A New Logistics Distribution Scheme Based on NFC

Jie CUI [1,2]

[1.] School of Computer Science and Technology, Anhui University, Hefei, 230039, P.R. China
[2.] Co-Innovation Center for Information Supply & Assurance Technology, Anhui University, Hefei, 230039, P.R. China

Dong SHE, Jinyi MA

School of Computer Science and Technology, Anhui University, Hefei, 230039, P.R. China

Qingxin WU

School of Computer Science and Technology, Anhui University, Hefei, 230039, P.R. China

JiaQiang LIU

School of Computer Science and Technology, Anhui University, Hefei, 230039, P.R. China

***Abstract*— There are many disadvantages in the logistics distribution scheme today. The package may be taken by mistake and the information of consumers on the package may be hooked up illegally. What is more, it needs lots of couriers and costs plenty of money. To solve these problems above, a more effective logistics distribution scheme based on Near Field Communication is proposed. Many key technologies, such as the data exchange technology among android APP, server and NFC module, the data transmission technology by NFC and so on, are used in this scheme. The information is encrypted by ASE while transmission from one place to another. By contrasting the existing schemes and the new scheme, it is obvious that the new scheme has more advantages. Finally, the performance of the scheme is tested. The scheme makes logistics distribution automated greatly by the NFC, PN532and arduino. In addition, it can ensure the safety of consumer privacy largely. All in all, the data of the test indicates that the new scheme has better performance.**

Keywords— NFC; AES; Logistics distribution; Arduino

I. INTRODUCTION

With the popular of the computer and Internet, e-commerce develops rapidly as a new industry ,as a result, the express industry develops quickly. The online retail sale is up to 500 billion yuan in 2010 and reaches 1500 billion yuan in 2013. We gradually form the habit to buy commodity online by express. However, the current system to distribute express has many disadvantages. Firstly, the efficiency is low, especially in some festivals. The courier must read the name and check the information in the express paper one by one. After that, we can finally get our express. Sometimes, we even keep waiting for half an hour or more. As the time goes on, more and more people are shopping online, a more convenient and high-efficient way for logistics distribution is needed. Besides, more and more people worry about their privacy today but the traditional system of logistics distribution can not ensure the safety of privacy [1, 7].

To solve these urgent problems in express industry, we propose a new logistics distribution scheme. Our scheme is based on the technology of NFC. All the data in the system are encrypted with AES algorithm. It overcomes many disadvantages existing in old system.

II. PRELIMINARIES

A. NFC

NFC (near field communication) is a kind of communicational technology, which run wirelessly at a high frequency; and it can work in 20 cm by 13.56 MHz. It can transmit data at three speeds which are respectively 106Kbit/s, 212Kbit/s and 424Kbit/s.The NFC has become a standard of the ISO/IEC IS 18092, EMCA-340 and ETSI TS 102 190[2].The NFC has two work modes which are initiative mode and passive mode [9].

Card emulation mode: In this mode, the NFC tag is equivalent to a IC card which adopts RFID technology. The NFC tag can replace many IC cards used now(including credit ,card entrance card used in supermarket, easy card, control card, ticket to vehicle, ticket to door and so on). In this mode, it is a great advantageous that the RF domain of Non-contact card reader can supply power to NFC tags; so, the tag can work even the host device is out of battery. The NFC tag must be equipped with Security Element (SE for short) if it wants to apply the function of Card Emulation.

P2P mode: this mode just likes the data transmission technology by infrared ray; however, it runs in a more short distance but that it is founded faster, can transmits data at more lager speed and consumes less power (similar to Bluetooth) [3, 12]. Two mobile phones with NFC function can exchange information by P2P mode if the NFC devices in mobile phones are connected, in this case, we can download music, exchange pictures and synchronise device address book. Through NFC technology, the devices such as digital cameras, PDAs, computers and mobile phones can exchange information [8].

Reader/Writer mode: in this mode, the NFC device is

978-1-4799-1843-0/15 $31.00 © 2015 IEEE
DOI 10.1109/ICNISC.2015.48

used as no-contact card reader. For example, we can read the information in poster and electric tag by NFC device [4, 13].

Compared to Bluetooth, the RFID (13.56MHz ISO/IEC 18000-3) device is compatible in NFC technology. The NFC device consumes less power and has similar protocol with Bluetooth 4.0 ‘s low consumption protocol. When NFC devices run at a no power device (such as the shutdown of mobile phone, Contactless smart CARDS or smart poster), it consumes much less power than Bluetooth 4.0.

B. AES

AES (Advanced Encryption Standard), it is called Rijndael cipher in cryptology. AES has been adopted by the US government.

We suppose readers are familiar with the principle of the AES. We will describe the process of AES encryption algorithm briefly with AES-128. AES operates on a 4×4 column-major order Byte- Matrix, termed the state. It also can regard as a 16×1 column order matrix ($(a_{ij})=(a_{00},...,a_{30},a_{01},...,a_{31},...,a_{33})^T$). AES encryption includes four transformations (except the last round): Byte-Sub, ShiftRow, MixColumns and AddRoundKey[5].

1) Confounding of Nonlinearity

Every elements in the Byte- Matrix shall be substituted according to the S[#] table. S-box includes three transformations [6].

(1) Calculating $y=x^{-1}(0^{-1}=0)$ in GF (2^8).

(2) Calculating $z=L_A\bullet y$, L_A is a matrix of 8×8.

(3) The output of S-box is $L_A\bullet y+63$.

2) Linear Diffusion

Do cyclic shift to each row of Byte -Matrix by a certain offset. Make the a_{ij} byte be $a_{i(j-i \bmod 4)}$. This process can use a 16*16 Byte- Matrix R_A to achieve[5].

$$\left\lfloor a_{i(j-i\bmod4)}\right\rfloor_{16\times1}=R_A\bullet\left\lfloor a_{ij}\right\rfloor_{16\times1} \quad (1)$$

(1) Regard every row of Byte-Matrix as a four-dimensional vectors in $GF(2^8)$.Then use $y=D\bullet x$ to count, in this formula D is a 4*4 matrix in $GF(2^8)$. Similarly, we can use a 16×16 diagonal matrix to complete the MixColumns. Its linear diffusion is[10]:

$$Mix_A\left[a_{i(j-i\bmod4)}\right]=\begin{bmatrix}D&0&0&0\\0&D&0&0\\0&0&D&0\\0&0&0&D\end{bmatrix}\bullet R_A\bullet\left[a_{ij}\right] \quad (2)$$

3) The AddRoundKey

Take every byte in byte matrix xor with key in the round [11]. The round can be denoted as:

$$\mathrm{Round}_A(x,(k_A)_i)=\mathrm{Mix}_A(R_A(S(x)))+(k_A)_i \quad (3)$$

III. THE NEW LOGISTICS DISTRIBUTION SCHEME

A. Processes of the Whole Scheme

Our scheme is organized by the android App, Server and NFC module. Besides, the android App is composed of the user App and the administration App. The scheme contains the following steps:

Step 1. To scan the two-dimensional code on the goods, the administration must use user name and password to login administration App, then the Server will send an empty locker number to the administration App.

Step 2. The administration opens relevant locker by NFC function of the smart phone, then puts the express into the locker.

Step 3. Server sends the information to the user smart phone, then, user can get his or her express by the information.

The whole process of the new logistics distribution scheme is shown in Figure 1.

B. Data Transmission Design

Step 1. the administration App can get the information about the good while the NFC reader scan the two-dimensional code .the information will be encrypted before arrive the server, and the server stores this information into the database.

Step 2. Server gets an empty locker number by search the database, then sends the number which has been encrypted into the administration App along with a HashKey. Then, the administration App deciphers the information and shows on the screen.

Step 3. The Administration App sends the information and HashKey mentioned above to NFC module ,and NFC module stores it.

Step 4. Server sends the same information encrypted and HashKey to specific User App, then, the user App deciphers the information and shows on the screen.

Step 5. When the user tries to get his express, the NFC module will compare the administration information and the user information to check if the user is legal .

We adopt AES arithmetic to make sure the data and user privacy safe while the information transmits among different parts of the system. To avoid the illegal user take the express, we use the user information and the HashKey to check man’s identity which tries to open the locker.

C. Database Design.

Following is the data relation of the program(including entity type, category of contact, attribute and identifier):

Goods (goods ID, user ID, administration ID ,delivery time, time of getting goods ,the state of the good)

Courier (courier ID, courier nickname, courier password, courier name, courier mobile phone number, courier address)

Consignee (consignee ID, consignee nicknam, consignee password, consignee name, consignee mobile phone number, consignee address)

Address of the express (the details of the address, consignee ID)

Locker(locker ID, goods ID, courier ID, consignee ID, locker number ,the details of the locker address, hash ID)

Hash (Hash ID, HashKey)

The E-R diagram of the database is shown in Figure 2.

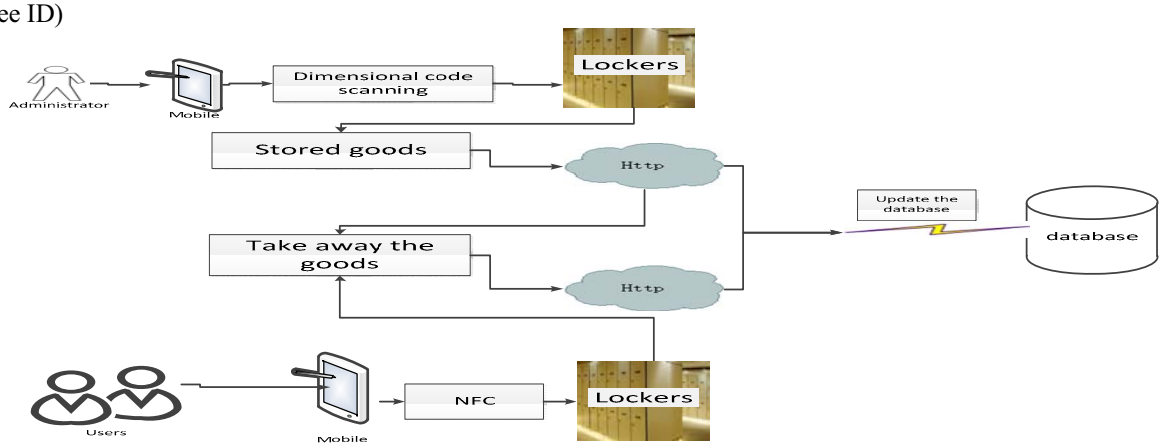

Figure 1. Program flow chart of the new scheme

IV. THE PERFORMANCE ANALYSIS OF THE NEW SCHEME

A. Security Analysis

a) The information of goods is encapsulated in two-dimensional code for safety. All messages in two-dimensional code are encrypted with AES. So, the malicious users can't get the plain -text even though they scan two-dimensional code .By this way, our users' private information is protected from revealing.

b) The data transmission among different parts of the system is secure because the data is encrypted by AES. What is more, we use the timestamp after operating twice DJBHash as the source of key. So, even the information is intercepted, the malicious user can not get the plaintext.

c) The system will not only match username and password but also match the changed key which produces by the function Hash when the user takes the goods, which makes sure that the locker is only open by specific user.

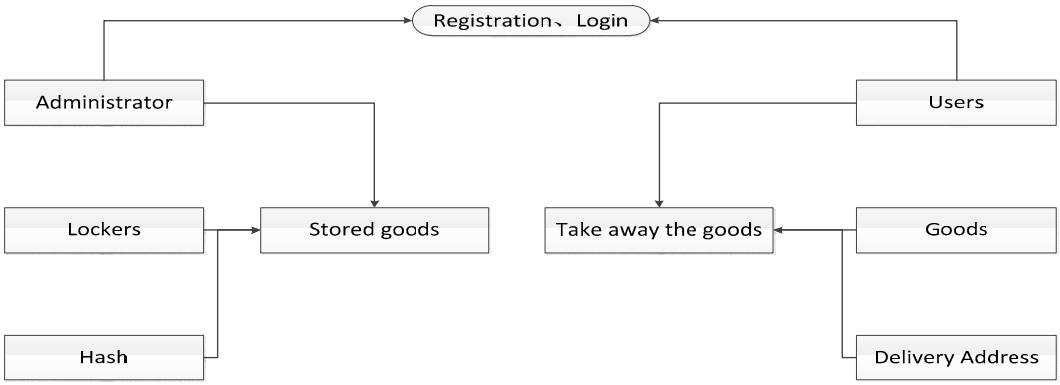

Figure 2. The E-R diagram of the database

B. Efficiency Analysis

Compared with the artificial logistics, the system with NFC not only improves the security but improves the efficiency. At first, it improves the efficiency of courier. Through statistical analysis, we find that the courier of YuanTong (which is a express company) works from 11 am to 5:30 pm. The courier has to wait all the time because the student will go to take the express in different time, which makes the efficiency very low. However, if the system based on NFC is adopted, the courier just needs to scan the two-dimensional code and puts the goods in the locker, which is all the work they need to do. We also have some concrete data. For example, in the Anhui University, the courier of YuanTong has to distribute 500 expresses to students in average. In order to inform the consignee that the express is arrived, it costs 90 seconds to edit and sent per message in existing schemes, while it only costs 30 seconds to complete the same work in our scheme.

Some comparisons in efficiency are shown in table 1

TABLE I. COMPARING THE EFFICIENCY OF THE EXISTING SCHEMES AND OUR SCHEME

Efficiency index	Existing schemes	Our scheme
The average time of distribution express(for couriers)	Long	Short
The average time to wait (For the consignees)	Long	Short
Whether the consignee need to take express in fixed time	Yes	No
Whether the courier needs to send message or phone	Yes	No

C. Economic Analysis

In the future, if our scheme gets popular, just like community mailbox, a city can be divided into several areas, each area sets an express of the hubs which achieves a high-degree automation. A mass of vigor, manpower and money are saved. Firstly, the scheme will reduce lots of employees of the express company, and this will save plenty of money for the company. What's more, the bill of message also is saved. Secondly, for the consumers, the cost of mailing express is cot down because the cost of express company has been cut down.

V. CONCLUSION

The scheme adopts AES algorithm in data transmission, and it can solve the problem that information leakage. Besides, the user information is encapsulated with two-dimensional code which can be read by smart terminal (such as smart phone), and this reduces the trouble of filling express form and saves the paper. What is more, this reflects the concept of green and environmental protection. For the past few years, the "poisonous express" occurred frequently. The scheme minimizes the damage of the workers. Besides, the information about the "poisonous express" in the database makes it easy for policemen to investigate it, which makes the express industry safer. For the express company, the scheme can save lots of money because the system is low-cost and reliable.

The scheme also has some disadvantages. Firstly, the express maybe take by someone if the smart phone is lost. Secondly, if the smart phone can not support NFC technology, the user can not take the express. We will try our best to make the scheme more efficient and practical.

ACKNOWLEDGMENT

The work was supported by the National Natural Science Foundation of China (No. 61173188, No. 61173187, No. 61272074), the Educational Commission of Anhui Province, China (No. KJ2013A017), the Research Fund for the Doctoral Program of Higher Education (No. 20133401110004), the Science and technology project of Anhui Province (No. 1401b042015), and the Doctoral Research Start-up Funds Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] Sun F Q, Chen T B. Design and implementation of dynamic integration for 3 PL based on J2EE and Web services[J]. Application Research of Computers, 2007, 24(2): 233-237.

[2] Kostinger H, Gobber M, Grechenig T, et al. Developing a NFC based patient identification and ward round system for mobile devices using the android platform[C]//Point-of-Care Healthcare Technologies (PHT), 2013 IEEE. IEEE, 2013: 176-179.

[3] Mansfield-Devine S. Paranoid Android: just how insecure is the most popular mobile platform?[J]. Network Security, 2012, (9): 5-10.

[4] Coskun V, Ok K, Ozdenizci B. Professional NFC application development for Android[M]. John Wiley & Sons, 2013.

[5] Kotturi D, Yoo S M, Blizzard J. AES crypto chip utilizing high-speed parallel pipelined architecture[C]//Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on. IEEE, 2005: 4653-4656.

[6] Zhang X, Parhi K K. High-speed VLSI architectures for the AES algorithm[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2004, 12(9): 957-967.

[7] Rui-yan CAI. Principle and application of Arduino[J]. Electronic Design Engineering, 2012, 16: 047.

[8] Haselsteiner E, Breitfuß K. Security in near field communication (NFC)[C]//Workshop on RFID security. 2006: 12-14.

[9] Mulliner C. Vulnerability analysis and attacks on NFC-enabled mobile phones[C]//Availability, Reliability and Security, 2009. ARES'09. International Conference on. IEEE, 2009: 695-700.

[10] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm[M]//Cryptographic Hardware and Embedded Systems-CHES 2004. Springer Berlin Heidelberg, 2004: 357-370.

[11] Feldhofer M, Wolkerstorfer J, Rijmen V. AES implementation on a grain of sand[J]. IEE Proceedings-Isssnformation Security, 2005, 152(1): 13-20.

[12] Nandakumar, Rajalakshmi, Krishna Kant Chintalapudi, Venkat Padmanabhan, and Ramarathnam Venkatesan. Dhwani: secure peer-to-peer acoustic NFC. InProceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, pp. 63-74. ACM, 2013.

[13] Hasoo Eun, Hoonjung Lee, and Heekuck Oh. Conditional privacy preserving security protocol for NFC applications. IEEE Transactions on Consumer Electronics, 2013, 59(1): 153