, many computer network users have generally used various antivirus software.

6. Conclusions

Aiming at the current computer multimedia security problems caused by hacker attacks, natural causes, and computer viruses, this study designs a computer multimedia security protection system that includes an application layer, a core layer, and a hardware layer. Experimental analysis shows that the security protection designed in this study is applied. After the system, the computer multimedia can save 20% of the CPU space occupancy rate under normal operation, so that the memory occupancy is not more than 120M, and at the same time, it can ensure the normal and stable operation of the computer.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research study was sponsored by the projects "Research on Credibility Evaluation System of Dynamic Cloud Services Based on Multisource Information Fusion" by the Hebei Natural Science Foundation (F2019105134) and "Research on Digital Image Manipulation Forensics Based on Deep Learning Pervasiveness," the Scientific Research Fund Project of Tangshan Normal University (2020A04).

References

[1] L. Shi, Q. Zhou, Y. Zhao et al., "Oxidation mechanism and protection strategy of ultrathin indium selenide: insight from theory," *The Journal of Physical Chemistry Letters*, vol. 8, no. 18, pp. 4368–4373, 2017.

[2] C. Li, G. Li, Y. Dong, W. Hu, and W. Chao, "Protection strategy of current suppression resistor used in mmc-hvdc startup process," *Gaodianya Jishu/High Voltage Engineering*, vol. 45, no. 1, pp. 39–45, 2019.

[3] Y. Mingxin, W. Sun'An, W. Canyang, and L. Kunpeng, "Hybrid ant colony and immune network algorithm based on improved apf for optimal motion planning," *Robotica*, vol. 28, no. 6, pp. 833–846, 2010.

[4] D. M. Zhao, J. X. Liu, and J. F. Ma, "Risk assessment of information security based on improved wavelet neural network," *Computer Science-Research and Development*, vol. 37, no. 2, pp. 90–93, 2010.

[5] S. M. Wörmann, K. N. Diakopoulos, M. Lesina, and H. Algül, "The immune network in pancreatic cancer development and progression," *Oncogene*, vol. 33, no. 23, pp. 2956–2967, 2013.

[6] R. Wang and P. Li, "Research on network malicious code immune based on imbalanced support vector machines," *Chinese Journal of Electronics*, vol. 24, no. 1, pp. 181–186, 2015.

[7] F. J. Siddiqui, H. Ashraf, and A. Ullah, "Dual server based security system for multimedia services in next generation networks," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7299–7318, 2020.

[8] W. Yang and P. Zhang, "Research on barrier free design of the landscape environment of the city walking street based on computer multimedia: a security perspective," *RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E8, pp. 292–301, 2016.

[9] C. Xiao, L. Wang, M. Zhu, and W. Wang, "A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft," *Journal of Network and Computer Applications*, vol. 59, pp. 117–125, 2016.

[10] L. Yan, Y. S. Jeong, B. S. Shin, and J. H. Park, "Crowdsensing multimedia data: security and privacy issues," *IEEE Multi Media*, vol. 24, no. 4, pp. 58–66, 2017.

[11] A. Dziech, M. Leszczuk, and R. Baran, *[communications in Computer and Information Science] Multimedia Communications, Services and Security Volume 566 || Ranking Based Approach for Noise Handling in Recommender Systems*, Springer, Berlin, Germany, 2015pp. 46–58, Chapter 4.

[12] K.-H. Choi and D. Lee, "A study on strengthening security awareness programs based on an rfid access control system for inside information leakage prevention," *Multimedia Tools and Applications*, vol. 74, no. 20, pp. 8927–8937, 2015.

[13] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Generation Computer Systems*, vol. 94, pp. 654–673, 2019.

[14] M. Ghadi, L. Laouamer, and T. Moulahi, "Securing data exchange in wireless multimedia sensor networks: perspectives and challenges," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3425–3451, 2016.

[15] A. Dziech, M. Leszczuk, and R. Baran, *[communications in Computer and Information Science] Multimedia Communications, Services and Security Volume 566 || a Multi-Agent Approach for Intrusion Detection in Distributed Systems*, Springer, Berlin, Germany, 2015pp. 72–82, Chapter 6.