Design of passive electronic lock system under trusted IoT

Qingyao Han*, Yanyan Yin, Wei Zhang, Xuanpei Song, Haibo Chang
CASIC Research Institute of Intelligent Decision Engineering, Beijing, 100074, China

ABSTRACT

In this article, a passive electronic lock system under trusted IoT is designed. The system is built on a combined public key frame structure and applies SM2/SM4 series of International Data Encryption Algorithm (IDEA). It can meet higher security requirement of various application scenarios like in military, hospital and financial systems. In this study, exclusive identification is issued to staffs, equipment, packages and systems that involved in the electronic lock system. Lifecycle management service is provided. The operator-lock-system bidirectional identity authentication and secure data interaction are achieved. In this method, the proposed system is advanced in terminal reliability, access authentication, transmission safety, data tracking and boundary control.

Keywords: Passive electronic lock, trusted IoT, data encryption

1. INTRODUCTION

Traditional mechanical locks have been used for hundreds of years, with its function being ultimately developed. Even though, they cannot meet the modern requirement of reliability, safety, informatization and intelligentization. Since semiconductor was invented in the end of 1950s, traditional lock has taken the advantage of it and multifunctional electronic lock was invented[1]. Pass electronic lock, as a new important branch of electronic lock, is different from active electronic lock largely because the power supply is moved to electronic keys[2]. Thus, the problems of high power dissipation, complex structure, high-frequency maintenance in traditional active electronic lock are completely solved[3]. As a result, passive electronic lock, as the most reliable, environmental friendly, cost effective and maintenance-free electronic lock, it has attracted growing attention in the industry and among the users. Series of products have also come onto the market[4]. However, passive electronic lock still has short comings in safety at present that the electronic keys are prone to be cheated and copied, restraining its development and adoption in some importance industries[5-7].

2. SYSTEM DESIGN

2.1. Logic structure

Modular design is adopted in the passive electronic lock system under trusted IoT. It is made up with passive electronic lock, smart key, hand-held terminal, supporting software and trusted IoT management platform. Among them, the passive electronic lock only remains the lock cylinder, security chip and a motor, while the smart key contains battery and trusted communication module. Once the smart key touches the contact zone of passive electronic lock, the chip and motor are powered through touching. Once the smart key information matches, a command will be sent to lock and the lock will receive the command, then open the passive electronic lock. The structure of passive electronic lock is shown in Figure 1.

2.2. System structure

The passive electronic lock system has integrated daily work, such as surveillance, multi-level authorization management, lock management and key managements, achieving intelligent management. By accrediting authority intellectually, we can realize all-round management. The structure design of passive electronic lock managing system is show in Figure 2.

The system is majorly divided into three layers, the data layer, service layer and display layer. Intellectual management of electronic lock can be achieved with the hierarchical design.

On display layer, various data sources are integrated to formulate a complex page, providing data with a form, which is easy to receive.

*felixhan@yeah.net

International Conference on Computer Application and Information Security (ICCAIS 2021),
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12260, 122601K · © The Authors.
Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2637684

On service layer, managements of authentication, locks, keys, tasks, users, diaries, systems and form reports are realized. Using the data service interfaces, the service layer and data layer can exchange data.

On data layer, the storage, standardization and exchange of task-related data in lock can be achieved.

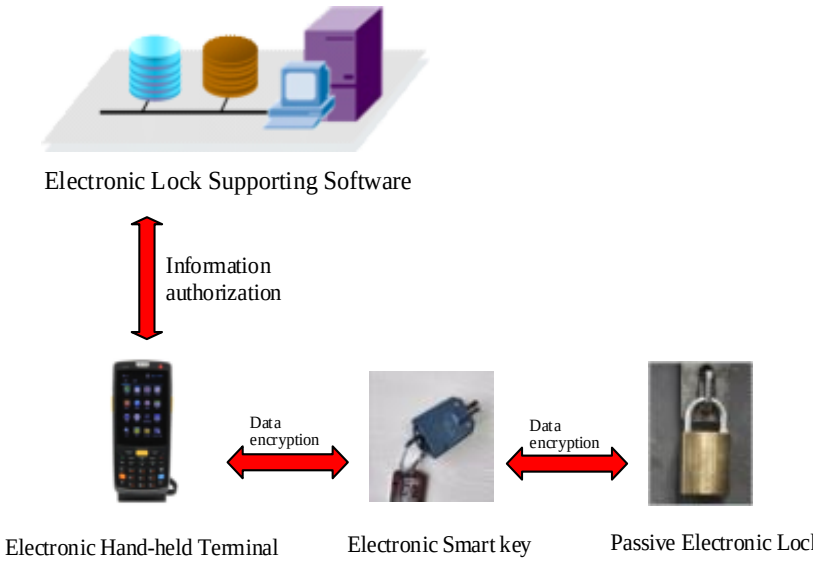

Figure 1. The logic structure of passive electronic lock.

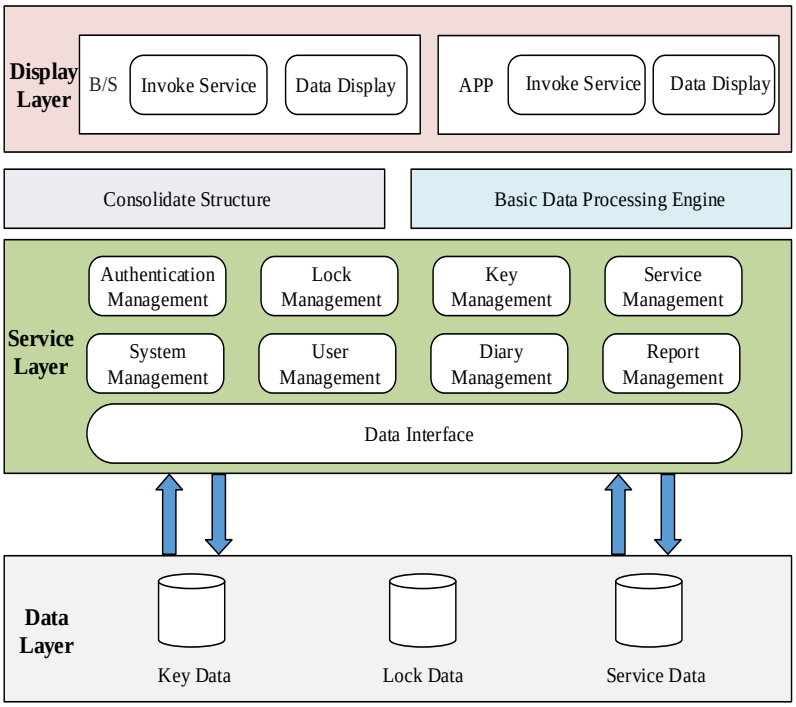

Figure 2. The structure of passive electronic lock managing system.

2.3. Working mechanism

Users can log in the hand-held terminal of electronic lock by using username/password authentication. Then, the system will pass secret key to the smart key for contact with passive electronic lock and verification. Upon success, the motor in cylinder will be powered and give command to lock or unlock the passive electronic lock. The working mechanism is

shown in Figure 3.

The electronic lock manage system can authorize user to unlock specific locks in specific areas and time. Users, with the hand-held terminal and smart key, can conduct operations in pointed authorized areas.

The hand-held terminal can get connected to smart key and give commands using Bluetooth. When smart key touches the contact zone of passive electronic lock, they compare the passwords and authenticate identity information. The unlock command will be given upon success and the passive electronic lock will receive it and unlock.

After onsite operation, users will lock it using hand-held terminal. By using Bluetooth, the lock will be locked under the command.

Figure 3. The working mechanism of passive electronic lock.

3. ESSENTIALS IN THE DESIGN

3.1. Trusted module

In this design, the low-power-consumption trusted module using IDEA is adopted. It contains 32 bit RISC security kernel[8], FLASH256K/SRAM32K. The operating frequency is 60MHz; the power consumption under idle mode is less than 1 uA. It can satisfy the requirement of different terminal manufacturers to converge and debug rapidly[9]. This module can be installed in passive electronic lock and smart key to realize reliability in terminal subject, terminal identity and terminal data.

3.1.1. Trusted terminal principal. When the handheld terminal is powered on and ready to be enabled, the integrity and legitimacy of the handheld terminal system program are verified by using challenge response and hash value[10]. If the security detection passes, the bootloader starts the firmware program[11]; If the safety test fails, the system startup is not allowed. The terminal startup process continues to perform security detection on the system process, and only the security process with signature is allowed to start and execute. The system enables firmware integrity verification to prevent attacks on terminal firmware.

3.1.2. Trusted terminal identity. The system conducts two-way identity authentication for all external information interactions of the handheld terminal through the trusted module, and only the authenticated interactions are allowed. Using two-way identity authentication mechanism, it can active defense against the interface attack,

man-in-the-middle attack, replay attack and other security risks.

3.1.3. Trusted terminal data. The system sign and encrypt the data generated by the handheld terminal and the interactive information between the smart key end and the passive lock, it add a unique password for each data Even if the untrusted terminal gets the data, it cannot be cracked to ensure data security.

3.2. Soft-shield module

The soft-shield module adopted here uses IDEA and is integrated with hand-held terminal. It can guarantee security of important basic information, such as secret keys, public keys, harsh value and signature. It will provide necessary safe computing environment and support during encryption/decryption, signature verification and identity verification.

3.3. System management platform

The system management platform is responsible for managing the lifecycle of identity and API service of the electronic lock system. It is the base of the overall structure. It includes the public key matrix manage system, public key manage system and soft-shield manage system. By providing operators, facilities and systems their unique identity identification certificates, it can ensure the credibility of identity of signer with the certificates. During data interaction, the signing and encryption technology can ensure the integrity and authenticity of data, thus to avoid the risk of manipulation and fabrication of data.

3.4. Secure transmission of electronically signed data

Before all information and data are exchanged, the IoT trusted management platform issues identification for the electronic handheld terminal, electronic smart key and passive electronic lock. In the process of data transmission and interaction, the data security is realized through encryption and decryption technology. In order to ensure the security of the encryption key, a new encryption key needs to be negotiated during each data exchange to ensure that the illegally obtained data cannot be cracked with the previous encryption key. The security architecture of data transmission is shown in Figure 4.

IoT trusted management platform issues identity authentication and is responsible for the life cycle management of identity. When bidirectionally verify identity, the passive electronic lock, smart key, hand-held terminal and electronic lock system each hold their own identity. Before interactional visiting, the signatures will be verified to confirm identity.

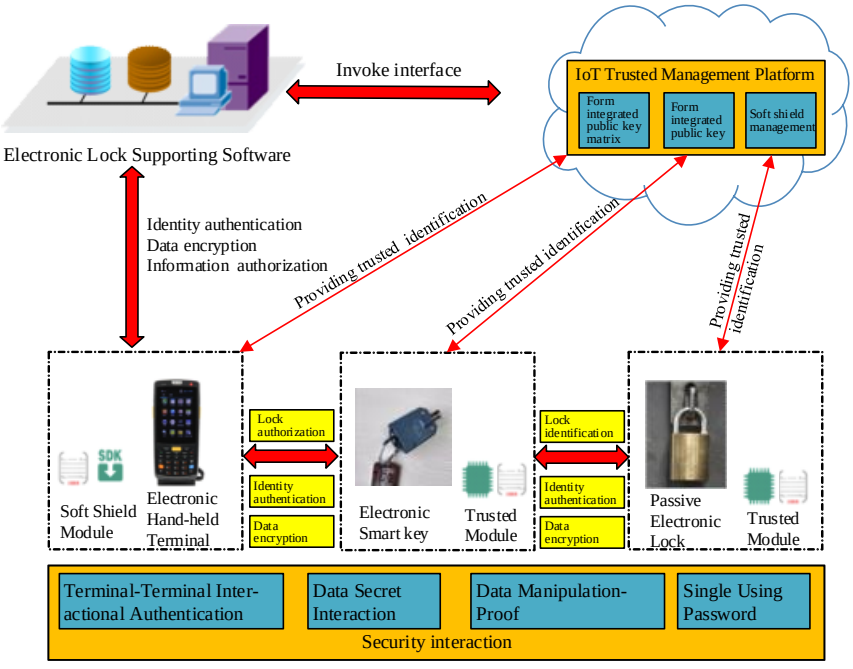

Figure 4. The security architecture of data transmission for passive electronic lock system.

Taking the data exchange between the electronic lock management system and the electronic lock handheld terminal as an example, before the information exchange between this two terminals, the trusted management platform should ensure the authenticity of the identities of both sides and carry out bidirectional identity authentication first; After passing this authentication, the system creates a encryption key, encrypts the transmitted data through this encryption key, and achieves the data encryption interaction; This trusted management platform uses asymmetric encryption of the encryption key with the other terminal's public key to prevent data from being tampered and forged; Each data transmission adopts a unique encryption key to ensure that the illegally obtained data cannot be cracked. After receiving the encrypted data and encryption key, the other terminal obtains the encryption key through asymmetric decryption, and then decrypts the encrypted data with the encryption key to obtain the original data. In the whole process, the identities of both parties, encryption keys and encrypted files are secure, thus ensuring the security interaction of this system. The interfaces and data flows during the interaction are shown in Table 1.

4. FUNCTION REALIZATION

The passive electronic lock system can realize primary functions including:

(1) User management. It allows administrators to add users in the system and appoint specific user to operate specific device during appointed time. This is widely adopted in importance facilities that need special management.

(2) Authorization management. Administrators can authorize different users with corresponding rights according to their identity, realizing divided-authority management.

(3) Lock management. It allows users to add/delete locks in the system, locate the lock's position. Administrator can check the number of the lock, its position and status, realizing intellectual management of locks.

Table 1. The interfaces and data flow.

Interface	Input	Output
Identity authentication interface	Identity authentication information	Result of identity authentication information
Signature interface	Raw data	Signature data information
Verify interface	signature data information	Result of signature verification
Encryption interface	Raw data	Encrypts data
Decrypt interface	Encrypts data	decrypts data

(4) Key management. It allows users to add/delete smart keys, and checking the status of keys, such as whether the key is in stock or used, and the time and user when a key is used.

(5) Task management. In the task management interface, administrator can examine the application of users and check undergoing tasks and completed tasks, including the duration of unlock, utility time, and the reason of utility.

(6) Diary management. The system can record the users that unlock it, the time of unlock and lock. It helps with tracking information when a problem occurs.

(7) System management. With the managing system, the electronic lock system can be intellectually managed.

5. CONCLUSION

The passive electronic lock system under IoT employs SM2/SM4 IDEA and sets up Lightweight certification system. It provides users, devices and systems involved in the process with exclusive identity certificates. It also provides basic key services. With these, it can achieve terminal-side and side-cloud bidirectional authentication and guarantee secure interaction. In this way, each user is identified and each usage is authorized, ensuring the safety of the electronic lock management.

REFERENCES

[1] Sheng, X. J., Shi, W. and Shan, D. K., "The application of modern information technology in electronic locks," Value-Engineering, 37(23), 229-231 (2018).

[2] Zou, X., Han, J. S., Qu, Y. H. and Xiao, J., "Passive biometric electronic lock via UHF RFID," Chinese Journal of Network and Information Security, 7(2), 126-140 (2021).

[3] Yang, Z. H., "Application of new-generation electronic lock in traditional scenario," China AutoID, 12(3), 98-100 (2008).

[4] Fang, A. J., Zhou, W. M., Zheng, H. X. and Ma, Q. Y., "Design of passive electronic clock system based on PIC single chip," Journal of Nanjing Normal University (Engineering and Technology Edition), (3), 22-27 (2014).

[5] Huang, Y. F., Wang, Y., and Zhou J. N., "Improvement Project on electronic lock," Technology Innovation and Application, (21), 22-23 (2016).

[6] Xu, X. T., Yang, C. and Wang, S., "Research on building information environment based on trusted IoT," Computer Network, 42(19), 73-75 (2016).

[7] Ma, X J, Sun, S M and Wu, J., "Design of onsite passive electronic lock based on single chip," Modern Electronics Technique, 33(9), 177-179 (2010).

[8] Xu, Z. C., Cui, A., Wang, Y. H. and Liu, T., "A containerization method for reinforcement learning based on RISC-V architecture," Computer Engineering & Science, 43(2) 266-273 (2021).

[9] Qi, Y. H., Wang, N. N., Wang, F. and Xie, D., "Electronic lock group intellectual management system based on IoT," China Science and Technology Information (20), 65-66 (2020).

[10] Zheng, C. A. and Wu, X. Z., "Design of short wave access authentication system based on symmetric key," Communications Technology, 48(6), 729-733 (2015).

[11] Wang, Y., Tan, Y. L., Zou, X. F. and Hu, Z. H., "Development and implementation of bootloader based on S32R274," Modern Information Technology, 5(2), 41-43 (2021).