Secured Mobile Transaction Using NFC Technology: Top-Up Printing System

Teddy Mantoro[1], Media A. Ayu[1], Goenawan Brotosaputro[2], Nur F. Ain[1], Noorzalina Ghazali[1]
[1]Integ Lab, KICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Faculty of Information Technology, University of Budi Luhur, Jakarta, Indonesia

{teddy, media, nurfain, ninag}@iium.edu.my, goenawan.brotosaputro@budiluhur.ac.id

Abstract: - NFC technology has become a success across a broad range of applications depending on its large-scale adoption by enterprises and consumers. Unfortunately, NFC security is still a major concern for the business. This study proposes a secure mobile transaction model for any transaction using NFC Technology. As proof of concept, a Top-up printing system is developed and for interaction with the web interface, an ACR 100 Reader with ACOS3 SIM card is used. As for the security measurement, MD5 algorithm is implemented to accept the system authorization. As a result, in employing NFC Technology, the users no longer need to wait in a long queue. Just "touch" or "wave" at the nearest reader to top-up.

Key-Words: -MD5, mobile transaction, NFC, radio frequency, RFID, smart card, tag, touch, wave.

1 Introduction

M-commerce first started with the use of wireless POS (Point Of Sale) swipe terminals and has since made its way into cellular phones and PDA's (Personal Digital Assistants). The use of NFC technology makes life easier and more convenient for users around the world by making it simpler to make transactions with a simple touch or wave from an NFC enabled device. NFC, as a radio frequency short range wireless connectivity technology, offers two-way interaction ('read' and 'write') [1] and also at the same time offers intuitiveness and simplicity in user interaction. NFC operates, once two devices are brought within 4-5 centimeters of each other, at 13.56 MHz and has the ability to exchange or transfer data with another device at speeds ranging from 106 kbit/s to 848 kbit/s [2]. NFC technology is based on the standard of proximity smart cards specified in ISO 14443 [3] and is standardized in ISO 18092.

The problem is the traditional transaction is sometimes expensive and time consuming. Consumers need to wait in a long queue for regular transactions such as paying electricity bills, or similar cases.

Cellular phones and PDA's have largely grown in reputation and as a result manufacturers have made significant improvements and added features to attract even more consumers and meet current owners' demands. One of those features is wireless transaction processing. These mobile devices with NFC enabled technology are able to process credit card and debit card transactions wirelessly within seconds at tradeshows, business seminars, or house calls, without having to stand up in a long queue at the bank or post office.

There are two types of Mobile processing solutions:

i. Wireless Terminals - devices manufactured specifically to allow businesses the freedom to process transactions freely without the interference of wires. These devices are committed to a specific network and carrier such as CDMA (Code division multiple access) and GPRS (General Packet Radio Service) that offer good coverage. They differ in size and functionality, but indeed offer the capability to accept swiped transactions with a stripe reader and to print a receipt upon usage.

ii. Owner of Cell Phones/PDAs - compatible cell phones and/or PDAs with Web-capability access. This solution requires a minimum of technical-savvy, but has proven to be the ultimate solution not only for traders who do not want to carry multiple devices, but also for the navy who need centralized control and reporting of the processing through their devices.

This study contributes a guaranteed privacy and security system when doing a mobile transaction with a capable and reliable encryption and must provide the existing and significant information to the users.

For the next section, it discusses related works in NFC and also mobile transaction technology; on how the technology is implemented in several countries and its applications will be described. In section 3, current problems concerning manual applications, such as top-up printing, will be presented and how NFC can solve these problems. The 4th section is our proposed solution to overcome the problem and section 5 describes the design of the proposed system. Meanwhile, in section 6, we discuss the technical part of Top-up printing system, and the paper is closed by a conclusion and future work in developing NFC application.

2. RELATED WORKS.

A smart environment is an environment fitted with a variety of sensors and electronically operated devices which allow the occupants to customize the functionality of their living environment (e.g. a domestic home). Using this system, it is possible to, for example, monitor light level, temperature, window and door status and who is currently in a house. Most research related to smart environments currently focus on context aware systems which adapt according to contextual information. Such environment are usually equipped with a set of smart objects which are augmented by sensors or actors to interact with their physical environment and which often provide a user interface. Touching relates to selecting a smart object by bringing the user's mobile device into contact with the object the user wishes to interact with. For this, the user must be near the object and be aware it is augmented with a touch capability.

The user has to touch the object which results in the related services being presented to the user on their mobile device. Through this, additional services can be accessed that are not provided by the device itself. This interaction technique is seen as natural because it conforms to our everyday physical interactions as we often touch objects with our hand or fingers to support the comprehension of the listener when talking about it.

Want et al. [4] were among the first to present a prototype for the touching interaction technique which incorporated RFID tags and a short range RFID reader in a mobile device (in this case a tablet computer). They used their prototype to demonstrate the augmentation of books, documents and business cards to establish links to services such as ordering a book or picking up email addresses. Another implementation was described by Välkkynen et al. [5] who developed an interaction technique called TouchMe that uses proximity sensors to sense the distance between the augmented object and the mobile device.

Common technologies for implementing this interaction technique are Radio Frequency Identification (RFID) and Near Field Communication (NFC) which means objects need not be touched directly, rather approximately 0-3 centimeters is sufficient for the selection. Haikio et al. develop an NFC based menu touch system for the elderly. The application was intended to be used by home-dwelling elderly persons who were eligible for home care provided by the town [6].

Leviadi et al. developed a prototype and usability test of a Near Field Communication (NFC) based Virtual Ticketing application. They conceived a usable application to allow the user to buy tickets for public transportation with a mobile phone. The application, named NFCTicketing, was developed following a user-centered approach, so obtaining a balance between the information reduction required by the user and the increase of application flexibility. The NFCTicketing application combines latest-generation technologies (such as NFC) with well-known technologies such as Short Message Service (SMS) [7]. Schoo and Paolucci identify security and privacy requirements of non-contact based applications in The PERvasive serviCe Interaction (PERCI) platform. Behind every poster there is attached an NFC tag containing the very same information displayed by the graphical boxes. As a result, by touching those with an NFC enabled phone the user could specify the movie (s)he wants to see, the theater, the show and the amount of tickets that (s)he wants to buy just by touching the tags with their phones [8].

Wiechert et al. explores NFC based applications for the retail stores and analyses the influence that these could have on the prevailing customer shopping process. NFC devices could hold the customers' payment cards, loyalty cards, and rebate coupons at the same time. Holding one NFC device up to a contactless reader could replace having to get two plastic cards and several coupons out of a wallet or purse. As these descriptions show, the NFC based applications would not fundamentally change the customer shopping process, but merely support it on the store floor and in the check out area. They also illustrate, that the majority of the promoted NFC applications are focused on supporting the check-out share of the customer shopping process [9].

3 NFC TECHNOLOGY

Near field communication technology or simply NFC, is a converging evolution of existing contactless standards towards the goal of global interoperability. NFC operates within the globally available and unregulated Radio Frequency band of 13.56 MHz and has three data transfer rates: 106 kbit/s, 212 kbit/s and 424 kbit/s. An NFC transaction always follows a straightforward sequence of Discovery, Authentication, Negotiation, Transfer, and Acknowledgment [3]. NFC's link layer includes a secure authentication procedure and anti-collision mechanisms that precludes a third party from hacking the link.

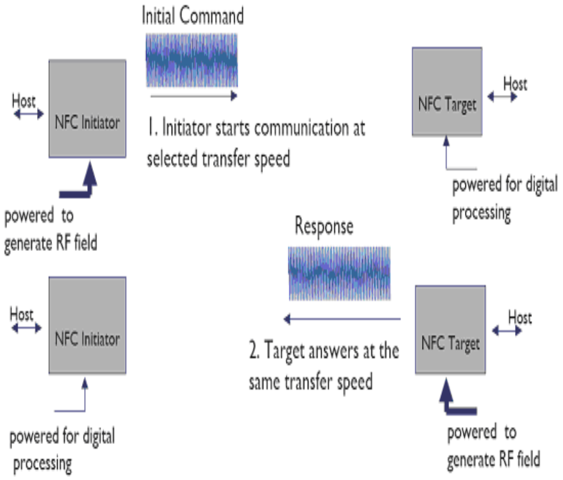

Initial Command
Host
NFC Initiator
1. Initiator starts communication at selected transfer speed
NFC Target
Host
powered for digital processing
powered to generate RF field
Response
Host
NFC Initiator
2. Target answers at the same transfer speed
NFC Target
Host
powered for digital processing
powered to generate RF field

Fig. 1 Illustrates a Typical NFC Interaction.

Figure 1 gives an illustration on an NFC interaction which uses a radio frequency short-range wireless connectivity technology. NFC offers two-way interaction ('read' and 'write') and also, at the same time, offers intuitiveness and ease in user interaction [10] as shown in Figure 2.

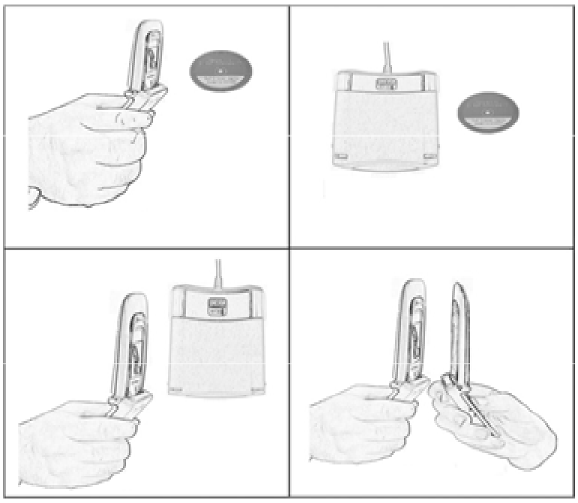


Fig. 2. An Example of a Cell- Reader Tag

This NFC device operates in a reader/writer mode [11]; the NFC device can read and alter data stored in NFC compliant passive (without battery) transponders. In this mode, the NFC device reads or writes data to or from an NFC compliant tag. The NFC device acts as the initiator and the tag as a target. Depending on the data stored on the tag, the NFC device takes an appropriate action without any user interaction.

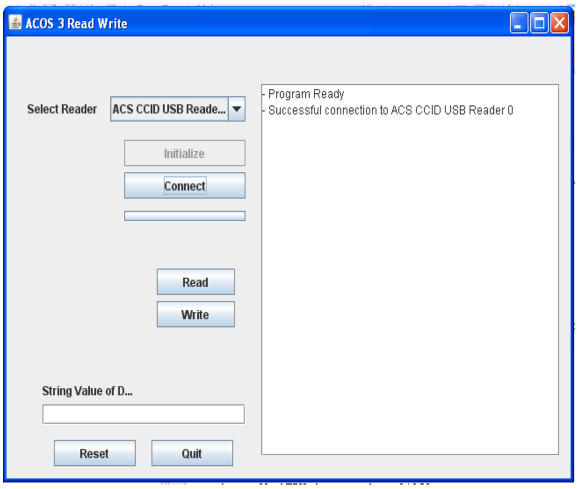
4. CASE STUDY: TOP-UP PRINTING SYSTEMS

In university environment setting, such as IIUM or UBL, every user, staff and students, can manually put a top-up printing system, provided by IT department, to supply the users with printing service. In order to use this service, every staff or student has to pay an amount of money to add into their account. This is troublesome because there is always a long queue waiting to pay at the front desk. Due to time constraints, the users always hesitate to use the system and bring their own printer to their hostels or dormitory. Furthermore, whenever their credit top-up balance is insufficient especially during pick hours, such as a meeting or the due date for student's assignment submission, it is very troublesome to go to the IT department just for the sake of replenishing their printing account. In addition, just like any normal working department, IT departments also end their operations at 5pm daily, Students, therefore, need to wait for another day to gain access to the system.

We came up with an application that uses NFC technology, which will ease the problem of user printing payment. This system, which uses an NFC enabled mobile phone, acts as a middle interpreter to the original printing system. By using NFC, a contactless payment can be made when the mobile phone is touched with a tag reading device that will interact with the printing service. The NFC capabilities can be directly associated to mobile phones. An NFC device contains both an NFC chip and a chip named secure element, which allows the storing of all personal information, so that such phones can be used to perform several day-to-day activities such as buying and accessing many services and different information sources.

The ACS CCID USB Reader together with ACOS3 SIM Card work in the background process in the application for administration purposes. The ACR 100 is a CCID (chip/smart card interface devices) compliance, which will help with less driver installation issues. It is a standard protocol between a USB smart card readers and computers, leading to a simplified plug and play method.

As shown in Figure 3, in order to connect the database with the reader, it must be initialized and recognized first. When the reader has been plugged in, the initial process can be started (by clicking the initiate button). This process is to set up the environment of the reader in the running server. Once the reader is acknowledged, the initialisation is performed and is followed by the connection process (by clicking the connect button). As soon as the NFC environment is ready, it can to link with the database. This is the process when the reader is connected.



- Program Ready
- Successful connection to ACS CCID USB Reader 0

Fig.3 Connecting the reader with the database.

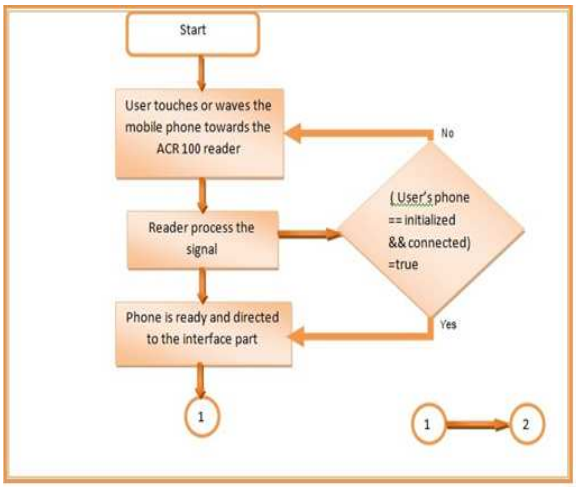

Start
User touches or waves the mobile phone towards the ACR 100 reader
Reader process the signal
(User's phone == initialized && connected) =true
No
Yes
Phone is ready and directed to the interface part
1
1
2

Fig. 4 Phone enableNFC processing

Figure 4 and 5 presents the server algorithm in handling the mobile client query from registering the user until the top up process. The user interface in the web server consists of user profile information and mobile credit information. When a user is directed to the interface, the user has to first register. Information such as Name, Matrix Number or Identification Number, and Password will be required and are stored in the User Profile Information database.

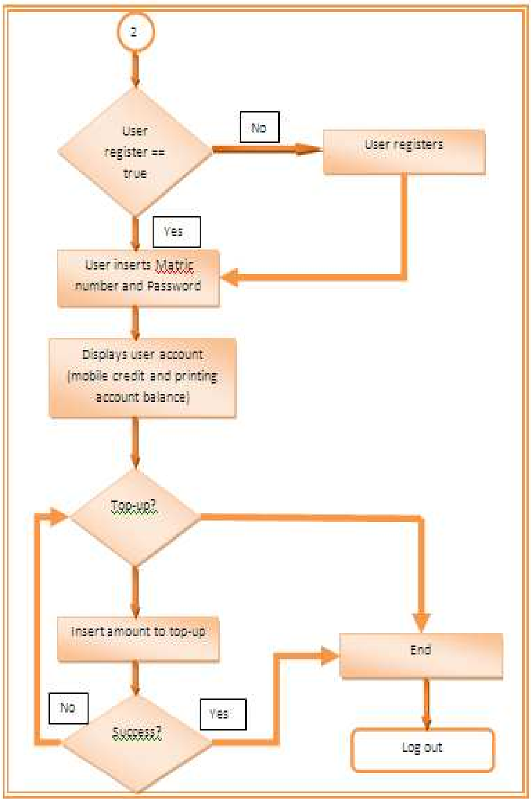
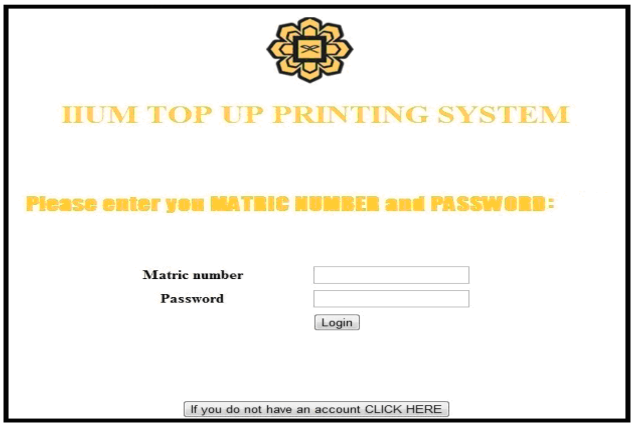

2
User register == true
No
User registers
Yes
User inserts Matric number and Password
Displays user account (mobile credit and printing account balance)
Top-up?
Insert amount to top-up
No
Yes
Success?
End
Log out

Fig. 5 Web Server Top Up Processing

Then, the user has to log in to the top up printing system by providing the user id and password. The following (Figure 6) is the interface of the application.



IIUM TOP UP PRINTING SYSTEM

Please enter you MATRIC NUMBER and PASSWORD:

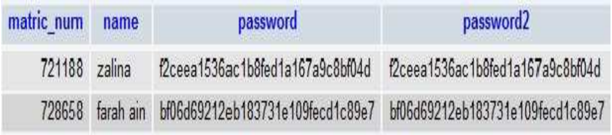
Matric number
Password
Login

If you do not have an account CLICK HERE

Fig. 6 Top Up Web Interface

The password is encrypted using an encryption technique called MD5 (Message-Digest algorithm 5). MD5 is a 128-bit hash algorithm. The password inserted by the user will be converted to a hash value and compared to the hash value stored in the database. If the hash value is a match with the database, the user is logged-in. Otherwise, the user will be prompted to re-enter the password.

When a user enters his password, the password will be converted to a 128-bit hash value for users' security authentication (Figure 7). In this application, MD5 encryption technique is used.



matric_num	name	password	password2
721188	zalina	f2ceea1536ac1b8fed1a167a9c8bf04d	f2ceea1536ac1b8fed1a167a9c8bf04d
728658	farah ain	bf06d69212eb183731e109fecd1c89e7	bf06d69212eb183731e109fecd1c89e7

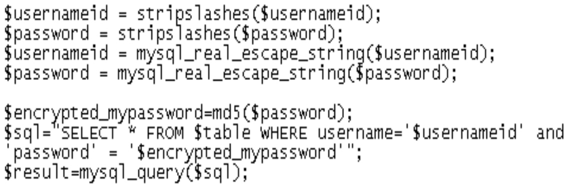
Fig.7. MD5 hash encryption

Once the user has successfully logged into the interface, the user's Printing Account balance and Mobile Credit balance will be displayed. The user has the option to either proceed with the top-up process or log-out of the system. To proceed with the top-up process, the user has to insert the amount to top-up into their printing account and click submit button.

The system will do a confirmation to ensure whether user has enough balance in their Mobile credit. If there is enough credit, the amount is directly deducted and added to the printing account and then the top-up process is successful. Otherwise, a message will be displayed to the user saying that the top-up process is unsuccessful due to insufficient balance in their mobile credit.

5 DISCUSSIONS

In this study, MD5 algorithm is used in the NFC interface to encrypt user's password to a 128-bit hash value. The following is part of the query that uses MD5 in our implementation:



```
$usernameid = stripslashes($usernameid);
$password = stripslashes($password);
$usernameid = mysql_real_escape_string($usernameid);
$password = mysql_real_escape_string($password);

$encrypted_mypassword=md5($password);
$sql="SELECT * FROM $table WHERE username='$usernameid' and
'password' = '$encrypted_mypassword'";
$result=mysql_query($sql);
```

Once NFC's user has registered, the password will be converted to a hash value and stored in the User Profile information database. When the user wants to log-in, the user input password will be compared to the hash value stored in the database. User will only be allowed to log-in if the hash value inserted is identical to the one stored in the database.

From this study, the development of this NFC application could bring lots of benefits for the users, such as:

- Users' are able to reload their printing account at their own convenience as the system is available 24/7
- Reduce time and simplify the process of reloading their printing account
- Easy, fast and secure transaction
- Mobile credit is used instead of cash.

6. CONCLUSIONS

Near Field Communication technology represents a converging evolution of existing contactless standards toward the goal of global interoperability. This new evolving technology has the potential to revolutionize our daily lives in the near future. Its versatility, interoperability, technology-enabling and security-ready characters makes it even more attractive to develop and implement this NFC technology to suit our day-to-day activities, from consumers and business to ordinary people.

As a proof of concept, we developed a Top-Up Printing System with MD5 encryption to replace the existing/manual Top-Up printing system. The NFC Technology, i.e. ACR 100 Reader with ACOS3 SIM card is used for the interaction with the interface in processing printing top-up printing.

By applying this measure, it becomes more convenient for the user at it saves time and can be accessed 24/7.

References:

[1] Mobile Commerce Wireless Payment Processing Guide, Available at http://www.comparemerchant.com/109, Accessed on 3 November 2011**.**

[2] Patauner C., H. Witschnig, D. Rinner, A. Maier, E. Merlin, E. Leitgeb, High Speed RFID/NFC at the Frequency of 13.56 MHz, The First International EURASIP Workshop on RFID Technology, RFID 2007.

[3] ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards, ISO/IEC. Available at http://www.iso.org.

[4] Want, R., Fishkin, K.P., Gujar, A., Harrison, B. L.: Bridging physical and virtual worlds with electronic tags. *In* Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit (CHI '99). ACM, New York, NY, USA, 1999, pp. 370-377.

[5] Välkkynen P., T. Tuomisto. Physical Browsing Research. In: Workshop Pervasive Mobile. Interaction Devices (PERMID 2005), Munich, Germany, 2005

[6] Haikio J., M. Isomursu, T. Matunmikko, A.Wallin, H. Ailisto, T. Huomo. Touch-based user interface for elderly users. In Proceedings of the 9th international conference on Human

computer interaction with mobile devices and services (MobileHCI '07). Pp. 289-296.

[7] Ghiron S. L., S. Sposato, C. M. Medaglia, A.Moroni, NFC Ticketing: a Prototype and Usability test of an NFC-based Virtual Ticketing application. First International Workshop on Near Field Communication. 2009. NFC 2009, pp. 45-50.

[8] P. Schoo, M. Paolucci. Do you talk to each poster? Security and Privacy for Interactions with Web Service by means of Contact Free Tag Readings. First International Workshop on Near Field Communication, 2009, pp. 81-86.

[9] T. Wiechert, A. Schaller, F. Thiesse. Near Field Communication Use in Retail Stores: Effects on the Customer Shopping Process. Lecture Notes in Informatics, Mobile and ubiquitous information systems development, implementation and application, 2008, pp. 137-141.

[10] NFC Forum. Available at http://www.nfc-forum.org/home

[11] Madlmayr, G.; Langer, J.; Kantner, C.; Scharinger, J.; Third International Conference on Availability, Reliability and Security, ARES 08, 2008.. pp. 642 – 647.