

Remote Computer Monitoring System Based on HTTPS Communication

Yuanhang Cao, Jiyan Zhang*, Ruidan Xue and Jiao Li
National Institute of Metrology, China

Keywords: Computer Monitoring, End-to-End Encryption, Laboratory Computer Management.

Abstract: To achieve computer monitoring for laboratory research instruments, we have designed and developed a remote computer monitoring system based on HTTPS communication. The system encompasses architecture, communication protocol, data encryption and decryption algorithms, and user interface design. It employs HTTPS communication protocol with hybrid RSA and AES encryption for end-to-end communication, providing a secure, simple, and convenient deployment method. Moreover, the absence of control commands effectively prevents password leaks that could compromise laboratory security. Through this system, users can remotely monitor and manage the computers associated with laboratory research instruments, obtaining real-time information on computer status, operational logs, and performance data to promptly address issues and enhance laboratory management efficiency and security. Experimental results demonstrate the system's stability and security, making it suitable for laboratory computer monitoring needs.

1 INTRODUCTION

With the continuous advancement of technology and the expansion of laboratory scale, computer-aided design (Chan, 2022) and computer-aided experiments (Nie, 2022) have become increasingly prevalent in laboratories. However, during prolonged experiments, it is challenging to ensure continuous human supervision and real-time knowledge of experiment progress, which adds complexity to laboratory management. Therefore, there is a pressing need for a tool that enables remote monitoring of laboratory computers and experiment progress. Traditional methods of laboratory computer monitoring, such as widely used software like Teamviewer (Norena, 2022) and Oray, have shortcomings. Account and password leaks could lead to complete exposure of computers to unauthorized control, potentially resulting in confidential information leakage and equipment damage. Additionally, these methods lack the ability to customize experiment monitoring, only allowing remote computer operation without easy access to experiment status and progress. Furthermore, data transmission heavily relies on the stability of service providers. To address these issues, this paper proposes a remote computer monitoring system based on HTTPS communication, employing HTTPS communication and RSA-AES hybrid

encryption in data transmission to provide secure, simple, and convenient deployment while effectively preventing password leaks that could compromise laboratory security. This paper will detail the system's design and implementation process and validate its performance and stability through experiments.

2 SYSTEM DESIGN

2.1 System Function Design

The proposed remote computer monitoring system based on HTTPS communication consists of two main functions: remote monitoring and real-time logging and performance data recording. Users can remotely view the monitored computer's screen content in real-time, ensuring the security of experiment data through end-to-end encryption. Additionally, users can access real-time status information of the monitored computer, such as CPU usage, memory consumption, disk usage, network traffic, etc., as well as customize contents like experiment progress. The system presents these data using intuitive charts and progress bars, enabling users to promptly understand the computer's operational status. Encrypted historical monitoring

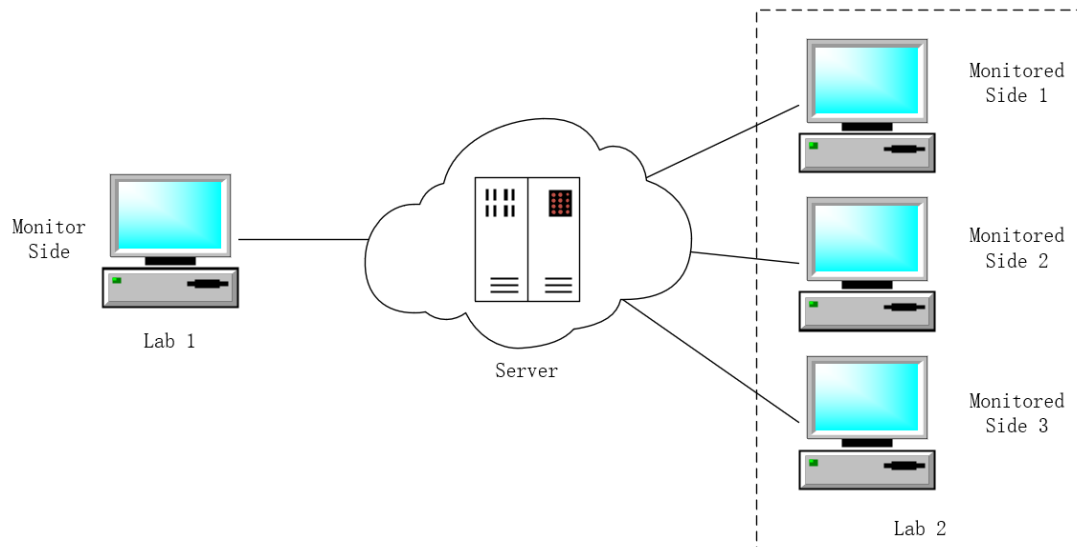


Figure 1: System Design.

data is saved on the server, allowing users to access historical computer and experiment statuses.

2.2 System Architecture Design

The architecture of the remote computer monitoring system based on HTTPS communication comprises three components: the server-side, the monitoring-side, and the monitored-side. The system employs HTTPS communication, and the server authenticates each endpoint while ensuring end-to-end encryption during data transmission. The public internet server acts as a bridge between the monitoring-side and the monitored-side, forwarding data securely. The communication process is illustrated in Figure 1.

2.3 User Interface Design

In this remote computer monitoring system based on HTTPS communication, the GUIs of the monitoring-side and the monitored-side are designed and implemented using the PyQt library to provide user-friendly graphical interfaces.

1) Monitoring-side GUI Design

The monitoring-side GUI aims to facilitate users' remote monitoring and management of laboratory computers. The main design elements of the monitoring-side GUI include:

Login interface: Provides a login system interface where users need to input their usernames and passwords for identity verification, ensuring only authorized users can access the system.

Main interface: Displays a list of computers in the laboratory, allowing users to select the

computers they want to monitor and manage. The interface also shows computer status information and connection status.

Real-time monitoring interface: Displays real-time status information of the monitored computer, such as CPU usage, memory consumption, network traffic, etc. Data is presented using charts and progress bars to facilitate users' understanding of the computer's operational status.

Operation log interface: Records the operational log of the monitored computer, including action logs and error logs, enabling users to review and analyse the computer's operational history.

Performance data interface: Displays performance data of the monitored computer, such as CPU temperature, disk usage, etc., allowing users to assess the computer's health status. Users can interact with the interface through buttons, dropdown menus, etc.

Settings interface: Allows users to configure system settings and personalized options, such as password modification and network settings.

2) Monitored-side GUI Design

The monitored-side GUI aims to provide monitoring and management functionalities for the local computer. It includes the following interfaces:

Basic information display: Shows the basic information of the local computer, such as the operating system and hardware configuration status.

Operation log interface: Records operational logs, including action logs and error logs, for the local computer.

Performance data interface: Displays performance data, such as CPU usage and memory consumption, for the local computer.

Configuration interface: Allows users to configure the local computer and personalize settings, such as network and security settings.

3 SYSTEM IMPLEMENTATION

3.1 Server-Side

To achieve remote monitoring and management, the system utilizes a public internet server as an intermediary node responsible for forwarding communication between the monitoring-side and the monitored-side. During the authentication stage, the public internet server receives requests from the monitoring-side and the monitored-side, decrypts and verifies their identities, and then forwards the requests to the target endpoints. During data transmission, the public internet server receives encrypted messages from the monitoring-side and the monitored-side and forwards them to the target endpoints. The public internet server acts as a bridge connecting the monitoring-side and the monitored-side, ensuring secure data transmission and end-to-end communication.

The server-side is the core of the entire system, responsible for receiving and processing requests from the monitoring-side and the monitored-side. The server needs to handle HTTPS requests and can achieve HTTPS communication using the SSL/TLS protocol. The server authenticates the monitoring-side and the monitored-side connected to the system, ensuring that only authorized endpoints can communicate with the system. Identity authentication can be achieved through digital certificates or other secure mechanisms. Once the authentication is successful, the server receives and processes requests from the monitoring-side and the monitored-side based on the request type and content. Additionally, the server is responsible for encrypting and forwarding communication between the monitoring-side and the monitored-side, ensuring data security and integrity during transmission. The authentication process between the monitoring-side and the monitored-side is shown in Figure 2.

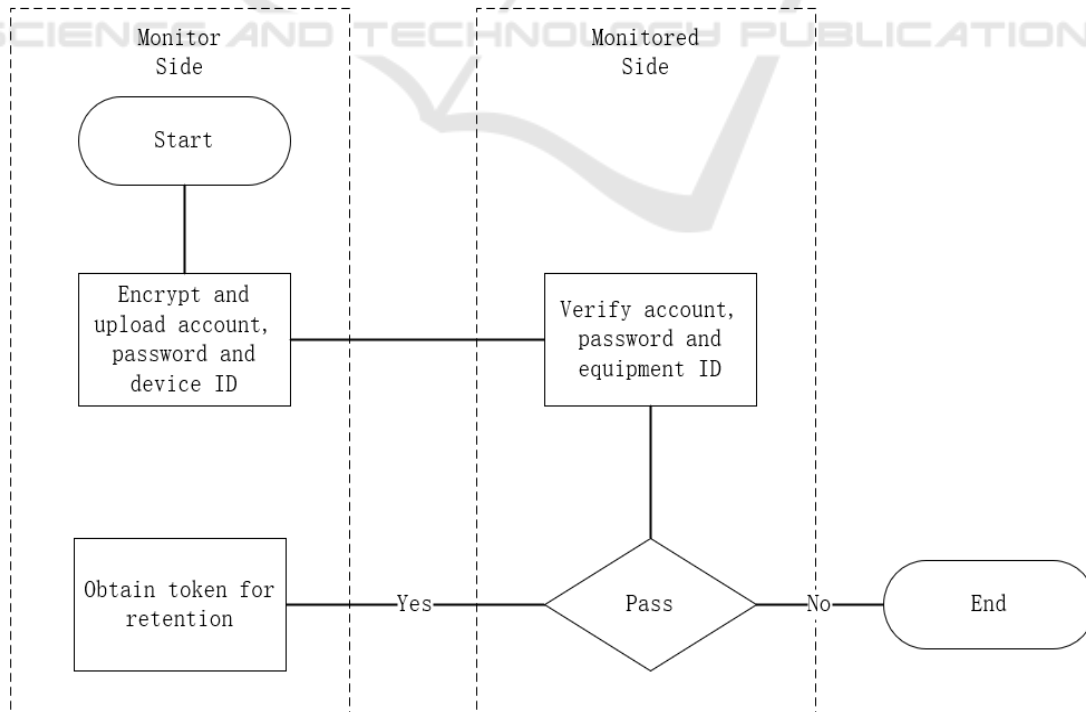


Figure 2: Authentication Process.

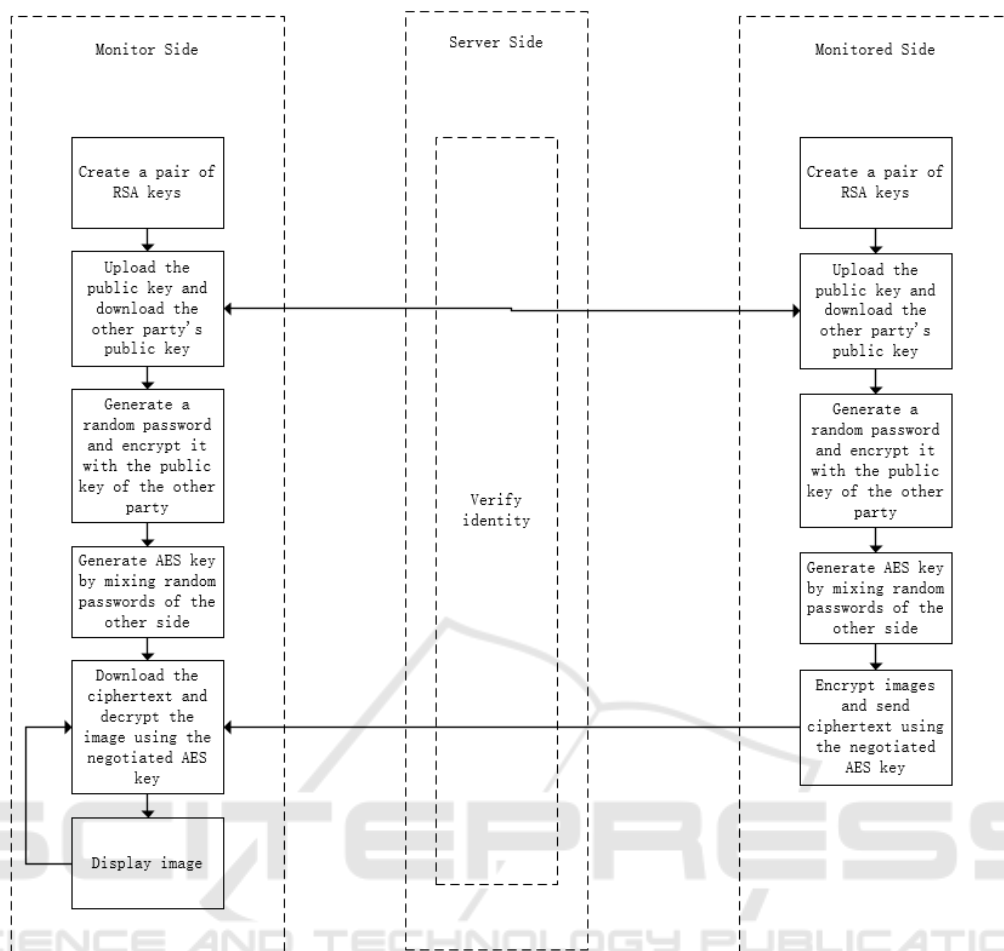


Figure 3: End-to-End Encryption Process.

3.2 Monitoring-Side

The monitoring-side is the user's terminal for remote monitoring and managing laboratory computers. Users can send requests to the server through the monitoring-side to obtain status information, operational logs, and performance data of the monitored computer. The monitoring-side establishes a secure HTTPS connection with the server and gains access rights through identity authentication. Once the connection is established, the monitoring-side can send requests to the server and receive responses. The monitoring-side is also responsible for forwarding user instructions and requests to the monitored-side and transmitting the monitored-side's response back to the server.

3.3 Monitored-Side

The monitored-side represents the computer in the laboratory that requires monitoring and

management. The monitored-side establishes a secure HTTPS connection with the server and gains access rights through identity authentication. Once the connection is established, the monitored-side periodically sends its current status information, operational logs, and performance data to the server. The monitored-side also receives instructions and requests from the monitoring-side and processes them accordingly.

3.4 Data Encryption and Decryption Algorithms

In this remote computer monitoring system, the communication between the server-side and the monitoring-side employs HTTPS protocol, which inherently ensures data transmission security. HTTPS, based on the SSL/TLS protocol, guarantees the confidentiality and integrity of communication. During the establishment of an HTTPS connection, the server-side generates a public-private key pair

and sends the public key to the monitoring-side. The monitoring-side uses the server-side's public key to encrypt data, ensuring only the server-side's private key can decrypt it.

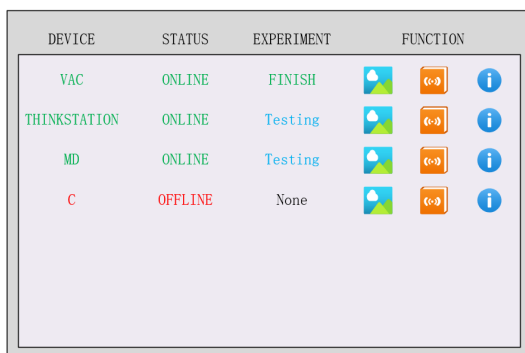
For the end-to-end encryption between the monitoring-side and the monitored-side, the system adopts a hybrid RSA-AES approach. First, the monitoring-side and the monitored-side each generate an RSA public-private key pair. The public keys are used for encrypting data, and the private keys are used for decryption. The monitoring-side and the monitored-side then negotiate the AES encryption key through RSA-encrypted content, which is subsequently used for encrypting data during the communication. All data exchange occurs through HTTPS. The end-to-end encryption process is illustrated in Figure 3.

Through the designed data encryption and decryption algorithms, the system ensures the confidentiality and security of data, achieving end-to-end encryption and decryption. Additionally, combined with the use of HTTPS protocol, the security and integrity of the entire communication process are guaranteed.

4 TESTING AND APPLICATIONS

4.1 System Performance and Stability Testing

Under the condition of one monitoring-side and three monitored-sides, the system operates smoothly with all functions functioning properly. The CPU utilization of the monitored-side does not exceed 20% during monitoring and does not exceed 5% during standby. The system runs continuously for 14 days without any issues, as depicted in the running screenshots in Figure 4.















DEVICE	STATUS	EXPERIMENT	FUNCTION
VAC	ONLINE	FINISH	  
THINKSTATION	ONLINE	Testing	  
MD	ONLINE	Testing	  
C	OFFLINE	None	  

Figure 4: Running Home Screenshots.

4.2 Security Analysis and Evaluation

The system adopts the HTTPS communication protocol, ensuring the confidentiality and integrity of data transmission through SSL/TLS encryption, effectively preventing data tampering or theft. The content exchanged between the monitoring-side and the monitored-side is end-to-end encrypted, ensuring the confidentiality of data during transmission, as only the monitored-side possesses the private key for decryption. Furthermore, an identity authentication mechanism is implemented: the system uses identity authentication to verify the connections of the monitoring-side and the monitored-side, ensuring that only authorized users can access the system and enhancing the system's security.

4.3 System Advantages and Disadvantages

The system achieves remote monitoring and management of laboratory computers through HTTPS communication, allowing users to conveniently access and control computer status and operational conditions, thereby enhancing laboratory management efficiency and flexibility. The adoption of HTTPS communication protocol with SSL/TLS encryption ensures data transmission security, preventing data tampering or theft and enhancing data transmission security. The system employs RSA-AES hybrid end-to-end encryption between the monitoring-side and the monitored-side, ensuring data confidentiality during transmission, as only the monitored-side possesses the private key for decryption, enhancing data transmission confidentiality.

Security relies on algorithms and implementation: The system's security heavily relies on the adopted encryption algorithms and implementation. Vulnerabilities in algorithms or implementation could pose security risks. Real-time monitoring and encrypted data transmission may impose a certain burden on computer resources and network bandwidth, potentially affecting system performance and efficiency. The system emphasizes security considerations and restricts the permissions of the monitored-side, sacrificing certain convenience in remote management operations.

5 CONCLUSION

In conclusion, the remote computer monitoring system based on HTTPS communication demonstrates essential monitoring and management

capabilities in the laboratory environment, characterized by security, encryption, real-time monitoring, and logging. Through the system's design, laboratory computers associated with research instruments can be remotely monitored and managed, with operational logs and performance data recorded to improve laboratory management efficiency. The experiments have proven the system's stability and security, making it well-suited for laboratory computer monitoring and management needs. Future efforts will focus on regular security assessments and performance optimization, further refining security strategies (Al Hasib A, 2008) and encryption algorithms (Xiao Z, 2014) to better meet the high-standard monitoring to satisfy the needs of laboratories.

ACKNOWLEDGMENTS

This work was financially supported by National key research and development plan project "Research on the development and Traceability Method of medical surgical robot positioning phantom", project number: 2022YFC2409605.

REFERENCES

- Chan TJ, Long C, Wang E. The state of virtual surgical planning in maxillary Reconstruction: A systematic review[J]. *Oral Oncology*. 2022;133. <https://doi.org/10.1016/j.oraloncology.2022.106058>
- Nie SL, Gao JH, Ma ZH. An artificial neural network supported performance degradation modeling for electro-hydrostatic actuator[J]. *Journal of the Brazilian Society of Mechanical Sciences and Engineering*. 2022;44(6). <https://doi.org/10.1007/s40430-022-03518-7>
- Norena EC, Munoz GT, Ieee. Remote implementation of a discrete temperature control by hysteresis[C]. 15th International Conference of Technology, *Learning and Teaching of Electronics (TAE)*; 2022. <https://doi.org/10.1109/TAE54169.2022.9840638>
- Al Hasib A, Haque A, Ieee Computer SOC. A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography[C]. *3rd International Conference on Convergence and Hybrid Information Technology (ICCIT 2008)*; 2008,505-510. <https://doi.org/10.1109/ICCIT.2008.179>
- Xiao Z, Hu C, Jiang Z, Chen H. Optimization of AES and RSA algorithm and its mixed encryption system[J]. *Application Research of Computers*. 2014;31(4): 1189-94, 1198. <https://doi.org/10.3969/j.issn.1001-3695.2014.04.056>