Identification System Based on Near Field Communication and Fingerprint Technology for Android Mobile Devices

Yuyang Zhang [1, a], Cheng Xin[1, b], Wenru Liu[1,c], Jin Ding[1,d] and Quanyin Zhu*[,e]

[1]Faculty of Computer Engineering, Huaiyin Institute of Technology, Huaian, Jiangsu Province, China

[a]497665230@qq.com, [b]claudex@sina.cn, [c]1125564165@qq.com, [d]hyicdj@163.com, [e]hyitzqy@126.com,

Keywords: Near field communication; fingerprint identification; Android; mobile devices; identification system; encryption

Abstract. With the sustained increase in usage of mobile devices over the world, mobile application can be used in many areas such as Identity Recognition. In this work, we put forward an architecture for identification system on Android based on Near Field Communication (NFC) technology, using smart card's secure element (SE) technology to ensure tamper resistant. This system uses RFID card as the key in identification and transfers the NFC module to identify information of the card, combining mobile public platform to push notifications. The architecture consist of Android application and service of the server side, it can provide convenient identification service without other device, meanwhile, the encryption algorithm of the architecture can also give a secure and reliable data recording in staff management. The system will be used extensively in public management field.

Introduction

As a non-contact and interconnect technology, NFC gives a simple and touch control scheme to provide users with service including information exchange, content reading and content writing. As NFC technology becoming more mature, it has been widely used in mobile devices field, corresponding applications also comes up. Such as smart posters [1], shopping application [2], ticketing application [3], healthcare system [4], smart home [5], and so on as [6]. It is certain that NFC technology is promising.

In recent years, identity recognition rapidly develops by reason of the demand for public management. The Android application of the system adopts Reader/Writer pattern of NFC to read the information in the RFID card, encrypts the information and then uploads it to server of the system. The server decodes and verifies the information Android application uploads, then sends the result back to the Android application. Users can complete Identification by operating the application on an NFC mobile device.

Application Models

Definition

In the system, we name vetted people's RFID card Vetted Card, name application possessor's RFID card Admin Card. Name mobile of administrator Admin Mobile, name mobile of operators User Mobile. Shorten secure element to SE.

Implementation Environment

In this paper, we test the system using Samsung GALAXY Note 3 mobile device with Android 4.42.In Android framework (Android 4.42 or above), this system uses MIFARE Classic IK cards for reading and writing data using APIs. The Android framework provides a package includes NFC module.

Fingerprint recognition module uses FPM10A fingerprint module, which employs FPC1011F capacitive fingerprint sensing device. Use Bluetooth 4.0 in communication module.

Encryption algorithm Advanced Encryption Standard (AES) uses the native android package provides from http://developer.android.com/reference/javax/crypto/Cipher.html.

Framework

This paper proposes architecture for NFC based identification system as illustrated in Figure.1. Detailed description will be given in following section.

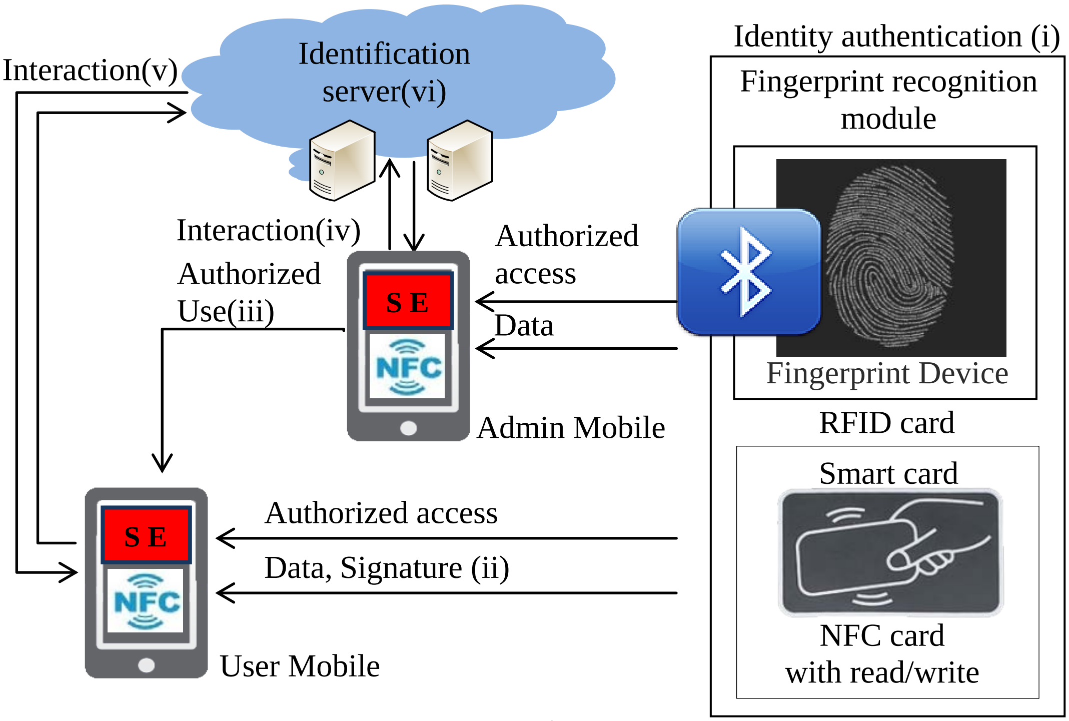


Figure.1 NFC based identification system architecture

(i)Identity authentication uses fingerprint recognition technology mixed NFC recognition technology. NFC recognition reads RFID card ID and personal data. Fingerprint recognition checks identity by comparing local fingerprint database. Fingerprint device communicates with mobile devices by using Bluetooth. The relation between card and application is illustrated in Figure.2.

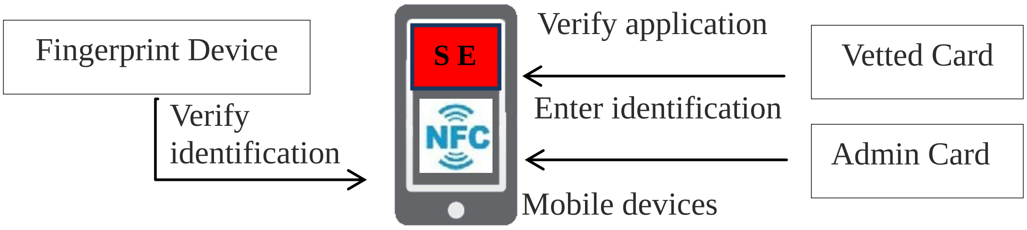


Figure.2 NFC based identification call graph

(ii)In the architecture, RFID card is retained on mobile device using card emulation and Java application installed on the SE. The application can read access and update the card’s data by using SWP protocol. In this section, NFC is mainly used to authorize user’s access and get unknown people’s identity. Android application receives data consists of RFID card data and fingerprint examine result.

(iii)To manage the system easily, the system adopts a traditional, hierarchical top-down model of management. Set Admin Mobile as the only administrator, set multi-User Mobiles under Admin Mobile, Admin Mobile can give User Mobiles permission in server to access server database. User can add and remove the authority by operating Admin Mobile. This part plays a leading role in the system.

(iv)During initialization, the system offers only one way to complete it in the current stage. Administrator needs to write and log NFC Identity data by Admin Mobile. The initialization data in Admin Mobile will also synchronize with server.

Admin Mobile and server communicate data by GPRS/ WIFI. Admin Mobile can upload identity verification information and permission change request. Identity verification information includes personal information in, card ID and fingerprint identification results. Sever records this upload and return judging result of this upload to Admin Mobile. Server provides Admin Mobile with user list and whole identity verification record. Data encryption method will be discussed in the next section.

(v)User Mobile and server communicate data as the way in (iv), except that this link doesn't contain access permission of user list and whole identity verification record.

Data Encryption Module

During communication between mobile application and sever, there is a lack of necessary measure insure the security. Although there already has been a mature encryption technology in network communication, it still exist a risk of data leakage and hacker attack. So it is necessary to use a reliable data encryption algorithm in the architecture.

In this work, we use a prevailing method of Advanced Encryption Standard (AES, i.e., 128) during data communication.The flow chart is showed in Figure.3.When users operate the application to upload or download the data, the AES encryption module will use 128 bit secret key to encrypt the data in sender and send data to acceptor over the network. Acceptor uses AES encryption module to decrypt the Encrypted data to plain text.

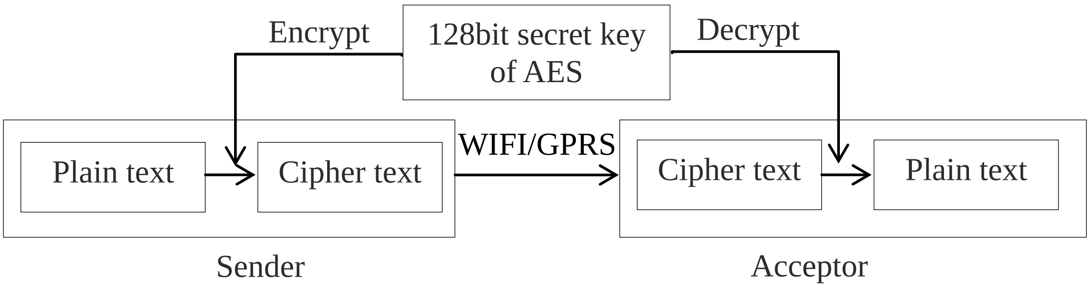
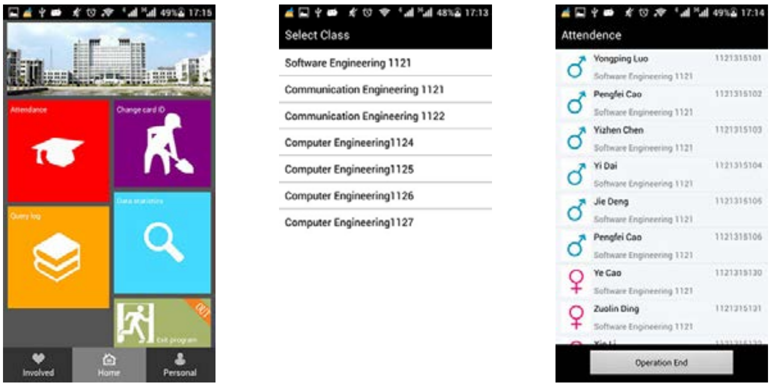


Figure.3 Data encryption and decryption flow

This encryption method can prevent data leakage and hacker attack effectively during network communication.Alhough encryption and decryption divert a certain amount of resources and time, it is obligatory and acceptable.

Conclusion and Future Work

In this work, the system we propose provides a simple, convenient and secure way to do identity recognition. Combining NFC, an emerging simple touch technology, with fingerprint technology, this practice has an advantage of smoother interfaces and higher accuracy. The application can reduce the cost and be operational on most of current mobile devices. This model benefits the urgent need to strengthen the comprehensive management and other field. It is predictable that this system model will be widely used. The screenshot of the Android application are given in Figure.4.



Select Class

- Software Engineering 1121
- Communication Engineering 1121
- Communication Engineering 1122
- Computer Engineering1124
- Computer Engineering1125
- Computer Engineering1126
- Computer Engineering1127

Attendence

♂	Yongping Luo Software Engineering 1121	1121315101
♂	Pengfei Cao Software Engineering 1121	1121315102
♂	Yizhen Chen Software Engineering 1121	1121315103
♂	Yi Dai Software Engineering 1121	1121315104
♂	Jie Deng Software Engineering 1121	1121315105
♂	Pengfei Cao Software Engineering 1121	1121315106
♀	Ye Cao Software Engineering 1121	1121315130
♀	Zuolin Ding Software Engineering 1121	1121315131

Figure.4. The screenshot of the Android application

We plan to promote this architecture of the server on private cloud in the future. This measure can enhance the security and control ability in real application. Further improvement will also be proposed for cost saving and users experience.

Acknowledgments

This study is supported by the National Students' Platform for innovation and entrepreneurship training program of China.

References

[1] Wu, J. ; Electr. & Comput. Eng., Carnegie Mellon Univ.: S-SPAN: Secure smart posters in Android using NFC, IEEE International Symposium on WoWMoM,2012,pp.1-3.
[2] Husni, E.; Sch. of Electr. Eng. & Inf.: Shopping application system with Near Field Communication (NFC) based on Android, International Conference on System Engineering and Technology (ICSET), 2012,pp.1-6.
[3] Nasution, S.M. ; Sch. of Electr. Eng. & Inf.: Prototype of train ticketing application using Near Field Communication (NFC) technology on Android device, International Conference on System Engineering and Technology (ICSET),2012,pp.1-6.
[4] Sethia, D.;Gupta, D.;Mittal, T.: NFC based secure mobile healthcare system, Sixth International Conference on Communication Systems and Networks,2014,pp.978-983.
[5] De Luca, G. ; Dept. of Innovation Eng., Univ. of Salento, Lecce, Italy: The use of NFC and Android technologies to enable a KNX-based smart home, 21st International Conference on Software, Telecommunications and Computer Networks,2013,pp.1-7.
[6] Mainetti, L. ; Dept. of Eng. for Innovation; Univ. of Salento, Lecce, Italy: IDA-Pay: An innovative micro-payment system based on NFC technology for Android mobile devices, 20th International Conference on Software, Telecommunications and Computer Networks,2012,pp.1-6.