Hindawi
International Journal of Distributed Sensor Networks
Volume 2024, Article ID 5699802, 13 pages
https://doi.org/10.1155/2024/5699802

Research Article

An Energy-Saving and Environment-Friendly Networked Intelligent Door Lock System for Offices

A. Wendong Zhao, B. Hao Wang, C. Mengjie Shi, D. Yinghao Li, and E. Yan Ma

School of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223001, Jiangsu, China

Correspondence should be addressed to A. Wendong Zhao; 11000418@hyit.edu.cn

Received 19 April 2023; Revised 29 November 2023; Accepted 30 November 2023; Published 8 January 2024

Academic Editor: Saeed Olyaee

With the development of IoT technology and the improvement of people's living standards, smart locks have become prevalent in ordinary households. However, for enterprises and institutions requiring unified management and control capabilities for networked smart locks, the technology has been relatively lagging, and there is a lack of established brands. Existing products are mostly based on wireless low-power network protocols, leading to common issues of low stability, limited network scalability, and high maintenance efforts. This paper addresses the problems existing in current networked lock systems and leverages the centralized office characteristics of enterprises and institutions. By integrating IoT technology and Power over Ethernet- (PoE-) centralized power supply, we have developed a networked smart lock system with unified management and control capabilities. This system is primarily designed for applications in offices, collective dormitories, and hotels of enterprises, institutions, and schools. The test results demonstrate that even with a scale of over tens of thousands of networked locks under unified control, the system maintains fast response times and low packet loss rates. It also incorporates energy-saving and environmentally friendly features, as well as easy automatic updates, facilitating convenient postdeployment maintenance. Thus, it effectively meets the requirements for centralized management and control in different application scenarios with centralized use of rooms. In conclusion, this research has led to the development of a unified management and control networked smart lock system, which is well suited for enterprises, institutions, and schools. Its scalability, speed, energy efficiency, and ease of maintenance make it an excellent solution for various application scenarios requiring centralized management and control of access.

1. Introduction

The development history of intelligent energy-saving office environments can be traced back several decades. With the continuous advancement of technology and the growing awareness of sustainability, research and practices in this area have gradually increased. In the last three years, researchers have conducted in-depth studies on intelligent energy-saving offices, aiming to achieve intelligent management and energy optimization in office spaces. Currently, potential options include raising energy awareness and optimizing the operation of electrical appliances within buildings [1].

Giacobbe et al. proposed an approach to implement the concept of "smart office," called the SmartMe Energy system. This system is based on the Internet of Things (IoT) and intelligent technology, aiming to provide intelligent, efficient, and sustainable office energy management solutions [2]. Li integrated key technologies such as IoT, sensor technology, and artificial intelligence to provide a smart office environment control and management solution, presenting a novel comprehensive office automation system [3]. Sayed et al. explored the application of intelligent edge recommendation systems in office energy management. By utilizing IoT and AI technologies, this system can provide personalized energy recommendations and optimization based on office energy demand and user behavior [4]. In addition to relying on energy demand and user behavior, Elkholy et al. proposed a real-time intelligent home management system for office environments, which combines real-time data monitoring, intelligent control, and energy optimization

technologies, aiming to achieve energy efficiency and intelligent management in office spaces. However, managing too many sensors can be troublesome [5]. Copiaco et al. used energy time series images for building energy consumption deep anomaly detection. Their approach transforms energy time series data into image representations and utilizes deep learning techniques for anomaly detection, as opposed to traditional methods that rely on sensor data or energy time series data [6].

After studying the overall control of intelligent energy-saving office environments, researchers started focusing on the facilities and equipment within offices, including door lock systems. With the continuous advancement of technology and the maturity of intelligent solutions, smart door locks have become an important component of intelligent offices. Since the 1970s, electronic communication technology has rapidly evolved, and door locks have transitioned from mechanical locks to various types [7]. In the 1990s, smart lock systems based on hidden induction card (HID) technology began to emerge [8]. In 1990, S.R. Vishnubhotra and D.C. Poirier designed a microprocessor-based password lock system. By 1995, RFID technology had matured, leading to the rapid development of contactless access cards. In the early 21st century, electronic technology in Europe and America became more mature, and electronic password locks started being used in intelligent access control systems [9]. Initially, password locks were used in places like safes and vaults. With technological advancements and the maturity of smart lock solutions [9], high-security and technologically advanced electronic locks have been widely used in countries like the United States, the United Kingdom, and Singapore [10]. There are numerous smart lock manufacturers, such as OWQ smart locks from Germany, Samsung smart locks from South Korea, the renowned security-oriented Mul-T-Lock smart locks from Israel, and Doreen smart locks from the United States.

However, it is easy to observe that current smart locks in the market mainly target ordinary households [11, 12], and the management and control of locks must be executed on the respective locks, lacking a unified management and control platform. Networked locks for enterprises and organizations are still relatively rare [13], with existing networked locks primarily relying on wireless networks and RS485 technology.

Currently, the development faces the following challenges:

The instability of wireless networks makes wireless network locks less reliable and troubleshooting challenging, requiring professional personnel and resulting in high maintenance costs. Due to factors such as the transmission distance and signal interference of wireless networks, the scale of centrally managed wireless locks is limited. Wireless smart locks typically use traditional 5 V batteries as power sources, and traditional batteries are not environmentally friendly. The existing wireless network lock power supply method no longer meets the requirements for energy saving and environmental protection. Existing wireless network locks support mobile NFC card unlocking, providing convenience for ordinary household users. However, in the office environment of enterprises and organizations, the security of user access card numbers can be compromised, as they can be copied and used by unauthorized users to open doors. Existing networked locks cannot exchange information in real-time with the enterprise or organization's access control platform. The current networked smart locks use a predetermined interface with the enterprise's access control platform to update user IC card numbers. Therefore, if a user loses their IC card and obtains a new one, they cannot immediately unlock and enter their office. The access control system and the access control platform must update information at specified times before the user can refresh their card to unlock the door, leading to a poor user experience for such users. Smart locks are powered by batteries, and basic models usually install 4/5 batteries in the battery compartment. They need to be replaced every 3-6 months. If the battery life is not noticed, or if the owner does not replace them in several months, they may find that the smart lock has lost power when trying to open the door, which can be frustrating [14]. Locks based on RS485 technology are limited by short communication distances and cannot have too many locks. They also face issues of periodic battery updates and high equipment failure rates. Moreover, both types of networked locks require professional installation and maintenance, resulting in high maintenance costs [15–17]. To address the above issues, this paper proposes a design solution for networked smart locks suitable for enterprise or institutional offices, building upon the existing local area network. It comprehensively utilizes UDP protocol, IoT technology, fingerprint recognition technology, and Power over Ethernet- (PoE-) centralized power supply technology [18–21] to achieve centralized management and control of locks. This design not only resolves the existing issues with wireless network locks but also meets the requirements for energy saving and environmental protection advocated by the country. The main contributions of this paper are as follows:

(1) Proposing a new door lock system solution that effectively expands the scope and effectiveness of smart door lock usage in large-scale application scenarios

(2) The newly proposed optimized UDP method demonstrates significant advantages in speed and range compared to TCP communication

The rest of the paper is organized as follows: Section 2 is dedicated to system design, including the proposed system's use case diagram, the UDP optimization algorithm, and the system flowchart. Section 3 covers the application and development of the website and app. Testing is conducted in Section 4, and the conclusions are presented in Section 5.

2. Design of Networked Smart Door Locks Based on PoE-Centralized Power Supply Technology

To bring about excellent user experience, smart door locks for office rooms must not only realize the centralized management and control of door locks but also facilitate ease of daily use. To this end, the article is aimed at achieving

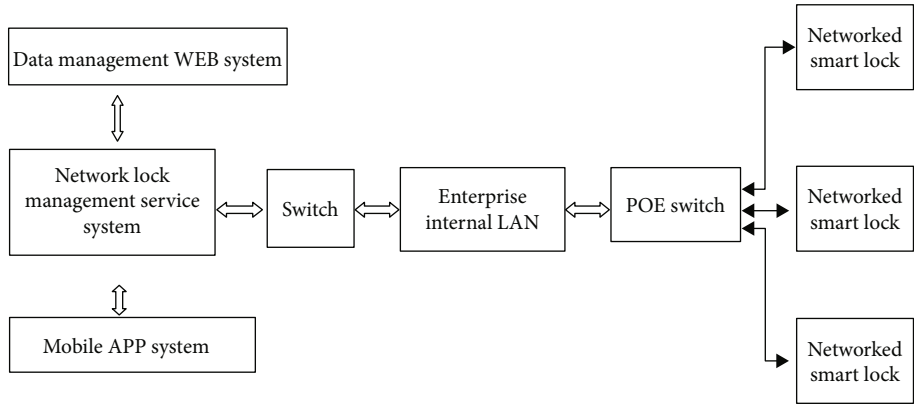

Figure 1: Overall structure diagram of the system.

the following design goals from the application requirements of university laboratory access control management:

(1) As all teachers and students in the school have IC cards, it is necessary to swipe the IC card to open the door

(2) The campus environment is a public place that must meet the needs of fire safety management

(3) The design must feature a mobile terminal self-service unlocking function

(4) The system adopts the existing network environment of the campus, which is in line with the environmental protection concept of energy saving and low carbon emission

(5) The unlock record can be checked any time

(6) The system can connect to the campus card platform and educational system in real time but does not add too much load to the existing network

On the basis of the above design goals, it is also necessary to avoid the existing problem of networked door locks. Based on IoT, fingerprint identification, and PoE-centralized power supply technologies, this article designs an energy-saving and environmentally friendly networked door lock for office rooms. The overall design diagram is shown in Figure 1.

From the structure diagram of the networked smart door lock shown in Figure 1, we can see that the smart door lock is connected to the PoE switch through a wired network cable, which in turn is connected to the smart door lock-centralized management server through a local area network. PoE switches provide data exchange for door locks as well as power supply support. This helps achieve centralized management and control of power supply, meets the environmental protection requirements advocated by the state, and does not pollute the environment during use.

2.1. Use Case Diagram. The use case diagram of the system includes three main actors: office manager, administrator, and employee. Each of these actors has different use cases that allow them to interact with the system in various ways.

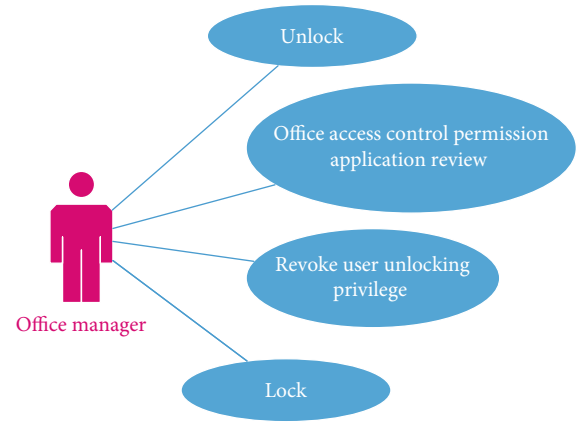

Figure 2: Use case diagram for the office manager.

2.1.1. Office Manager. As an office manager, the user can perform the following use cases:

(i) Lock/unlock door: the office manager can lock or unlock the office door using a physical key or the smart lock system

(ii) Office access request approval: the office manager is responsible for reviewing and approving access requests from employees. They can approve or deny access to individual users based on their job roles or other criteria

(iii) Revoke user access: the office manager can revoke access to the office for any user who no longer needs access

The use case diagram for office manager is shown in Figure 2.

2.1.2. Administrator. As an administrator, the user can perform the following use cases:

(i) Room management: the administrator can manage the rooms in the building, including adding or removing rooms and assigning room access to users

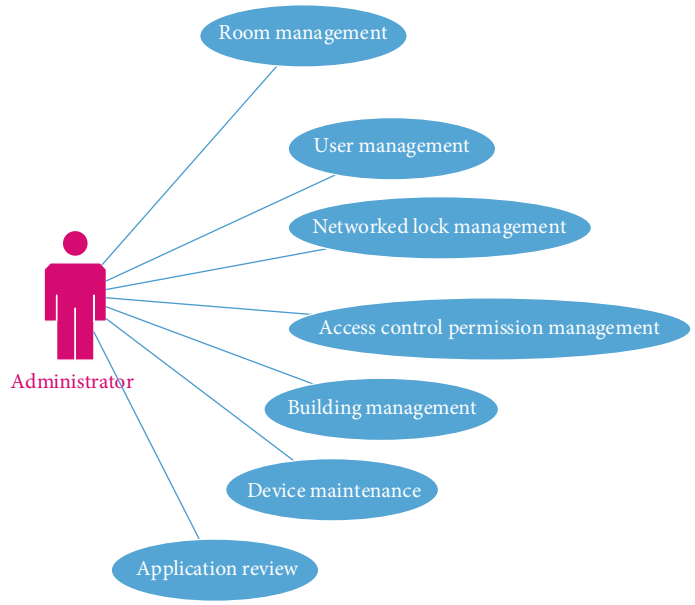

Figure 3: Use case diagram for the administrator.

(ii) User management: the administrator can manage the users in the system, including adding or removing users, assigning roles, and resetting passwords

(iii) Networked lock management: the administrator can manage the networked locks, including setting up new locks and configuring access permissions

(iv) Building management: the administrator can manage the building's security systems, including alarms and surveillance cameras

(v) Access permission management: the administrator can manage access permissions for individual users or groups of users

(vi) Device maintenance: the administrator is responsible for maintaining the hardware and software of the security system

(vii) Access request approval: the administrator reviews and approves access requests from employees, ensuring that only authorized personnel can access the building

The use case diagram for the administrator is shown in Figure 3.

2.1.3. Employee. As an employee, the user can perform the following use cases:

(i) Lock/unlock door: the employee can lock or unlock the office door using a physical key or the smart lock system

(ii) Office access request: the employee can request access to the office by submitting an access request to the office manager

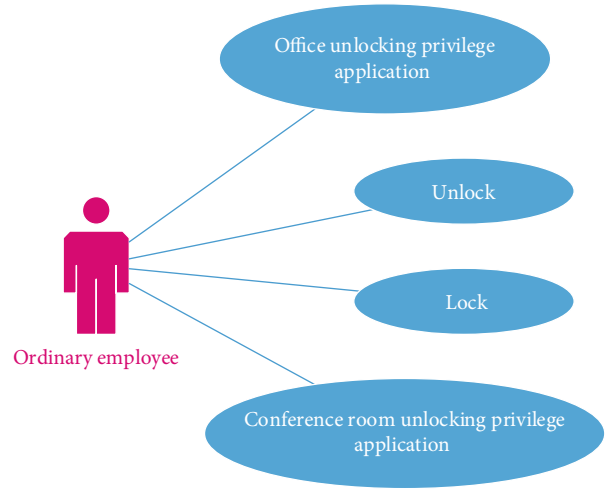

Figure 4: Use case diagram for the employee.

(iii) Meeting room access request: the employee can request access to a meeting room by submitting an access request to the office manager

The use case diagram for the employee is shown in Figure 4.

2.2. Improvement Algorithm of UDP Protocol Based on Confirmation Mechanism. Compared with the TCP transmission protocol, the UDP protocol has the advantages of low network resource consumption and fast processing speed and does not need to establish a connection. The disadvantage, however, is that it cannot guarantee the reliability of data transmission. Therefore, to ensure that the smart door lock will receive the card opening information every time, which is then reliably transmitted to the door lock management server, we added a confirmation mechanism between the access control panel and the door lock

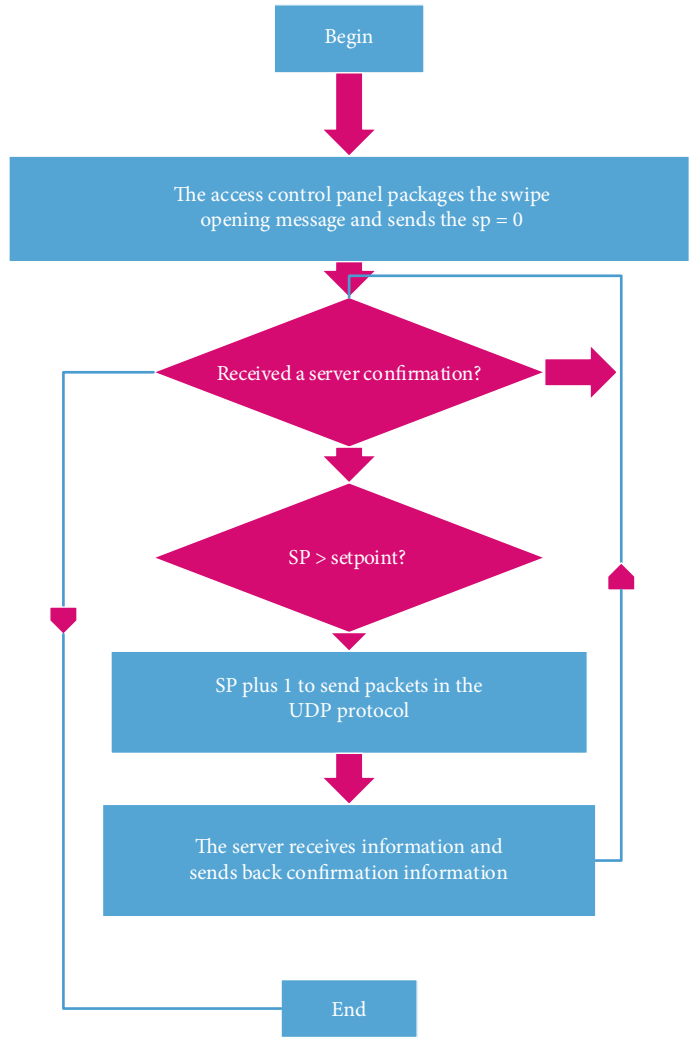

Figure 5: UDP protocol improvement algorithm based on the confirmation mechanism.

management server based on the UDP transmission protocol. The specific communication algorithm flow is shown in Figure 5.

The data transmission between intelligent door lock control panel and smart door lock management servers is described as follows:

(1) When the door lock control panel collects a swipe card unlocking information, it first finds out whether the white list of the card number exists locally. If it does not exist, the access control panel will type the IP address, physical card number, and data packet number of the lock into a data packet. Then, it sets the counter that marks the transmission times of the data packet (assuming SP) to 0 and then starts to send the data packet to the door lock management server with the UDP protocol

(2) After the specified time, the access control panel receives the confirmation message that the door lock server has received the data packet. Then, it proceeds to step (5). Otherwise, it continues to step (3)

(3) If the SP is still less than or equal to the set number of times, 1 is added to the SP, and the access control panel continues to send the same data packet to the door lock management server through the network with the UDP protocol; if the SP is greater than the set number of times, then it proceeds to step (5)

(4) After receiving the data packet from the door lock control panel, the door lock management server sends back a confirmation message to the door lock control panel. Then, it turns to step (2)

(5) Once the algorithm ends, the card reader can receive the next card swipe

The UDP protocol improvement algorithm based on the confirmation mechanism shown in Figure 5 can not only be used to transmit the data in the door lock control panel to the door lock management server but also realize that the door lock management server sends control instructions to the door lock. This helps realize the unified management and control of networked door locks at the service management end. Meanwhile, the requirements for the network are

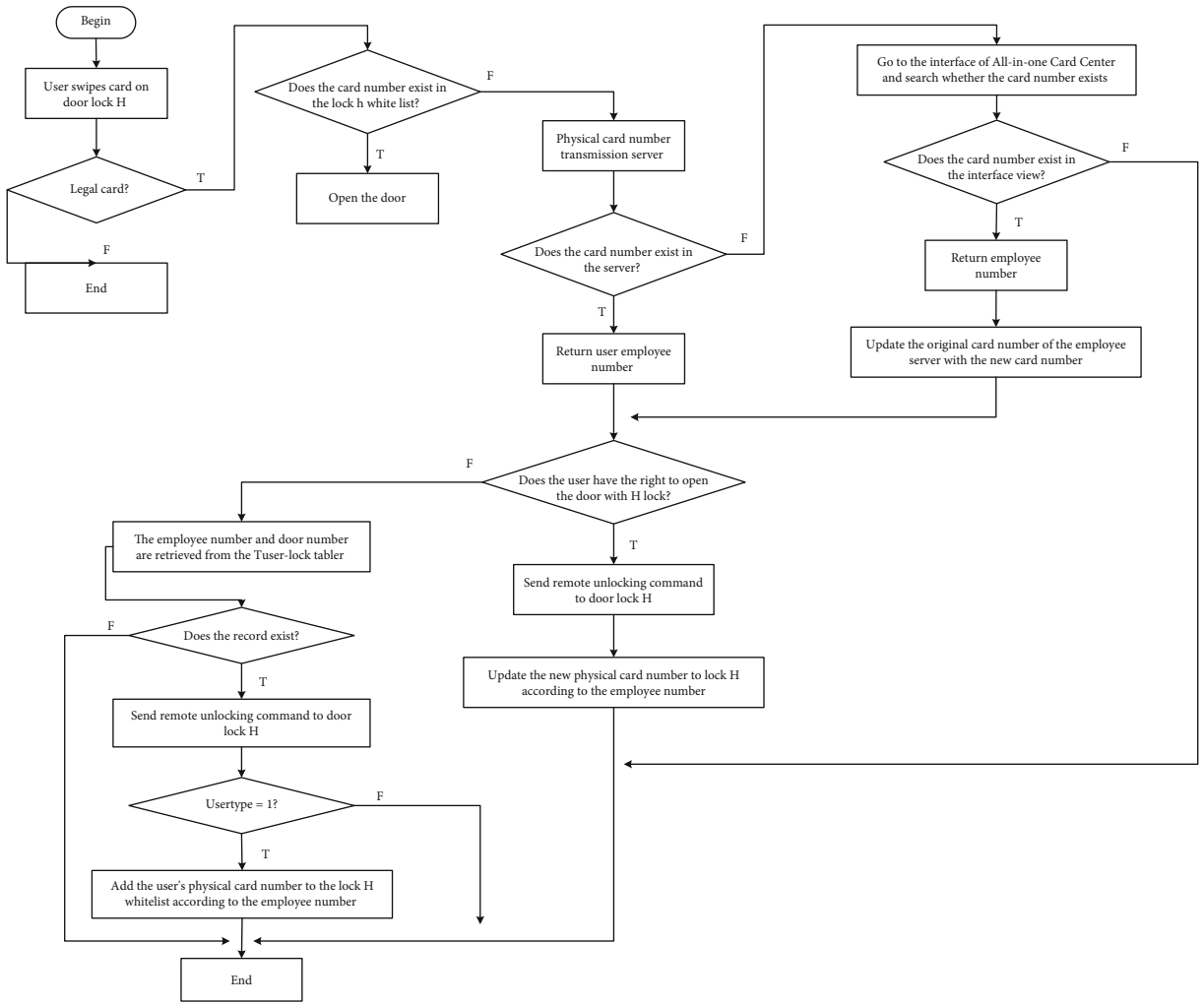

Figure 6: Flowchart of unlocking procedure.

not too high, and it does not add too much network load to the existing network.

2.3. Design of Access Control Panel Based on ARM Technology. On the basis of the overall structure diagram shown in Figure 1 and in accordance with the application requirements of university laboratory access control management, the control process shown in Figure 6 is designed. This helps realize the centralized control and management of door locks and actively connects to the All-In-One card platform according to real-time needs. Furthermore, it realizes the real-time unlocking operation of the user after the card is replenished and does not add more load to the network due to the regular updating of all data. When the user swipes the IC card in the door lock, the legitimacy of the IC card must be verified first. If it is an illegal card, it will not respond. If it is a legal card, the system will judge whether its physical card number exists in the local white list. The door opens when the number exists and is thus verified. If it does not exist, the physical card number is submitted to the door lock server, and the server will decide whether or not to open the door. Specifically, the following situations exist when a user swipes a card to unlock a door:

(1) A user swipes the card to open the door, after which the access control panel of the door lock compares the collected card number with the white list in the control panel memory. If the card number exists in the local white list, the door lock is opened, and the access control panel can flash green light prompts. It then submits an unlocking record to the door lock management server at the same time. The system proceeds to (7) to execute; otherwise, it continues to execute downward

(2) When a user's card number does not exist in the white list of the door lock control panel, based on the improved UDP protocol, the access control panel will transmit the card number to the door lock management server through the network. After receiving the card number, the door lock management server will check whether the card number has the right to open the door in the white list of the server. If it exists, it proceeds to (3) to execute; otherwise, it goes to (4) to execute

(3) The door lock management server sends the unlocking command to the designated access control panel. Once

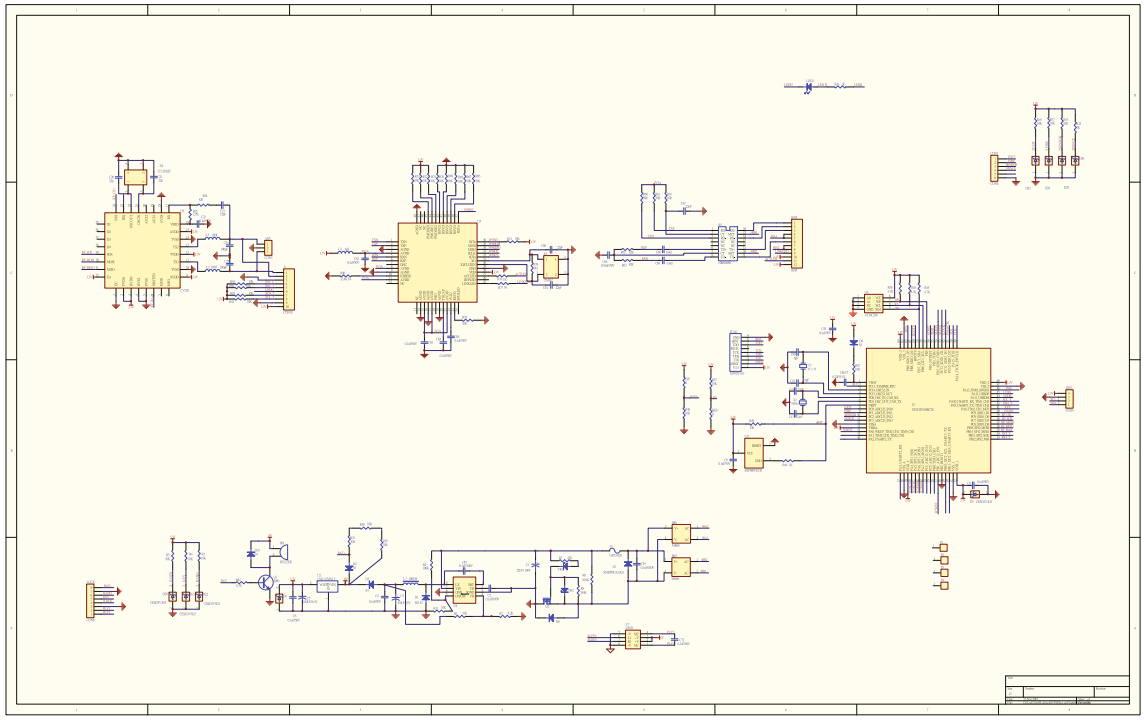

Figure 7: Schematic diagram of the proposed access control panel.

the unlocking command is received from the server, the access control panel can flash a green light to prompt to unlock the door. At the same time, an unlock record of this user is saved in the door lock management server. The system them turns to (7) to execute

(4) When the card number does not gain the right to open the door in the door lock management service, the door lock management server will look up the user information of the card number through the data interface provided by the All-In-One card center. If the information of this card number does not exist in the interface, the system then turns to (6) to execute; otherwise, it continues to execute downward

(5) According to the user information corresponding to the card number in the interface, the system initially updates the card number of the user in the system with the new card number. Then, it checks whether the user has the right to unlock the door in system. If so, the card number is updated to the white list to which the access control panel of this door corresponds and then goes to (3) to execute; otherwise, it continues to execute downward

(6) For illegal or unauthorized users, the access control panel can flash a red light to prompt and continue to execute downwards

(7) The process is completed

According to the construction needs of the laboratory and the frequent flow of personnel in the innovation laboratory, the paper divides cardholders into lock-end and server-end white-listed users. The user's card number can be saved in the white list of the access control panel belonging to the office door lock if the user is fixed in an office for a long time. Even if there is no network, the user can directly open the office door lock with the card. In giving a user temporary right to unlock a laboratory or office, for example, a teacher must be able to unlock the door of the corresponding laboratory according to the experiment schedule, the system can store the user information in the white list on the server side according to the schedule. This is a convenient way for a system to update the academic schedule according to the students' needs. When this user type unlocks door, it must have the support of the network. According to the unlocking process, it can also be seen that the system updates the user's card number synchronously when the user holds the card to open the door. Thus, the door lock service system actively updates the card number information of the user who just applied for the new card through the interface of the All-In-One card center, and other types of user information do not need to be updated. This reduces the system workload and the network load and, most importantly, allows new card replacement users to unlock office doors immediately without waiting.

2.4. Design of the Access Control Panel Based on ARM Technology. To achieve the unlocking control process shown in Figure 6, the article designs the access control panel shown in Figure 7 to control the opening and closing of the motor lock body based on ARM technology. The access control panel and the door lock service management end transmit data through the improved UDP protocol, thereby realizing unified management and control of door locks

through a door lock management server. The access control panel specifically completes the following functions:

(1) If the card-swiping user is a white-listed user in the lock or receives an unlock instruction from the door lock service, the access control panel will drive the motor to rotate forward, open the door lock, and flash a green light to prompt. Then, it automatically closes the door lock after 5 seconds

(2) If the unlocking mode is set to open normally, or when the command from the server is normally open, the access control panel will drive the motor to open the lock. In particular, the access control panel will drive the motor to reverse and close the door lock again until the white-listed user swipes the card again or receives an unlock message from the door lock server. This allows the office door lock to have a normally open function, which meets the needs of safety management in public places

(3) In turning off the door lock, when it is in the normally open state, or when the lock command is received from the door lock server, the access control panel will drive the motor to reverse and close the door lock

(4) The mobile terminal NFC-simulated card number unlocking function is disabled to ensure the access control security of the office environment. The specific implementation principle is to first design an algorithm and then use it to convert the card number of each card into a new 8-byte hexadecimal sequence and save it to the designated location of the card for storage. When the user holds the card to open the door, the access control panel will first read the number of the card and then use the same algorithm to convert it to obtain an 8-byte data sequence, which in turn is compared with the data stored in the designated position of the card. If it is equal, the door lock can be opened; otherwise, it can be judged as NFC simulation cards or unauthorized cards. A red light prompt can signal a refusal to open the door

(5) The access control panel drives the motor to rotate forward, and after holding the connecting rod of the motor lock body, it will submit a door-opening record to the service through the network for future reference once it detected that the door lock handle is pressed down

(6) If the card number for swiping the card to open the door does not exist in the white list of the control panel, it will be sent to the door lock server through the network for processing. Then, the door lock will be determined according to the instruction returned by the server

(7) In the event of a network disconnection or an offline state, the access control panel, as it cannot receive instructions from the online lock management system, is unable to be centrally managed and controlled by the management system. However, it can operate independently. During this time, only users on the lock's white list can use IC cards to unlock or lock the door. In the case of a power outage due to special circumstances, users can use a mechanical key to unlock and lock the door

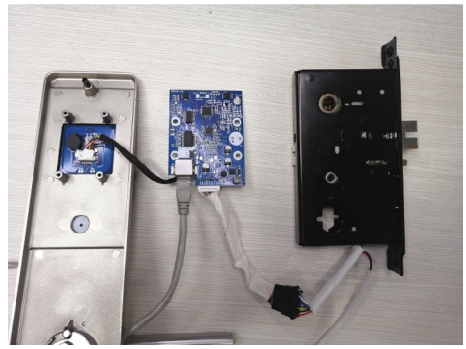

Figure 8: Connection diagram of the access control panel and lock body.

In addition, to prevent damaging the electromagnetic pulse to the control board, two measures of protection step-down and power isolation have been adopted. At present, the power supply provided by the PoE switch is a standard 48 V power supply. We added a PoE splitter at the front of the control board to reduce the 48 V voltage to 9 V and provide it to the control board through the RJ45 port together with the data information. Hence, the power signals and control logic unit ground information are separated. Through these two measures, the damage to the control panel by the surge signal is solved, and the service life of the control panel is ensured.

2.5. Optimization of Middleware Data Messages. At present, solutions involving cross-platform, heterogeneous architecture and multisystem integration are generally implemented through middleware, and each system module communicates through JSON format messages provided by the middleware. Therefore, the transmission efficiency of JSON messages is critical. The data elements and embedded objects in the commonly used JSON messages have the same attribute names, and similar repetitions increase the size of the JSON text, inevitably reducing the efficiency of data packet transmission. To improve the transmission efficiency of JSON messages, the paper [22] proposes a new JSON message syntax format. The core idea is to flatten the JSON objects with obvious hierarchical relationships and extract the keys common to all JavaBean objects. The template and preset key values are entered into the corresponding values according to specific rules, and the real data in the JavaBean object is flattened into an ordinary data array.

The JSON array object now includes the JavaBean object, and the overhead formula of its data transmission is expressed as

$$\sum_{k=1}^{m}\sum_{j=1}^{n}\left(A_k + D_{k,j} + L\right), \tag{1}$$

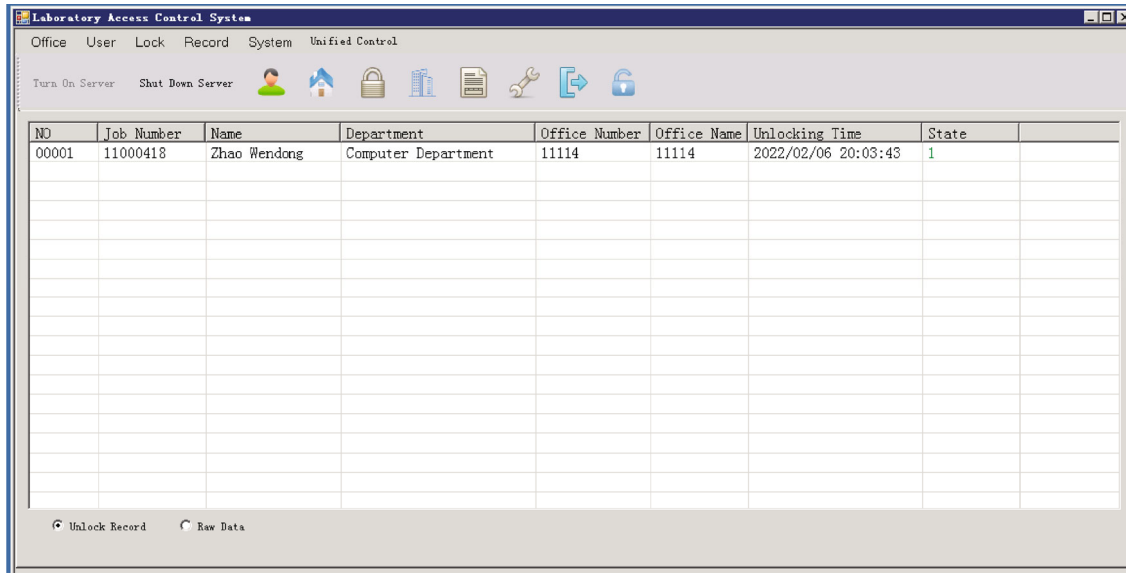

Figure 9: C/S structure networked door lock management system.

where A_k represent the length of the kth attribute of the JSON array element object, where $k \in 1, 2, 3, 4, \cdots, m$; let $D_{k,j}$ represent the data length corresponding to the kth attribute of the jth array element object, where $j \in 1, 2, 3, 4, \cdots, n$; and let L represent the character length of the key of the JSON array object. Due to the JSON syntax, A_k can be added repeatedly, thus increasing the data transfer overhead.

Therefore, we can perform flattening processing on the basis of formula (1). The flattening processing formula is shown as follows:

$$\sum_{k=1}^{m}\sum_{j=1}^{n} D_{k,j} + \sum_{k=1}^{m} A_k + L + \mathrm{tL}, \tag{2}$$

where tL represents the length of the extracted common template.

It can be seen from the experimental results that although the optimized data maintain the original overhead, the JSON text is transformed from the original two superpositions to just one traversal addition. Therefore, according to the optimization process of Equation (2), the JSON format can be changed. In particular, the message length is reduced, thereby improving the data transmission efficiency [23, 24].

3. Realization of Networked Intelligent Door Lock System Based on PoE-Centralized Power Supply Technology

3.1. Smart Door Lock Based on PoE Technology. According to the electrical characteristics shown in Figure 7, the article integrates the access control panel supported by data and power from the PoE switch. The connection between the access control panel and the electric lock, shown in Figure 8, is integrated into ARM's RealView Developer Suite. In the development environment, C++ language is used to realize the software control program of the access control panel.

3.2. Intelligent Door Lock Network Management Service System. According to the unlocking program flow shown in Figure 6 and combined with the functional characteristics of the door lock control panel shown in Figure 7, the article encapsulates the user's functions into classes in the .Net environment. Then, based on the three-tier architecture pattern and object-oriented programming method, the networked door lock management system of C/S structure is realized. The specific function interface is shown in Figure 9.

In the networked door lock management system shown in Figure 9, room, user, and card issuance management can be achieved, along with door lock settings and status browsing, remote control and network testing, and unlocking records and operating status. It also contains control programs of interfaces that facilitate the connection of third-party software.

According to the electrical characteristics shown in Figure 7, the article integrates the access control panel supported by data and power from the PoE switch. The connection between the access control panel and the electric lock, shown in Figure 5, is integrated into ARM's RealView Developer Suite. In the development environment, C++ language is used to realize the software control program of the access control panel.

3.3. Networked Door Lock Management System Based on B/S Structure. The management system based on the C/S structure is not convenient for daily management, so the interface program provided by our system realizes the networked door lock management system based on the B/S structure. The functional interface is shown in Figure 10. In this way, managers can break through the constraints of time and space and achieve the daily management functions of access control.

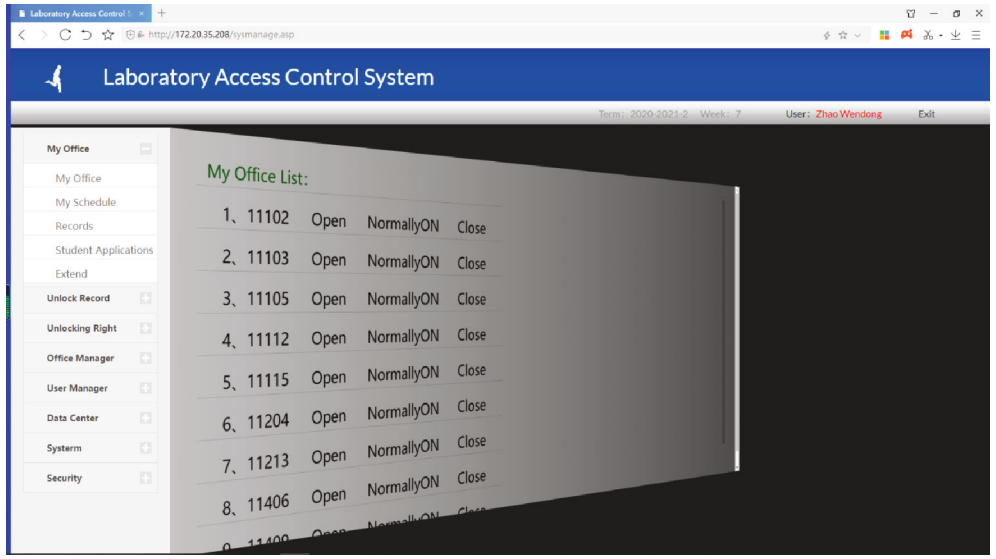

Figure 10: B/S structure networked door lock management system.

In the laboratory access control management system shown in Figure 10, managers can realize various functions, such as basic user and room information management, office application and review, allocation and cancelation of room door rights, management of room responsible persons, system management rights monitoring, and various online basic functions, such as opening and closing doors.

3.4. Access Control Self-Service Unlocking System APP. With the aim of facilitating the daily use of end users, through the interface program provided by the door lock management service system, this article develops an access control self-service unlocking APP system based on HTML5 technology. The interface after operation is shown in Figure 11.

As can be seen, on the mobile terminal, users can implement common functions, such as office and conference room applications, self-service unlocking, and unlocking record browsing. At the same time, room administrators can implement management functions, such as reviewing office applications and canceling housing rights on the basis of ordinary user functions. The administrators can also realize the common functions of the management of the person in charge of the office and the management of the department's authority on the basis of the room administrator function.

4. Door Lock System Testing

The article tested the system's load capacity and functional reliability based on actual application requirements.

4.1. Device Load Testing. Load testing is critical to ensure that devices can operate normally under high-concurrency and high-traffic scenarios. Typically, it involves gradually increasing the number of concurrent requests until the predetermined high-load level is reached and analyzing the system's response time, error rate, and resource utilization rate under different load conditions. The article used JMeter to

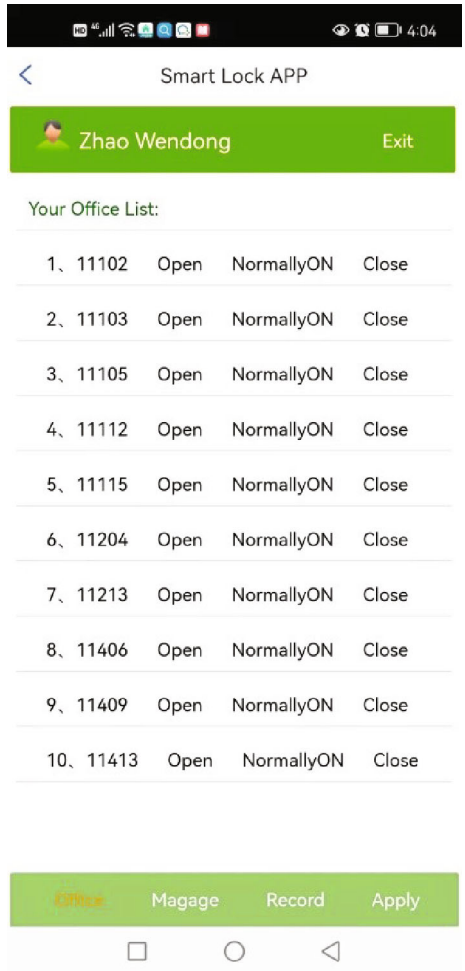

Figure 11: UDP protocol improvement algorithm based on the confirmation mechanism.

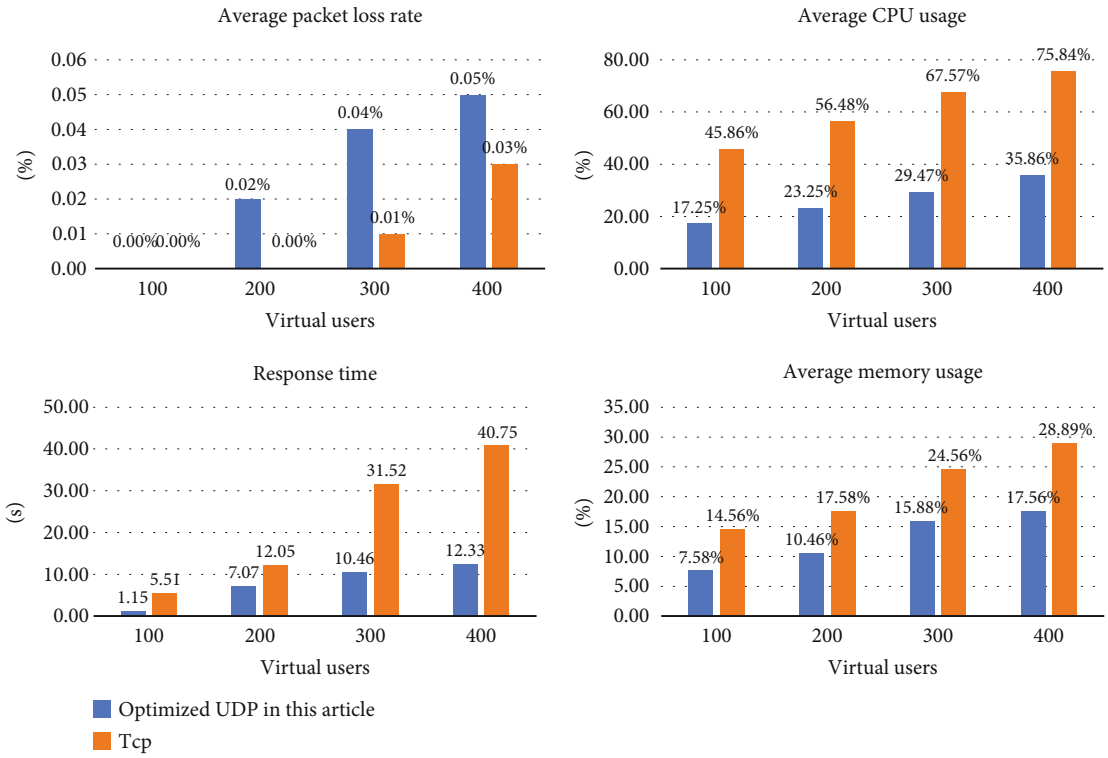

Figure 12: Comparison results of load testing with different communication protocols.

Table 1: Functional reliability test table.

Function test	All tested functional modules
Test steps	(1) Continuously parse a set of data packets for 50 rounds
	(2) Complete scanning of the lock port for 50 rounds
	(3) Continuous testing of the "unlock" and "lock" functions for 50 rounds
Expected results	(1) The validation results of 50 rounds of parsed data packets should be consistent, and incorrect data should be filtered
	(2) The scan results of 50 rounds should be consistent without missing or added ports
	(3) There should be no simultaneous "unlock" and "lock" situations after 50 rounds of testing
Actual results	(1) The processing results of 50 rounds of data should be consistent without errors
	(2) The scan results of 50 rounds should be consistent without missing ports
	(3) There should be no simultaneous "unlock" and "lock" situations after 50 rounds of repeated operations
Test conclusion	The testing meets the expected criteria and has passed

simulate client requests and send concurrent requests to the networked lock service system, gradually increasing from 100 concurrent users. At each load level, requests were continuously sent for a period of time, and data from the service management system was collected and compared with TCP communication. The test results are shown in Figure 12.

From Figure 12, it can be seen that the UDP communication algorithm based on confirmation mechanism proposed in the article is faster than the TCP protocol in transmission speed when the data packet is less than 1000 KB. Moreover, even when the load increases, the system response speed remains stable and fast, meeting the requirement of fast response capability for small data packet transmission in the networked lock system.

4.2. Functional Reliability Testing. To test the system's reliability, the article conducted multiple scans and detections on the data analysis module and communication ports, eliminating the randomness of a single detection. The test results are shown in Table 1.

The results shown in Table 1 indicate that the reliability of the tested functional modules has met the expected requirements and can meet practical applications.

After multiple rounds of scanning and testing, the data analysis module and communication ports of the system have demonstrated excellent reliability. During the testing process, the data analysis module was subjected to continuous parsing of a data packet set for 50 rounds, and the results showed consistent and error-free data processing in all 50 rounds, confirming the reliability of the module in handling

data. In the testing of door lock ports, a complete scan was performed for 50 rounds, and the results showed consistent scanning results without any missing ports, confirming the stability of the communication ports. Additionally, through 50 rounds of continuous testing of the "unlock" and "lock" functions, it was observed that no instances of concurrent "unlock" and "lock" operations occurred, demonstrating the reliability of the functional operations.

These testing results validate the system's reliability in terms of data analysis, communication ports, and functional operations. The consistent processing results and error-free performance of the data analysis module indicate its ability to consistently provide accurate results, ensuring high credibility. The stability of the communication ports ensures normal communication with external devices and further ensures the overall reliability of the system by preventing any port deficiencies. The reliability of functional operations indicates that the system can perform "unlock" and "lock" functions correctly without conflicts or errors. In conclusion, through multiple rounds of scanning and testing of the data analysis module and communication ports, the system exhibits consistent and expected reliability in functional aspects. The successful results of these reliability tests provide strong support for the service management system's ability to respond to networked lock application requests in real time and accommodate the networking scale effectively.

5. Conclusions

This paper presents the design and implementation of a networked smart lock system suitable for centralized office use in enterprises and institutions, integrating IoT and Power over Ethernet- (PoE-) centralized power supply technologies. Addressing the issues of low stability, limited capacity, and high maintenance costs observed in wireless networked door locks on the market, the proposed system utilizes a networked lock service management system that connects the web-based management system, mobile app system, and networked smart locks, forming a unified whole. By linking previously independent devices and personnel into a digital network, the system achieves unified management, centralized authentication, flexible authorization, statistical analysis, and traceability functionalities. This solution not only realizes unified management of people and assets but also enables centralized and refined management of dispersed and aggregated housing assets, supporting intelligent and efficient management of enterprise offices. The application results demonstrate that the designed networked smart lock system exhibits high stability, ease of postdeployment maintenance, low maintenance costs, and energy efficiency and incorporates a certain level of artificial intelligence. When users use a newly issued IC card to unlock, the system can proactively update user information through the information center's interface, ensuring that the newly issued IC card can be used for immediate unlocking. As a result, the proposed networked smart lock system shows promising application prospects and significant economic benefits.

Currently, the system can assist enterprises in achieving unified management and control of all networked locks through a single server. However, the unlocking methods provided to users are relatively limited, as users can only use IC cards or the app for unlocking. Additionally, when faults occur in the networked lock terminals, management personnel can only discover the issues through user feedback or by actively checking in the service management system. The next step is to integrate biometric technology with the existing system, providing users with fingerprint unlocking, facial recognition unlocking, and other more user-friendly application requirements. Moreover, adding the capability for networked smart terminals to actively report abnormal situations to servers or management personnel's mobile devices will enhance postdeployment maintenance efficiency.

Data Availability

The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Jiangsu Province Industry-University-Research Cooperation Project (BY2020289).

References

[1] Y. Himeur, K. Ghanem, A. Al-salemi, F. Bensaali, and A. Amira, "Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives," *Applied Energy*, vol. 287, article 116601, 2021.

[2] M. Giacobbe, G. Pellegrino, M. Scarpa, and A. Puliafito, "An approach to implement the "Smart office" idea: the #SmartMe Energy system," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–19, 2018.

[3] H. Li, "A novel design for a comprehensive smart automation system for the office environment," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, pp. 1–4, Barcelona, Spain, 2014.

[4] A. Sayed, Y. Himeur, A. Alsalemi, F. Bensaali, and A. Amira, "Intelligent edge-based recommender system for Internet of energy applications," *IEEE Systems Journal*, vol. 16, no. 3, pp. 5001–5010, 2022.

[5] M. H. Elkholy, T. Senjyu, M. E. Lotfy, A. Elgarhy, N. S. Ali, and T. S. Gaafar, "Design and implementation of a real-time smart home management system considering energy saving," *Sustainability*, vol. 14, no. 21, article 13840, 2022.

[6] A. Copiaco, Y. Himeur, A. Amira et al., "An innovative deep anomaly detection of building energy consumption using energy time-series images," *Engineering Applications of Artificial Intelligence*, vol. 119, article 105775, 2023.

[7] Q. Chi, *Design and implementation of intelligent door lock system based on cloud platform, [M.S. thesis]*, Xidian University, 2021.

[8] Y. Yun, "Analysis of the application of information security technology in electronic anti-theft locks," *China Security Technology and Application*, vol. 4, pp. 1–136, 2019.

[9] R. Doss, R. Trujillo-Rasua, and S. Piramuthu, "Secure attribute-based search in RFID-based inventory control systems," *Decision Support Systems*, vol. 132, pp. 113270–113270, 2020.

[10] H. A. Taslim, N. A. M. Lazam, and N. A. M. Yahya, "Development of Smart Home Door Lock System," in *International Conference on Innovative Technology, Engineering and Science*, Springer, Cham, 2020.

[11] C. H. Zhentao Z. Xianyu et al., "Research on the application of intelligent access control based on Internet of things technology in smart community," *Police Technology*, vol. 6, pp. 8–10, 2019.

[12] Z. Zhentao, Z. Xinyu, and W. Junxiu, "Research on the application of intelligent access control based on internet of things technology in smart community," *Police Technology*, vol. 6, no. 3, 2019.

[13] P. J. Zhu, Z. M. Lin, and S. He, "Current status and security protection of intelligent door lock products," *Quality and Standardization*, vol. 1, pp. 46–48, 2019.

[14] Y. C. Gan, S. Y. Xu, and R. D. Cai, "Application of RS485 in access control system," *Electronic Quality*, vol. 5, 2004.

[15] H. Xiaolin and Z. Lin, "Design and implementation of intelligent fingerprint lock based on cloud service," *Electronic Design Engineering*, vol. 28, no. 7, pp. 50–54, 2020.

[16] Z. Wu, C. Weiguang, and Z. Ruiheng, "Design of large capacity identity identification access control system based on RFID technology," *Electronic Design Engineering*, vol. 29, no. 9, pp. 136–141, 2021.

[17] S. Hen, "Design and development of intelligent door lock system based on IoT," *Digital Technology and Applications*, vol. 36, no. 1, pp. 177-178, 2018.

[18] Z. Q. Jiang, H. Zhong, and J. P. Shen, "Analysis of effective power supply length of Ether net (PoE)," in *Proceedings of the 2020 Annual Conference of the Communication Line Committee of the China Institute of Communications*, pp. 240–245, Shenzhen, China, 2020.

[19] J. J. Xu, *Research on IoT application based on NB-IoT, [M.S. thesis]*, Beijing University of Posts and Telecommunications, 2017.

[20] H. M. Li, M. H. Yan, H. B. Ren, and S. X. Fu, "Research on the method of secure and efficient data transmission based on UDP protocol," *Journal of Beihua Aerospace Industry College*, vol. 32, no. 6, pp. 8–10, 2022.

[21] H. Y. Zeng, W. J. Mu, and Y. Wei, "Research on fingerprint recognition system based on IoT," *Science and Technology Innovation and Application*, vol. 12, no. 34, pp. 130–133, 2022.

[22] X. Pan, *Research on Network Transmission Performance Optimization for Mobile Interconnection*, Hangzhou Dianzi University, 2015.

[23] Y. Zhao, L. Cheng, and Y.-j. Li, "Design of intelligent access control system based on image detection," *Machine Tool Hydraulics*, vol. 48, no. 6, p. 1, 2020.

[24] W. Wang and Z. Qiuhong, "Design and implementation of multichannel acquisition and switching system based on FPGa and TCP/IP," *Application of Electronic Technique*, vol. 45, no. 6, pp. 125–129, 2019.