Kassymbayev B., Kalym K., Sagyndykova Zh.

ASSESSMENT OF THE QUALITY OF DRIED VEGETABLE PRODUCTS

Annotation

In the article the results of experimental researches at drying of fruits and vegetables in a gel-drying module of the established polyfunctional helio-dryer-hothouse in the educational-production economy of the Kazakh National Agrarian University are considered.

Key words: Helio dryer, solar energy, solar drying module, drying, polycarbonate, heat exchange.

UDC 004.89

Seidaliyeva G., Seidaliyeva G.

Kazakh national agrarian university

NFC- BASED ACCESS CONTROL AND MANAGEMENT SYSTEM

Abstract

This article considers research on the application of the NFC (Near Fild Communication) method based on the principle of near-proximity communication. This technology allows you to create a system of access control and management using mobile devices equipped with an NFC module, which in turn replaces heavy metal keys, badge cards, etc. on the cryptographic keys of the smartphone.

Keywords: NFC - technology, smart phones, Android, access control and management system.

Introduction

In current fast-growing technology world, most of mobile devices are equipped with many different wireless modules, which can be used to solve the problems with keys. Almost all of them are equipped with Bluetooth and infrared, latest ones also have NFC installed on- board. NFC technology has the following benefits compared to other short-range technologies:

- Slow speed and short range – this allows NFC to consume as little power as possible so it can be left on at all times and not affect the phone's battery by that much (Bluetooth) [1];
- Hassle-free approach to connections – with NFC, bringing the two devices within range is enough to facilitate the communication between the two (vs. Bluetooth);
- Free-line of sight – no direct line of sight is required to establishes connection.

NFC-based Access Control and Management System will allow people to lock/unlock doors just by tapping mobile device to NFC reader. It will also perform all the functionality that other ACMS's do, such as logging entrance time, controlling access privileges, etc. This system can be applied as:

- Independent and complete ACMS (Access Control and Management System);
- The system for checking attendance of students in educational institutions, as well as observation of student location within the institution;
- Small ACMS for home, as an addition to "smart house" system.

NFC is one of the most popular latest wireless communication technologies. With NFC technology, communication occurs when an NFC- compatible device is located within a few centimeters of another NFC device or an NFC tag [2]. The big advantage of the short

transmission range is that it secures from eavesdropping on NFC-enabled transactions. NFC technology opens up exciting new usage scenarios for mobile devices. Until recently, payments using smart phones were possible using NFC card emulation combined with secure element. Traditionally, you would have to store security information, for example the security keys from a debit card (which are stored in the tamper resistant card chip) in a similarly tamper resistant chip on your device – the Secure Element [3]. The Secure Element emulates the card and can be found either on the SIM card or in a chip embedded in the phone handset. Generally, the mobile carrier controls SIM and the handset manufacturer controls embedded chip. When an NFC card is emulated using host- based card emulation, the data is routed to the host CPU on which Android applications is running directly, instead of routing the NFC protocol frames to a secure element.

Materials and methods of research

There were some research done in previous years for implementing the attendance control systems in universities. Authors of research work used RFID (Radio Frequency Identification**)** - technology as an automatic monitor of student classroom attendance. They demonstrated how to automate an entire student-attendance registration system within an educational institution by the use of Ethernet. However, there were some other research work done with different views for attendance checking system. In, authors designed and implemented wireless iris recognition attendance management system, whereas in authors proposed attendance management system extended with computer vision algorithms. Finally, in, authors implemented a system for attendance checking based in RFID-technology. In most of this research work, RFID-technology was used a framework for building systems, whereas authors of this research paper presents an NFC-enabled Access Control System, which by the help of mobile devices, NFC technology and HCE mode, introduced in Android, makes possible for people to use only one single key. To emulate a smart card and the data exchange between the mobile device and NFC-reader, ISO 7816-4 smart card standard is used. User brings his device to the reader; reader reads the data from device using NFC interface and transmits it to the server for authentication [4]

The main use of the system is divided into two stages: Registration stage; Door lock/unlock stage. Registration stage: Before using mobile devices as keys to lock/unlock door locks, keys must be registered in the system. Since this system might be deployed in different places, such as at home, in the offices, or in universities, we have used identification number for distinguishing these systems. Moreover, suppose that any user wants to get access to doors by the help of smart phones. In addition, before starting any user should register in these systems and get a key (UID) for this specific system. Furthermore, each system has its own identification number (the system-id). To register any device in the system, it must be brought to special registration device. At this point, server generates unique key-identification (the UID) and then sends it to the device, together with public-key of the system (the p-key), which is used to encrypt transmitted data and system-id. If system-id, UID and p-key are successfully received, then server permanently stores UID in database. Now device can be used to lock/unlock the doors (figure 1).

Both registration and lock/unlock stages are implemented using the “smart card standard” named ISO 7816-4. There are two different data exchanges that are performed during two different stages: registration and door lock/unlock stages. The first data exchanges at registration stage are performed in 8 consecutive command-response pairs grouped into 2 sub-phases.

Sub-Phase 1: Between Server and Controller data exchange. Data exchange is initiated by server application. Server sends “reg” command to controller, performing handshake procedure. Controller responds with ACK_REG_OK acknowledgement. Server generates UID and sends it with “uid” command. Controller responds with ACK_UID_OK acknowledgement. Server sends systems public key with “key” command. Controller responds with ACK_KEY_OK

acknowledgement. Server sends “end” command, indicating that data exchange is finished and now UID and key can be transferred to device.

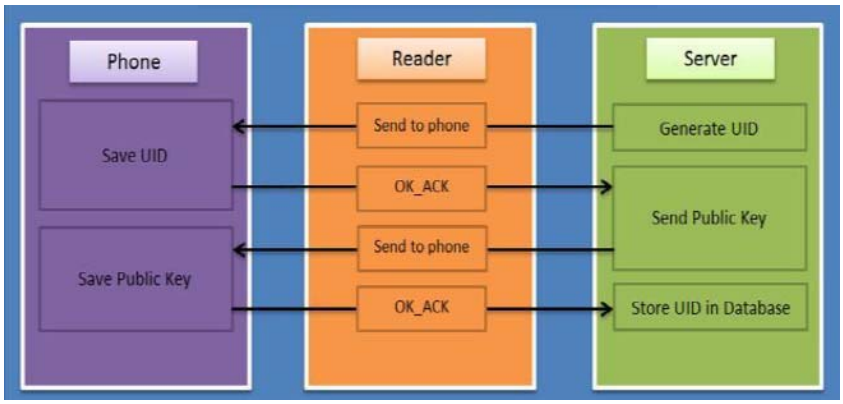

Figure 1. Scheme of registration stage

Sub-phase 2: Controller – Device data exchange. Controller waits until device is brought close enough to begin data exchange. Controller sends SELECT APDU instruction to start communicating with required AID at device (Registration AID). Device responds with 90 00 OK acknowledgement. Controller sends WRITE BINARY instruction with UID to device. (P1 = 0x00). Device responds with 90 00 OK acknowledgement. Controller sends WRITE BINARY instruction with public key to device. (P1 = 0x01). Device responds with 90 00 OK acknowledgement. This step continues in loop until public key is completely transferred to device. Controller sends WRITE BINARY instruction indicating end of data exchange (P1 = 0x02).

Device Responds with 90 00 Ok Acknowledgement: The latter data exchanges at door lock/unlock stage are always initiated by mobile device and performed in consecutive command-response pairs supplemented with requests to server. Controller always waits device to be brought close enough to begin data exchange. Controller sends SELECT APDU instruction to start communicating with required AID at device (Unlock AID). Device prepares data to send (encrypts UID with public key). Device responds with 90 00 OK acknowledgement. Controller sends READ BINARY instruction to device (P1 = 0x00). Device responds with part of encrypted data concatenated with 90 00 OK acknowledgement. Controller sends encrypted data to server. Steps 2-4 are continued in the loop until encrypted data is completely transferred from device to server. Server decrypts and validates data. If everything is OK, responds with GRANT command, else responds with DENY command. If controller receives GRANT command, signal to unlock the door is sent. Security Aspects: The UID for device is generated by using Key Generator class for AES-256 algorithm. Asymmetric keys are generated automatically one time upon server’s first start, but can be regenerated manually from server application. Keys are generated by using RSA algorithm with 1024-bit as the size of the key. In order to prevent man-in-the-middle attack, before sending UID to server, it is concatenated with mobile device’s system time and then encrypted with system’s public key. At server side, data is decrypted, UID and System time are checked so that difference between device’s system time and server’s system time is less than 5 second (this parameter will be configurable at server application). In this way, even if encrypted data is intercepted by attacker, it cannot be reused as it is.

Results and discussion

Access control systems are always in high demand and are deployed everywhere. By reducing the number of physical keys and cards people need to carry and using smart phone as a single device to access to multiple locations is a good choice against lost, left at home or work keys. In addition, even if smart phone is lost, no need to change the lock at door, just disable or

delete lost devices UID, registered in system from centralized DB. For the future work, there are some plans to replace the connection to the wireless connection as well as making some improvements concerning the safety aspects, including replacing system time to something more efficient.

Reference

1. Silva F., Filipe V. and Pereira A. Automatic control of students' attendance in classrooms using RFID, in Third International Conference on Systems and Networks Communication (2008) 384-389.

2. Dan Nosowitz. Everything you need to know about Near Field Communication (January 3, 2011).

3. Consult Hyperion. Host Card Emulation- why it matters. Retrieved from http://www. chyp. com/assets/uploads/Documents/2013/11/hce.pdf.

4. Ben Joan. Difference between NFC and Bluetooth (April 2, 2012).

5. Kadry S. and Smaili M. Wireless attendance management system based on iris recognition, Scientific Research and Essays, 5(12) (2010) 1428-1435.

Сейдалиева Г., Сейдалиева Г.

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ NFC

Аннотация

В статье приведены исследования по применению метода NFC, основанного на принципе ближней бесконтактной связи. Данная технология позволяет создавать систему контроля и управления доступом с помощью мобильных устройств, оснащенных модулем NFC, что в свою очередь заменяет тяжелые металлические ключи, карточки-пропуска и т.д. на криптографические ключи смартфона.

Ключевые слова: технология NFC, смартфоны, операционная система Android, система контроля доступа и управления.

Сейдалиева Г., Сейдалиева Г.

NFC НЕГІЗІНДЕ БАСҚАРУҒА ҚОЛ ЖЕТКІЗУ ЖӘНЕ БАҚЫЛАУ ЖҮЙЕСІ

Андатпа

Мақалада ішкі қатынассыз байланыс принципіне негізделген NFC әдістемелігіш қолдану зерттеулері келтірілген. Бұл технология NFC модулімен жабдықталған мобильді құрығылар көмегіне қол жеткізе басқару және бақылау жүйесін құруға мүмкіндік жасайды, бұл дегеніміз өз алдына ауыр металды кілттерді, кіріп – шығу карточкаларын және т.б. криптографикалық смартфон кілттерін алмастырады.

Кілт сөздер: NFC технологиясы, смартфондар, Android операциялық жүйесі, кіруді бақылау және басқару жүйесі.