Hindawi
Journal of Robotics
Volume 2024, Article ID 9893014, 1 page
https://doi.org/10.1155/2024/9893014

Retraction

Retracted: Security Risk and Preventive Measures of Multimedia Database System under Remote Control of Network Robot

Journal of Robotics

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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) Manipulated or compromised peer review

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] W. Deng and P. Yan, "Security Risk and Preventive Measures of Multimedia Database System under Remote Control of Network Robot," *Journal of Robotics*, vol. 2023, Article ID 9276208, 8 pages, 2023.

Hindawi
Journal of Robotics
Volume 2023, Article ID 9276208, 8 pages
https://doi.org/10.1155/2023/9276208

Research Article

Security Risk and Preventive Measures of Multimedia Database System under Remote Control of Network Robot

Wenyan Deng[1] **and Pengfei Yan**[2]

[1]*Information Technology Department, Shanxi Professional College of Finance, Taiyuan, China*
[2]*Qinhuangdao Vocational and Technical College, Qinhuangdao, Hebei 066000, China*

Correspondence should be addressed to Pengfei Yan; ypftrybytry@163.com

Received 4 November 2022; Revised 1 February 2023; Accepted 29 April 2023; Published 17 May 2023

Academic Editor: Shahid Hussain

The rapid development of network technology makes the world enter a new era, but it also brings a variety of severe information security problems, which makes the network security more and more important. Based on the existing literature and information, this paper expounds the current situation of database information system security. In view of the security risks of the media database information, this paper proposes to use the remote control system of the network robot, through sorting out the organizational structure characteristics and technology of multimedia data, establish the security defense system, and try to manage the multimedia data security. This system takes the mobile robot as the control object and adds the vision and ultrasonic transducer for the robot, so that it can carry on the semi-autonomous movement under the control of human. In addition, the host PC is used as the main control terminal to send instructions to the remote robot and receive the feedback data information. The simulation results show that the robot remote control system has good security, can ensure the establishment of database security defense technology system, and has the characteristics of convenient operation, easy to expand, and strong mobility. From the research point of view of this paper, the combination of robotics and multimedia information security is booming and will become a new application prospect.

1. Introduction

With the continuous development of computer system technology and database technology, the current society has gradually become a "data society," producing all kinds of data, and the same is true for multimedia data [1–3]. The database is the main part of the computer system. It provides convenient information storage function for our users. However, when using the database, it has the characteristics of resource sharing, so there are certain security problems. If you are not careful, the data security of our users will be threatened, resulting in unpredictable losses. Therefore, we must ensure the security of the computer database. In the process of multimedia data storage or transmission, it is very necessary to store, manage, and search multimedia data in a timely and efficient manner. In order to meet the needs of the development of social informatization, we must pay attention to the research and improvement of the current multimedia database, develop new technologies, and continuously improve its use effect [4–6]. The development of robotic remote control technology began in the early 1960s. With the continuous expansion of people's cognition of the natural world and the application of robots, some harsh working environments cannot be avoided, such as exploration in volcanoes, sea exploration, space exploration, patrol, reconnaissance, and monitoring of military bases, and biological, chemical, and nuclear test site operations. High-risk environments bring great harm to the personal safety and mental health of workers and sometimes even endanger their lives. Therefore, many robots working in such harsh environments have changed their on-site control methods from the previous on-site control to wireless remote control [7, 8]. In China, the remote monitoring system of heterogeneous monitoring platforms developed by the

Institute of Automation of Shenyang Branch of the Chinese Academy of Sciences, the shared control system of space robots developed by Harbin Institute of Technology, the remote monitoring system based on the Internet developed by Beijing University of Aeronautics and Astronautics, etc. are prime examples of robotic remote monitoring systems [9–11]. The current models of remote monitoring systems are mostly based on a single point-to-point network control. When the robot is in a complex environment or when multiple robots are required to cooperate, this control method cannot cope with it. The control method based on wireless local area network can easily extend a single robot into a robot group and let it balance its movements while ensuring real time and stability of data transmission.

Multimedia information data have the characteristics of many types, large data scale, and complicated transmission. Therefore, when storing, searching, and managing, it must have a comprehensive design and ensure its data security. Faced with such requirements, this paper, according to the network robot remote control system, organizes the important characteristics of database security, integrates the structure management of multimedia information, and carries out mutual blending to establish a preventive system for information security, aiming at discussing the security management of multimedia database.

2. Network Robot Remote Control System

In the specific use of the database, data backup should be based on effective security principles. If there is a problem with the database due to some reason, the relevant data content can be restored in the case of data backup, so as to ensure the accuracy and comprehensiveness of the data. With the application of this method, problems such as data changes and malicious attacks during database operation can be avoided. A complete set of hardware equipment diagram is shown in Figure 1.

The upper host computer communicates wirelessly with the lower computer based on the wireless connector. In order to ensure the signal quality between the two production workshops and achieve remote wireless control of the robot, a router is added between the two production workshops, which can increase the strength of the signal, prolonging the signal transmission time. The onboard computer uses the EPIA-P700 serial Pico-system motherboard, which has many extended interfaces, small size, and low power. The use of the embedded system motherboard saves development time and increases the stability of the system. Imaging devices and ultrasonic sensors have been added to this motherboard to improve the functionality of every aspect of the mobile robot.

The overall robot system can be divided into wireless communication module, body controller module, motor control unit and main program, sensor, and image collection module. The configuration diagram of each module is shown in Figure 2.

According to the framework of the mobile robot control system in Figure 2, the body operation controller of the robot, as a key part of the control system, that is, the brain of

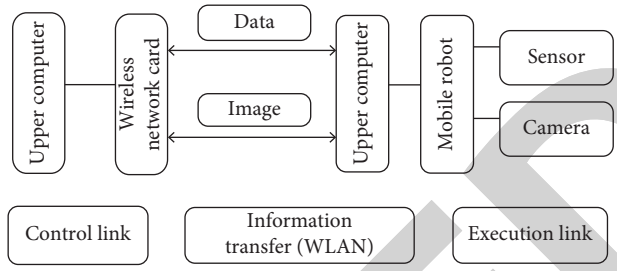

Figure 1: System hardware structure diagram.

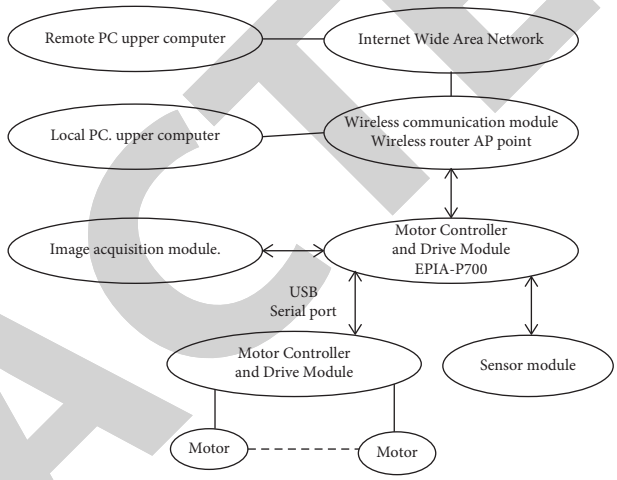

Figure 2: Frame diagram of mobile robot control system.

the robot, not only needs to use the wireless module to communicate with the host computer but also executes according to the received information instructions and sends the received information and instructions to the controller of the next level according to its own port to realize the control of the motor. In addition, the function module for receiving image information can transmit data information to the host computer, so that the main control terminal can know the environment where the mobile robot is located at all times.

The advantage of using templated distributed control is that each control template of each layer of the control system is basically independent of each other. When a problem occurs, it is easy to find out where the error occurred. At the same time, it also simplifies the shift of the system. Any template can be shifted to other systems, as long as the underlying function corresponding to the new system is changed. The vehicle-mounted PC uses a small control board and forms a wireless LAN environment based on a WNIC, a router, and its upper-level control PC [12, 13].

Because the remote control of the robot is mainly based on the received data information, the wireless communication module carried by the host computer PC and the robot itself mainly uses the socket communication method, combined with different transmission data information instructions. Sockets can be divided into connection-facing data flow sockets and connectionless data flow sockets. The

system uses connection-oriented data streaming sockets in this paper, as shown in Figure 3.

When using face-to-face streaming socket communication, the server side should be turned on first; otherwise, an error will occur when the client connects. The communication steps are shown in Figure 3. The vehicle-mounted controller is used as the communication server. After turn-on, first use socket () to set up a socket, then call bind () to combine the socket with the local network IP, and then use listen () to make the socket ready for listening. Ask for the length of the queue, and then use accept () to receive the connection from the PC client. The remote PC can use connect () to establish a connection with the server after turning on the setup socket. As long as the connection is established, the ddc of the frame and the remote PC can transmit and receive information according to the wireless network based on the sub-functions send () and recv () identified by the system.

After the fuselage ddc receives the instructions sent by the remote host computer (the detailed walking path or pace), it will be saved. When the data information is received, close the socket, forward it to the next motor ddc, the motor ddc interprets and executes it, and the body ddc transmits it to the motor ddc. The data transmission steps are shown in Figure 4.

Before the serial communication between the fuselage computer and the motor computer is turned on, the serial port should be set first. Here, we use the underlying function library of the motor computer [14, 15].

Suppose that the input of the Qth sample is P_n and the output of the Qth sample is P_{n-1}.

$$I_{qj} = \sum_{i=1}^{n} w_{ij} \times x_{qi} - \theta_j. \tag{1}$$

The ith neuron in the hidden layer and the weight value are P_{back}. At the same time, P_n is the threshold.

The output value of the jth neuron is shown in the following formula:

$$Q_{qj} = f\left(I_{qj}\right) = \tan sig\left(I_{qj}\right) = \frac{2}{1 + e^{-2I_{qj}}} - 1. \tag{2}$$

The input value of the jth neuron is shown in the following formula:

$$I_q = \sum_{j=1}^{h} w_j \times Q_{qj} - \theta. \tag{3}$$

The output value of the qth neuron is shown in the following formula:

$$Q_q = f\left(I_q\right) = \tan sig\left(I_q\right) = \frac{2}{1 + e^{-2I_q}} - 1. \tag{4}$$

3. Analysis of Security Prevention Technology of Multimedia Information Database

3.1. The Main Characteristics of Database Security. According to the important characteristics of database security, its characteristics include many aspects such as security, comprehensiveness, concurrent control, and fault recovery. The important features of database security are described in detail. The details are as follows [16, 17].

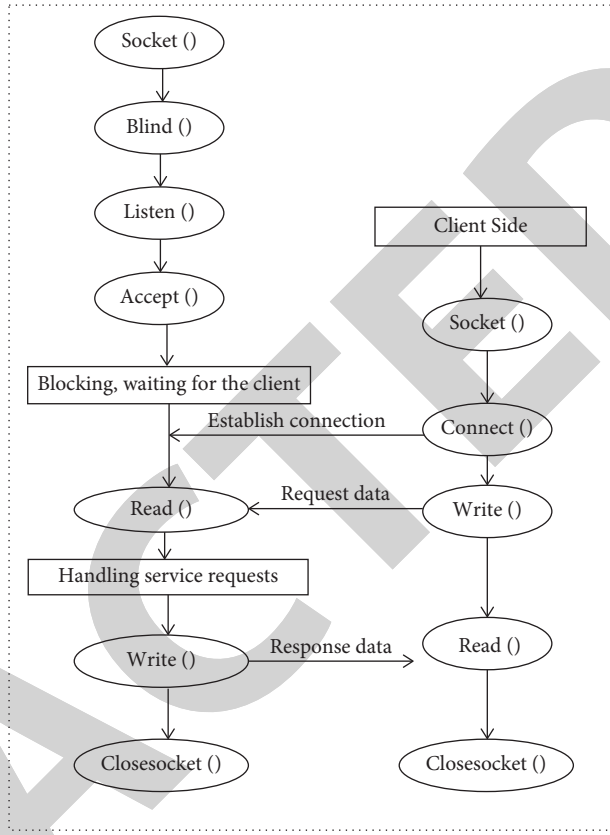

Figure 3: Flow socket programming flowchart.

Security. In order to better ensure the security of database information, the important data should be managed separately and separated from other data during management, so as to better ensure the security of the data and prevent the loss of important data. In addition, attention should be paid to standard access, timely control of access, and access through relevant requirements to ensure the security of the database in each link. In addition, all kinds of information stored in the database should be encrypted, and audit-related work should be done to ensure the security of the information.

The data collection interface is the main component in the application of the multimedia information database. It completes the data exchange between the production process control system and the real-time database system. The industrial communication gateway based on the embedded configuration has the advantages of high reliability, small size, light weight, easy to carry and maintain, easy to extend, and sufficient functions. The main service software of the embedded computing platform can run on the desktop. Because the data are complete and easy to forward, they can be used at ease. At the same time, the platform can access different types of protocols and convert them into standard protocols (such as OPC methods) to connect with other systems. Therefore, the data collection gateway is used in the field data collection system and the real-time database server to realize data collection.

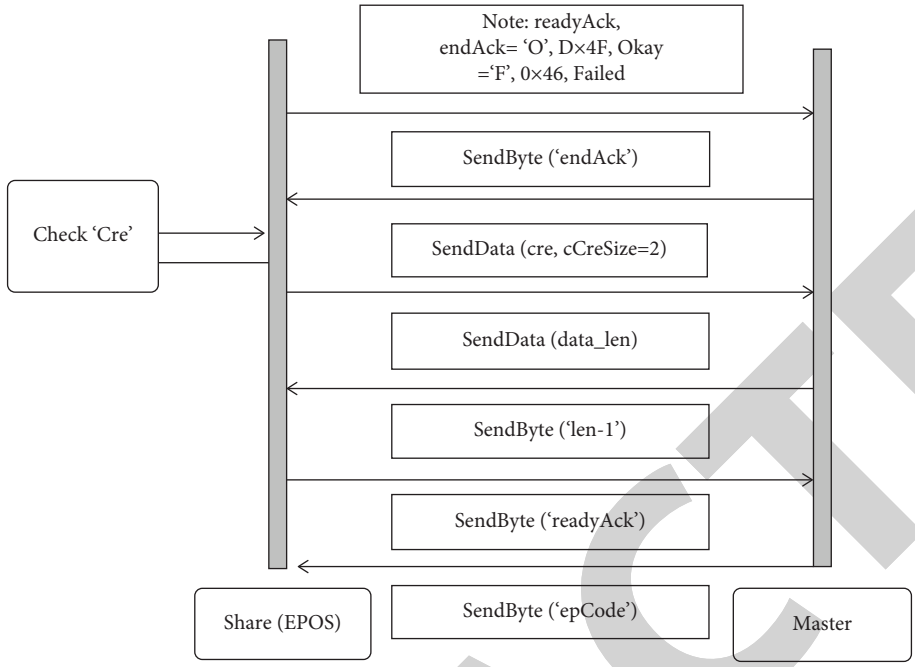

Figure 4: Flowchart of data transmission of robot control system.

Comprehensiveness. Comprehensiveness mainly includes many contents such as data accuracy, validity, and compatibility, and these contents cannot be lost. If lost, the integrity of the data will be affected.

Concurrency Control. In a database, each data resource is used not only for a single purpose but also for multiple users. Users who use resources together can also operate the database, that is, multiple users manipulate data. Although this method has certain convenience, it also has many disadvantages. When carrying out the same operation, if users access the relevant data together, it is easy to cause errors and pose a serious threat to the security of the data. In this case, concurrency control is very necessary. Fourthly, in terms of the function of fault recovery, it is beneficial to ensure data security. In addition, the database can self-correct and recover the correct information, so that the fault in the first time can be efficiently handled, which plays a great role in ensuring data security.

The purpose of database management is to efficiently implement unified management and security inspection of the information transmitted by the network database, which needs to ensure the correct logic of the data, and in addition, the transmitted data information needs to be implemented according to the actual use needs. There are many ways of user identification and identification, and user identification and identification are often used together in a system in multiple forms. While ensuring database security to a certain extent, it is significantly more expensive during operation.

The most prominent expression in the system is the communication and interaction between the object and the subject. Under normal circumstances, users determine the access of subjects and objects at the level of data deletion and modification, which shows many advantages such as comprehensiveness, practicability, and confidentiality of data information. Furthermore, access manipulation is also a major part of establishing resource access handling. Access control can best show that its essential purpose is to carry out forced control, especially in the face of special circumstances, and this method of forced control should be implemented. Mandatory access manipulation is quite different when compared to this approach. Its security attributes are often aggregated at the subject and object level, but this security attribute cannot be changed by the database user. At this time, the access rights are limited to administrators for management and distribution. No matter which of the two methods mentioned above is used, the security of the database can be ensured. Therefore, the above two methods can be used to achieve the goal of ensuring the security of the database.

The main process of auditing database information is to provide information managers with a set of data that can be used for analysis and then perform security audits on this set of information, so that all unsafe information can be found in time. Such a method is very convenient and is conducive to improving the work progress of managers and carrying out management work efficiently [18–20]. If the auditing function is turned off in data management, it is easy to increase the probability of data loss, which will have a negative impact on the development and improvement of the enterprise. It is necessary to pay attention to the work of security audit, in order to ensure the security and comprehensiveness of information.

3.2. Organization and Management Technology of Multimedia Information. For multimedia, different from other data management, the data type of multimedia information is

complex and the amount of data is large, such as video, audio, and image. There are obvious differences in each type of multimedia data, and they cannot be stored or retrieved directly according to a rule or method [18, 19].

For the corresponding data management and storage of the existing relational database, its essence is to carry out a meaning mapping to the unformatted data through a fixed file. The relational database does not need to consider unformatted data and only stores the corresponding index files. Users can access the indexes in the database and directly find the location of the multimedia files. This ensures the efficiency of data retrieval. The storage of multimedia information data can ensure the safety and effectiveness of the data.

The database operating system is used to connect with the data information function module of the operating platform, so as to realize the real-time management of the asymmetric speech data information. The method adopted in this paper is to assume that the data information of a specific row and column appears in the relationship between the two. As an asymmetric structure, these row and column data can be stored in a specific folder, and the name of the folder is stored in the corresponding location [20]. This method can be used not only to make the DBMS regardless of the storage configuration of the unformatted data but also to complete the management of DBMS unstructured information. It only manages the use of unstructured information, that is, file names, but not unstructured data. Therefore, under this method, the DBMS lacks the common control and recovery of unstructured data, and this can only be completed by using the OS system and application programs. In addition, this method needs to include OS file I/O in the disposal, resulting in a relatively low progress. But it can easily expand the database management platform that does not support unstructured data and indirectly "manage" unstructured data. The biggest advantage is that it can make good use of the advantages of the OS platform to complete the file sharing of unstructured information data. It is very important to store only this data name in the database to reduce the unnecessary storage of unformatted information, so most of the unstructured data are relatively large.

In addition, the formatted data of multimedia information and unformatted data can be encapsulated together to form a complete closed loop. Since unformatted multimedia information occupies a major part and the data volume is large, more data storage space needs to be set.

Unformatted data can be divided into index parts or data sources according to the attributes of the data, and the data space can be matched and set according to the attributes. If it is the data index part, the space does not need to be set too large; if it is the data source, you need to consider the size of the data volume.

In addition to the original relational data model, there is also an object-oriented data model. In terms of supporting multimedia information data, the object-oriented data model can well perform data aggregation, realize and handle complex objects such as multimedia information, and support the definition and operation of abstract data types of multimedia information data; it can further reduce the redundancy of multimedia information data, improve the retrieval and management efficiency of multimedia information data, optimize the query process, and directly conduct relevant retrieval and query of multimedia information through the index.

4. Application Analysis of Multimedia Information Security Protection System

4.1. Process Description. For the construction of the multimedia information security protection system, the specific process can be described as follows [21, 22].

The ciphertext C is

$$C = ECB(DCA(K)). \tag{5}$$

After receiving C, B obtains the key K through the encryption algorithm:

$$ECA(DCB(C)) = ECA(DCB(ECB(DCA(K)))) = ECA(DCA(K)) = K. \tag{6}$$

In this way, B is sure that the key K is sent from A, and the text content is obtained through the key K (P) of the encryption algorithm.

4.2. System Security Analysis. Now based on the network robot remote control system, fingerprint identification and hash function are added to construct a new encryption system [23, 24]. The architecture is shown in Figure 5.

For the multimedia information security protection system, the process is that A first calculates the multimedia information through a quantitative function, encrypts it with an encryption algorithm, then performs identity authentication after signing, and then passes the signature together with the multimedia information to B. During the whole process, if someone wants to pass the message directly without authentication, it will be displayed as unsuccessful.

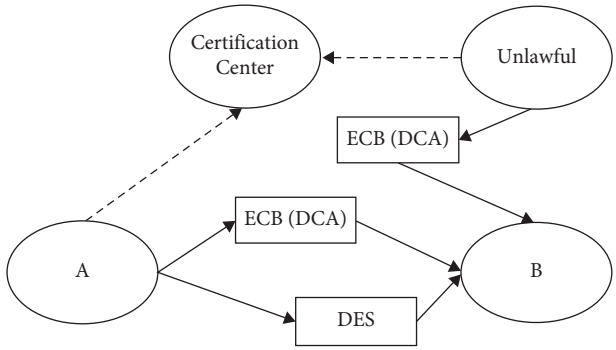

Figure 5: Security analysis flowchart.

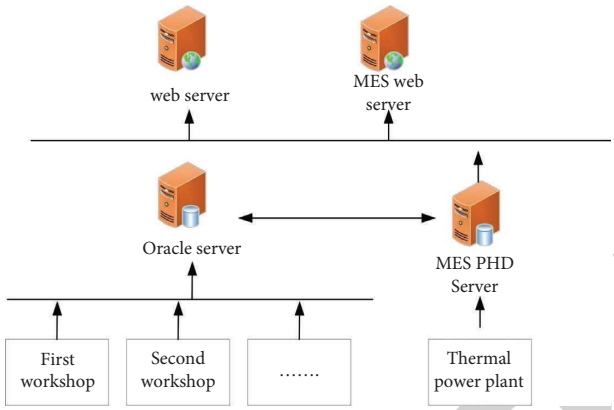

Figure 6: Real-time database system network topology.

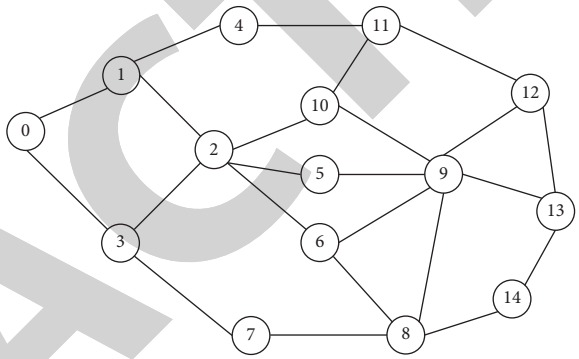

Figure 7: Open multimedia information transmission node diagram.

If B wants to directly modify the data passed by A, it cannot be modified without A's secret key.

For simple data in transmission, no protocol is used to constrain it, but for some advanced data, format conversion must be implemented first, which must be implemented in the corresponding service level, and finally the purpose of encapsulation is completed (Figure 6).

For the validity detection of encrypted multimedia information retrieval, transmission, and management, in the environment of simulation experiment, 20 multimedia information data are selected and corresponding data samples are set [25, 26]. After a certain transmission rule is implemented, the specific multimedia information data transmission node is shown in Figure 7, and the probability of its transmission crossing is set to 0.95.

From the analysis of the data results, it can be seen that when the multimedia information data are transmitted, due to the large amount of data, the effect of transmission control may have a certain weakness, and the information required by the user is not directly placed in the corresponding transmission channel. However, the network robot remote control system proposed in this paper uses the desired control method to encrypt, so that users can obtain safe and effective multimedia information data through reasonable

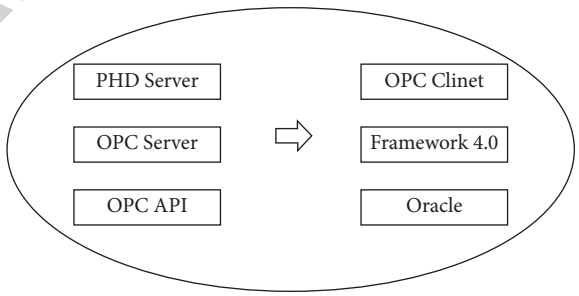

Figure 8: Principle of PHD external data output.

transmission and effectively realize the data control of multimedia information transmission (Figure 8).

From the result analysis in Figure 9, it shows that the circle represents the packet loss that occurs when the remote control system of the network robot is not used. It can be seen intuitively from the results that the multimedia information data security of the network robot remote control system is higher, and the packet loss rate remains below 7%. The results show that the network robot remote control system proposed in this paper has obvious multimedia security prevention technology, which ensures the safe and effective storage, management, and transmission of multimedia information data.

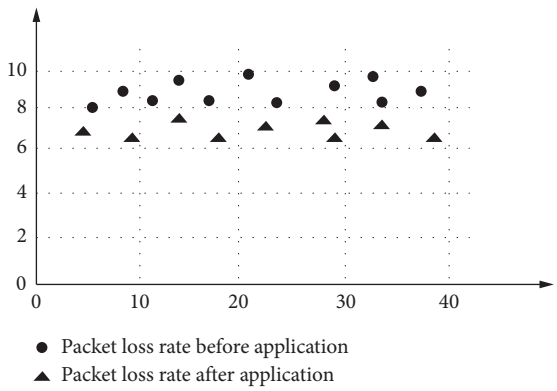

Figure 9: Relative packet loss rate in the state of information network congestion.

5. Conclusion

With the continuous development of social economy, multimedia data show a growing momentum, thus causing the problem of data security. For this demand, this paper relies on the network robot remote platform control system and establishes a security defense system by sorting out the organization and management characteristics and technologies of multimedia information. The application of the remote control platform of the displacement robot through the wireless local area network allows the robot to leave the dependence on the upper control PC terminal in the region. During the work of the robot, the remote operator can continuously observe their working status and adjust their working conditions due to the working environment. The robot can control and deal with changes or emergencies in time, which greatly improves the flexibility of the mobile robot. This scheme uses a small embedded motherboard, which increases the speed of the robot's self-processing of data, improves the ability to recognize the environment, tries to implement multimedia data security management, and uses simulation experiments to verify the calculation method. The simulation experiment results show that the robot remote control system has high effectiveness and can support the establishment of the security protection system of multimedia information big data.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Toapanta, E. Mafla, and J. Orizaga, "Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador," *Materials Today Proceedings*, vol. 5, no. 1, pp. 636–641, 2018.

[2] G. D. Dalvi, S. D. Wakde, and P. V. Kale, "Database security using multi-shares visual cryptography," *IOSR Journal of Electronics and Communication Engineering*, vol. 14, no. 2, pp. 37–43, 2019.

[3] H. Tufail, K. Zafar, and A. R. Baig, "Relational database security using digital watermarking and evolutionary techniques[J]," *Computational Intelligence*, vol. 7, no. 3, pp. 42–60, 2019.

[4] W. A. Yasnoff, "Breach risk magnitude: a quantitative measure of database security," *AMIA Symposium*, vol. 2016, no. 4, pp. 1258–1263, 2016.

[5] F. Thams, A. Venzke, R. Eriksson, and S. Chatzivasilleiadis, "Efficient database generation for data-driven security assessment of power systems," *IEEE Transactions on Power Systems*, vol. 5, no. 6, pp. 1–10, 2019.

[6] S. Malhotra, M. N. Doja, and B. Alam, "Cloud Database Management System security challenges and solutions: an analysis[J]," *Csi Transactions on Ict*, vol. 3, no. 4, pp. 1–9, 2016.

[7] X. Tao, Y. Liu, and F. Zhao, "Graph database-based network security situation awareness data storage method[J]," *EURASIP Journal on Wireless Communications and Networking*, vol. 18, no. 1, pp. 56–63, 2018.

[8] W. El-Hajj, G. Ben Brahim, H. Hajj, H. Safa, and R. Adaimy, "Security-by-construction in web applications development via database annotations," *Computers & Security*, vol. 59, no. 3, pp. 151–165, 2016.

[9] C. Tan and X. Lu, "Research on user security authentication method of eco-environmental monitoring database," *Arabian Journal of Geosciences*, vol. 14, no. 11, pp. 1–11, 2021.

[10] S. Vavilis, A. Egner, M. Petkovic, and N. Zannone, "An anomaly analysis framework for database systems," *Computers & Security*, vol. 53, no. 9, pp. 156–173, 2015.

[11] J. D. Domingo-Ferrer, Sánchez, and J. Soria-Comas, "Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 8, no. 1, pp. 1–136, 2016.

[12] Jeong-hyeon and J C. Kim, "A recovery method for deleted records in the ESE Database," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 25, no. 5, pp. 1143–1151, 2015.

[13] R. Xu, K. Morozov, Y. Yang, J. Zhou, and T. Takagi, "Efficient outsourcing of secure k -nearest neighbour query over encrypted database," *Computers & Security*, vol. 69, no. 8, pp. 65–83, 2017.

[14] S. M. Darwish, "Machine learning approach to detect intruders in database based on hexplet data structure," *Journal of Electrical Systems and Information Technology*, vol. 3, no. 2, pp. 261–269, 2016.

[15] H. I. Kim, A. A. Hossain, and J. W. Chang, "A spatial transformation scheme supporting data privacy and query integrity for security of outsourced databases: t," *Security and Communication Networks*, vol. 7, no. 10, pp. 1498–1509, 2014.

[16] M. Y. AlYousef and N. T. Abdelmajeed, "Dynamically detecting security threats and updating a signature-based intrusion detection system's database," *Procedia Computer Science*, vol. 159, no. 5, pp. 1507–1516, 2019.

[17] O. M. Pereira, D. D. Regateiro, and R. L. Aguiar, "Secure, dynamic and distributed access control stack for database applications," *International Journal of Software Engineering and Knowledge Engineering*, vol. 25, pp. 1703–1708, 2015.

[18] G. Mohamed, Y. Attila, and H. Bechir, "Location privacy preservation in database-driven wireless cognitive networks through encrypted probabilistic data structures," *IEEE*

Transactions on Cognitive Communications & Networking, vol. 3, no. 2, pp. 61–69, 2017.

[19] A. Schulz, C. Sung, A. Spielberg et al., "Interactive robogami: an end-to-end system for design of robots with ground locomotion," *The International Journal of Robotics Research*, vol. 36, no. 10, pp. 1131–1147, 2017.

[20] A. Zh and B. Hha, "ProDB: a memory-secure database using hardware enclave and practical oblivious RAM," *Information Systems*, vol. 96, no. 3, pp. 109–118, 2020.

[21] H. Wang and J. Ren, "The design and implementation of information management system in laboratory of paper enterprises," *Paper Asia*, vol. 2, no. 3, pp. 113–116, 2019.

[22] D. Abadi, "Consistency tradeoffs in modern distributed database system design: CAP is only part of the story," *Computer*, vol. 45, no. 2, pp. 37–42, 2012.

[23] J. Lui, A. M. Vegni, L. Colace, A. Neri, and C. Menon, "Preliminary design and characterization of a low-cost and low-power visible light positioning system," *Applied Optics*, vol. 58, no. 26, pp. 7181–7188, 2019.

[24] Z. Li, Y. Xue, H. Zhou et al., "High-resolution mapping and breeding application of a novel brown planthopper resistance gene derived from wild rice (Oryza. rufipogon Griff)," *Rice*, vol. 12, no. 1, pp. 41–45, 2019.

[25] S. D. Rajan and M. A. Bhatti, "On designing a database management system for a computer-aided engineering software system," *Computers & Structures*, vol. 21, no. 5, pp. 1047–1057, 1985.

[26] I. C. Chen, H. Hamano, and H. Iwasaki, "An economic-environmental analysis of lithium ion batteries based on process design and a manufacturing equipment database," *Journal of Chemical Engineering of Japan*, vol. 52, no. 1, pp. 1–8, 2018.