NFC Secured Online Transaction in Mobile Computing Business

Teddy Mantoro, Media A. Ayu, Goenawan Brotosaputro, Nur F. Ain, Noorzalina Ghazali

Abstract— The growth and expansion of the Internet come in a rapid speed and took important place in many aspects of lives, including online payment for transaction information. 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 contactless interface, an ACR 100 Reader with ACOS3 SIM card is used. As for the security measurement, MD5 algorithm is implemented to process the system authorization. As a result of 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.

Keywords— *mobile transaction, NFC, smart card, touch and wave.*

I. Introduction

M-COMMERCE first started with the use of wireless POS (Point Of Sale) swipe terminals and has since made its way into smart phones and PDAs. 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 that 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.

Smart 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.

The next section 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 section 4 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.

II. Related Work

A smart environment is an environment fitted with a variety of sensors and electronically operated devices which allow the

Teddy Mantoro is with the Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia (email:teddy@ic.utm.my).

Media A. Ayu, Nur F. Ain, Noorzalina Ghazali are now with the Integ Lab, KICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia (e-mail: {media, nurfain, ninag}@iium.edu.my).

Goenawan Brotosaputro is with the Faculty of Information Technology, University of Budi Luhur, Jakarta, Indonesia (e-mail: goenawan.brotosaputro@budiluhur.ac.id).

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 which 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.

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. Table 1 shows the comparison between NFC Technology and other short ranged radio technology

Table 1. Comparison between NFC Technology and Other Short Ranged Radio Technology

	NFC	RFID	BLUETOOTH
Set up time	<0.1 ms	<0.1 ms	6 second
Range	Up to 10cm	Up to 3m	Up to 30m
Selectivity	High, given, security	Partly given	Data, centric, medium
Use cases	Pay, get access, share, initiate, easy to set up	Item tracking	Need to identify
Consumer information	Touch, wave, simply connect	Get information	Network for data exchange, headset
Usability	Human centric, easy, intuitive, fast	Item, centric, easy	Configuration needed

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.

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].

Tie-Ju and Lei-Na study Prepayment Meter (PM) which is a kind of new-style meter that purchase electricity by smart card and adopt micro-electronics techniques that can help the user to accomplish electricity prepayment function [9]. This mobile prepayment solution shows that it can be used for purchasing power without going to the agency.

Wiechert et al. [10] 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.

III. NFC Specification and Features

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.

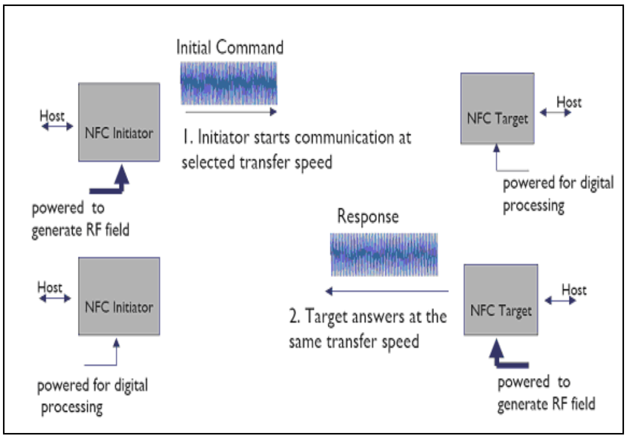

Initial Command
Host
NFC Initiator
1. Initiator starts communication at selected transfer speed
NFC Target
Host
powered for digital processing
powered to generate RF field
Response
Host
NFC Initiator
2. Target answers at the same transfer speed
NFC Target
Host
powered for digital processing
powered to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

Fig. 1 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 [11] as shown in Figure 2.

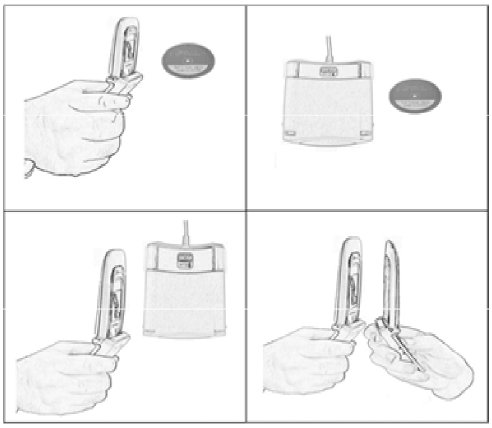


Fig. 2 An Example of a Cell- Reader Tag

This NFC device operates in a reader/writer mode [12]. 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.

NFC is designed for interactions between tags and electronic devices in close proximity (< 10 cm). The standards ETSI TS 102.190, ISO 18092, and ECMA 340 identically define the Near Field Communications Interface and Protocol-1 (NFCIP-1).

These protocols describe the air interface, initialization, collision avoidance, a frame format, and a block-oriented data-exchange protocol with error handling [13]. Additionally, they describe two different communication modes: active and passive.

The Near Field Communication Interface and Protocol-2 (NFCIP-2) specifies the communication mode selection mechanism (ECMA 352). NFCIP-2 compliant devices can enter in three different communication modes: NFCIP-1, ISO 14443, and ISO 15693 [13]. All these modes operate at 13.56 MHz and are designed not to disturb other RF fields at the same frequency.

NFC-Forum has defined four initial tag formats based on ISO 14443 [14]. These specifications are: NFC Data Exchange Format (NDEF), NFC Record Type Definition (RTD), NFC Uniform Resource Identifier (URI) Service Record Type Description, NFC Text Record Type Description and NFC Smart Poster Record Type Description.

The vCard use case consists of an NFC Forum Tag embedded into a business card that contains an electronic vCard (vCARD21, RFC 2425, RFC 2426) with the person details. Reading the tag using an NFC Forum device like a mobile phone or a notebook, the user can retrieve and save the vCard information into his address book. Once the information is correctly stored and saved, the user can use it as desired. This saves the user from manually typing the person details of the business card. If the memory space of the NFC Forum Tag is big enough even a Jpeg image can be stored in the electronic vCard [15].

Designed tag data is converted to corresponding Record Type Definition (RTD) and NFC Data Exchange Formats (NDEF), and automatically encoded on NFC-forum compatible tags. NFC TagMan provides a complete support for all NFCforum Mandated Tag formats (ISO 14443 A, B) from leading manufacturers. Users are presented with advanced menus for inspecting the memory map of the encoded tags, or use advanced manufacturer specific tag features such as locking the tag after encoding [13],[14].

IV. Near Field Communication Architecture

NFC harmonizes today's diverse contactless technologies, enabling current and future solutions in areas such as:

- Information collection and exchange
- Access control
- Healthcare
- Payments
- Transport

The main services of NFC standard architecture as shown in Figure 3 are the following [3],[14]:

1. Emulation: to emulate the smart card including NFC to test the operation for mobile device.
2. Establish a connection: a client (NFC peer-to-peer initiator) is searching for a host (NFC peer-to-peer

target) using NFC Logical Link Control Protocol (LLCP). LLCP is an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications.

3. Setup a connection: Record Type Definition (RDT) and NFC Data Exchange Format (NDEF) are used to transmit the data.

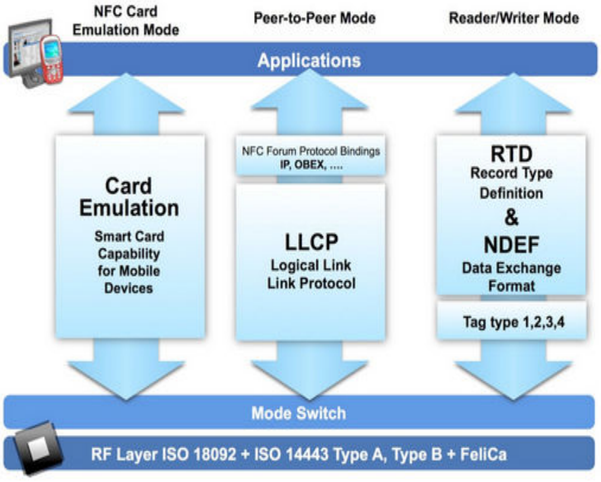


Fig. 3 Different components of the technical architecture of NFC [3],[14].

Figure 4 shows that smart card and NFC which can be used for secured mobile payment and transaction, peer-to-peer communication and access information on the move such as in smart poster, etc.

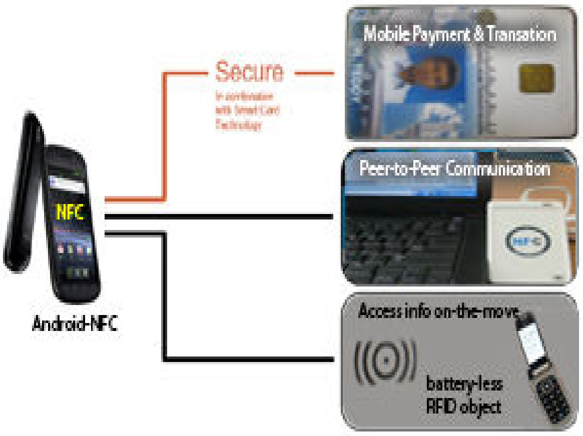

Secure
In combination with Smart Card Technology
Mobile Payment & Transation
Peer-to-Peer Communication
NFC
Access info on-the-move
battery-less RFID object
Android-NFC

Fig. 4 Smart Card and NFC

The advantages of the NFC architecture and its features are the following:

- improved robustness,
  securing sensitive data, private key primarily, in tamper-resistant smart card memory and accessing/updating it trough trusted gateway (PC application) or mobile network when requested
- multiple access technologies (GSM/UTMS and NFC),
  objects to the SIM card can be passed directly through the mobile network (rather than using NFC interface and the Internet), thus splitting delivery of the content, making connection tracking much more difficult
- portability and seamless usage,
  no need to manually configure or memorize anything
- mobile network provider as certificate authority (CA),
  mobile network is trusted third party in user communication, verifying identities of each participant and assigning the keys

In this study, ACRS CCID USB Reader with ACOS3 SIM Card Part have been used, the following is the feature of this NFC device:

- ACS CCID USB Reader together with ACOS3 SIM Card work at the background process in the application for administration use.
- To connect to the interface with the reader, it must be initialized and recognized first. INITIALIZE and CONNECT.
- Focus on READ and WRITE function.
- All user input such as user ID, time login, and current printing balance will be kept for administration purposes.
- A Log file is generated at the end of the transaction for administrative purpose.

V. Case Study: Top-Up Printing Systems

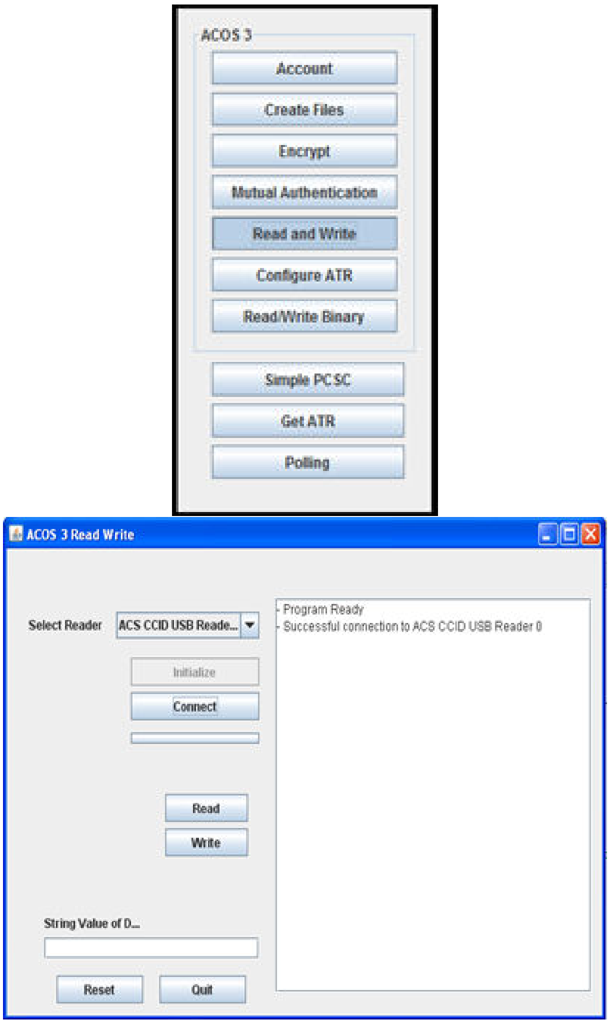
In a university environment setting, such as IIUM or UBL, every user, staff and students, can manually put a top-up printing system, provided by IT department, to supply the users with printing service. In order to use this service, every staff or student has to pay an amount of money to add into their account. This is troublesome because there is always a long queue waiting to pay at the front desk. As for instance in IIUM main campus, we have about 23000 students in one location, during busy period, there always a long queue waiting to pay at the front desk.

Due to time constraints, the users 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 peak 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. Thus, students will 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 [16]. 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 5, 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. 5 Connecting the reader with the database.

Figure 6 and 7 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.

Then, the user has to log in to the top up printing system by providing the user id and password. The following (Figure 8) is the interface of the application.

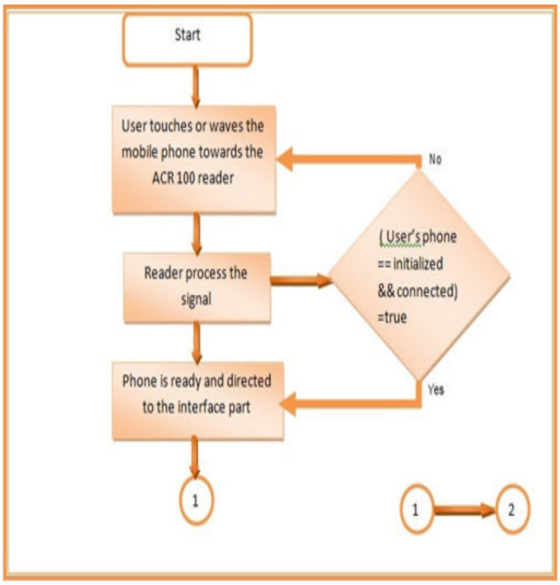

Start
User touches or waves the mobile phone towards the ACR 100 reader
No
Reader process the signal
(User's phone == initialized && connected) =true
Yes
Phone is ready and directed to the interface part
1
1
2

Fig. 6 Phone enable NFC processing

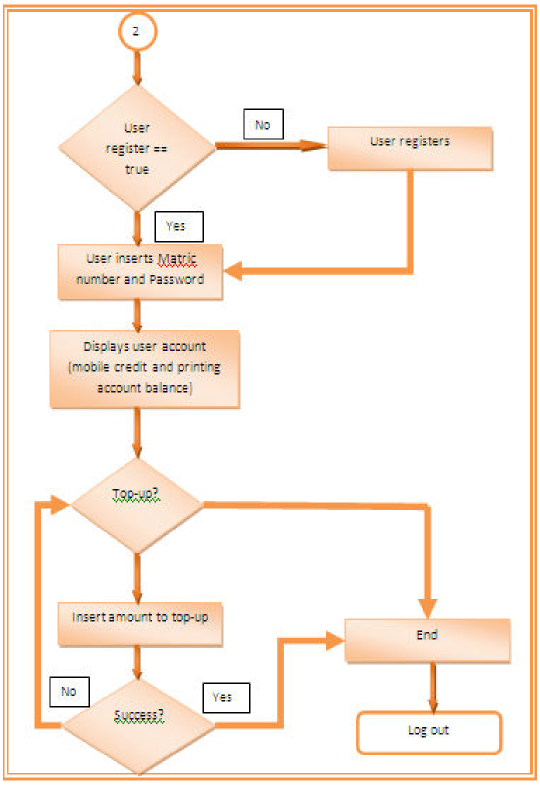
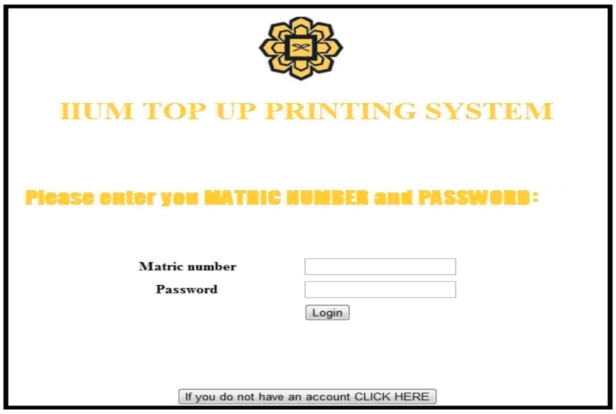

2
User register == true
No
User registers
Yes
User inserts Matric number and Password
Displays user account (mobile credit and printing account balance)
Top-up?
Insert amount to top-up
No
Success?
Yes
End
Log out

Fig. 7 Web Server Top Up Processing

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.



IIUM TOP UP PRINTING SYSTEM

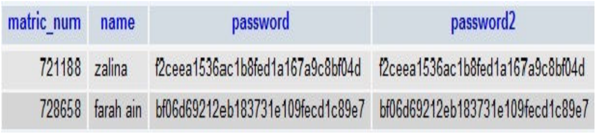
Please enter you MATRIC NUMBER and PASSWORD:

Matric number

Password

Fig. 8 Top Up Web Interface

When a user enters his password, the password will be converted to a 128-bit hash value for users' security authentication (Figure 9). In this application, MD5 encryption technique is used.



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

Fig. 9 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 and the top up processing the ready to serve. Figure 10 shows the top up process, when its process is successful and not successful. 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.

Table 2. Example of top-up printing log

Matrix No	Name	Date	Time	Balance
721188	Zalina	17/4/2011	16:15:33	100
728658	Amir	23/11/2011	09:24:13	17
911054	John	15/12/2011	12:04:47	29
832715	Andrew	12/10/2011	18:03:34	16
813651	Aisyah	17/08/2011	17:08:45	56

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. As mentioned earlier in Section 4 that a log file can be generated at the end of the transaction for administrative purpose. An example of a log file generated by the reader that interacts with the database is shown in the following table.

VI. DISCUSSIONS

Nowadays we can consider smartcards as the most secure moveable computing device. They have been covering successfully many applications involving money, proprietary and personal data including banking, healthcare, and insurance. The smartcard integration in information filtering process guarantees advanced security but it shows two main limitations, in conditions of computing capacity and storage capabilities [17].

The structure of User Profile based on information personalization approach, which has two kinds of explicit and implicit personalization. Explicit personalization asks users directly on their needs, while the implicit personalization studies the user operations on the network. Both methods collect automatically personal information related to the behaviour of the user. This information must be analyzed and classified and then stored in the database. The combination of the explicit and implicit personalization techniques proves to be more capable while integrating training techniques or the intelligent agents. These techniques created or re-value the user profile according to his actions.

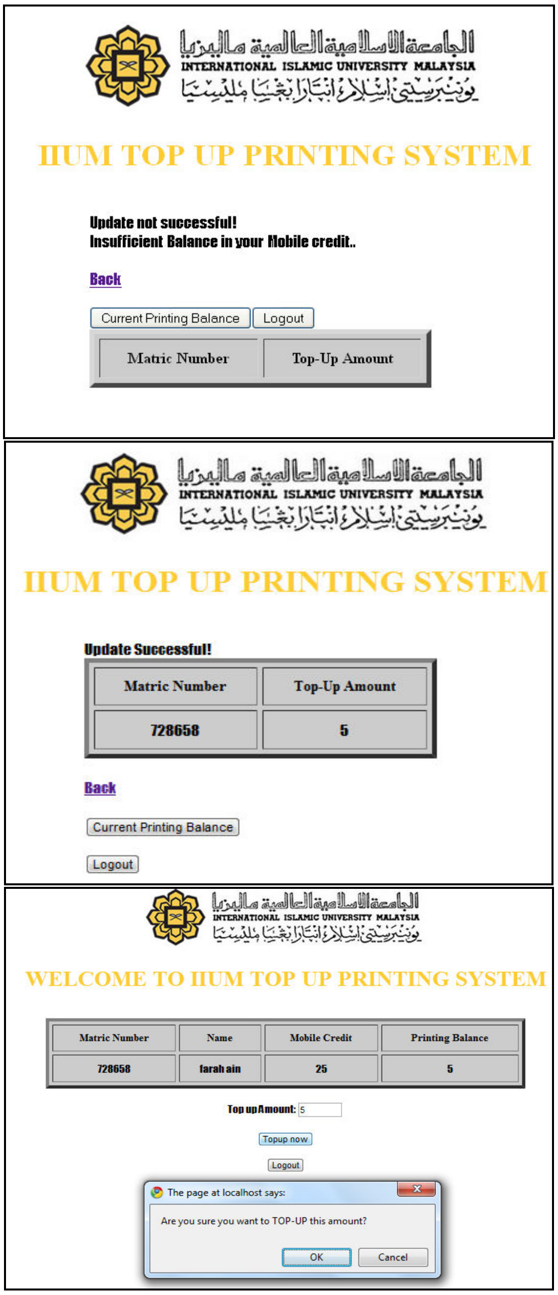
The implementation of user profile depends on the database structure and DBMS. However when user profile used the smart card, it has some limitations, which includes slow processing, area of the random-access memory very little, constrained stable memory, no autonomy, etc.. This situation makes traditional database technology irrelevant anymore. To overcome this problem Puchera et. al. propose a Pico DBMS (Pico-Data Base Management System) solution based on highly compact data structures, query execution without RAM and specific techniques for robustness [14].

In our previous work, there are three social aspects regarding electronic payment systems that provide users' trust and acceptance [17],[18],[19]:

- Anonymity: Protecting consumers' privacy by establishing security measures as well as preventing financial institutions and companies from tracking users by storing their relevant data, such as product preferences.
- User friendliness: Important factor for users when choosing the payment method entails convenience and ease of usage.
- Mobility: Users do not want to be tied to the PC when making an online purchase. Since many PCs have multiple users, preferred feature is payment system independence on computer hardware, i.e. system can be used anywhere [20][21].

Issues of anonymity and privacy are related to proper authentication, data integrity and non-repudiation (whereby participants are prevented from denying commitments made in a transaction). When talking about the convenience, questions of user friendliness and mobility come into the picture.

In order to improve user experience, online payment or banking system should guarantee security while money transaction activities remain simple and easy. System should be stable, update relevant information on time and record it accurately for proper account management [21].



IIUM TOP UP PRINTING SYSTEM

Update not successful!
Insufficient Balance in your Mobile credit..

Matric Number	Top-Up Amount

IIUM TOP UP PRINTING SYSTEM

Update Successful!

Matric Number	Top-Up Amount
728658	5

WELCOME TO IIUM TOP UP PRINTING SYSTEM

Matric Number	Name	Mobile Credit	Printing Balance
728658	farah ain	25	5

Top up Amount: 5

The page at localhost says:

Are you sure you want to TOP-UP this amount?

Fig. 10 Prototype sample screen shoot

Customers realize greater risk they are exposed to while conducting payments over the internet and that is one of the main obstacles for faster acceptance of e-commerce trend. Survey presented in one of the reviewed papers shows that, among consumers that do not use online payments, 43.44% are not confident because of "the security risk", 19.67% are not paying online because "they do not like online banking", 22.13% feel the payment procedure lacks convenience and the remaining 14.75% are not making online payments for "other reasons". The 63.76% of the participants believe that their personal financial information might go to a third party while using online payment systems. The survey also shows that a great number of participants lack awareness related to the security issues. So, for instance, 66.41% are not familiar with the concept of phishing [22].

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.

VII. CONCLUSIONS

NFC technology represents contactless standards toward the goal of global interoperability. This new evolving technology has the potential to revolutionise our daily lives in the near future.

Its versatility, interoperability, technology-enabling, security-ready characters makes it more attractive to develop and implement to suit our day-to-day activities, from consumers and business.

This study proposes Secured Mobile Payment using NFC Technology. Our approach used Mobile phone enabled NFC that acts as a middle interpreter to the original system. By using NFC, a contactless payment will be made when the mobile phone is touched with a tag reading device that will interact with the printing service.

As a proof of concept, "A Top-Up Printing System" has been developed to replace the existing system by using ACR

100 Reader with ACOS3 SIM card. By applying this, time for lining up in the queue is cut short and top-up process is available 24/7.

Currently MD5 algorithm is used to secure the password and the transaction. In the future we will enhance the encryption by using RSA algorithm or other better algorithm.

REFERENCES

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

[2] Patauner C., Witschnig H., Rinner D., Maier A., Merlin E. and E. Leitgeb, High Speed RFID/NFC at the Frequency of 13.56 MHz, The First International EURASIP Workshop on RFID Technology, RFID 2007. 24-25 September 2007. Pages 1-4.

[3] ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards, ISO/IEC. Available at http://www.iso.org. Accessed on 2nd January 2012**.**

[4] Want, R., Fishkin, K.P., Gujar, A. and 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. and T. Tuomisto. Physical Browsing Research. In: Workshop Pervasive Mobile. Interaction Devices (PERMID 2005), Munich, Germany, 2005. Pages 123-128.

[6] Haikio J., M. Isomursu, T. Matunmikko, A.Wallin, H. Ailisto and 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). 2007. Pages 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, Pages 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. Pages 81-86.

[9] Tie-Jun P., and Lei-Na Z., Mobile Payment System for Prepayment Meter. Proceedings of the 5th WSEAS Int. Conference on Information Security and Privacy, Venice, Italy, November 20-22, 2006. Pages 136-140.

[10] 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. Pages 137-141.

[11] NFC Forum. Available at http://www.nfc-forum.org/home. Accessed on 2nd January 2012**.**

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

[13] Garrido P.C. , Miraz G. M., Ruiz I. L. and Gómez-Nieto M. A., A Tool for the Tag Management for the Building of Smart Environments, Proceedings of the WSEAS International Conference on Applied Computer Science. Malta, 2010. Pages 520-524.

[14] Pucheral P., Bouganim L., Valduriez P. and Bobineau C.: PicoDBMS: Scaling down Database Techniques for the Smartcard. in VLDB Journal , 10(2-3), 2001.

[15] Balitanas M.O., and Kim T., Anti-Collision Protocol for RFID-Sensor Network and the Security Threats. Proceedings of the 12th WSEAS International Conference on Automatic Control, Modelling & Simulation. 2010. Pages 364-372.

[16] Mantoro T, Ayu M.A., Brotosaputro G., Ain N. F., and N. Ghazali. Secured Mobile Transaction Using NFC Technology: Top-Up Printing System. . Proceedings of 10th WSEAS International Conference on Information Security and Privacy (ISP '11) Jakarta, Indonesia 2011. Pages. 21-26.

[17] Ahmed A., and Mantoro T., "A User Profile for Information Filtering Using RFID-SIM Card in Pervasive Network", The IEEE 2nd International Conference on Multimedia Computing and Systems (ICMCS'11), 7-9 April 2011, Ouarzazate, Morocco.

[18] Mantoro T., and Milisic A. "Online Payment Procedure Involving Mobile Phone Network Infrastructure and Devices", The IEEE 2nd International Conference on Multimedia Computing and Systems (ICMCS'11), 7-9 April 2011, Ouarzazate, Morocco.

[19] Mantoro T, A. Milisic, and M. A. Ayu, Online Authentication Using Smart-Card Technology in Mobile Phone Infrastructure, The International Journal of Mobile Computing and Multimedia Communications (IJMCMC), Vol 3 (4). 2011. Pages 67-83.

[20] International Organization and Standardization. Proximity Card. ISO/IEC 14443, 2003. Available at http://wg8.de/sd1.html. Accessed on 2nd January 2012**.**

[21] Lee, Z.-Y., Yu, H.-C., and Ku, P.-J. (2001). An analysis and comparison of different types of electronic payment systems. Portland International Conference on: Management of Engineering and Technology, *2001*. (pp. 38-45).

[22] Karim, Z., Rezaul, K.M., and Hossain, A. (2009). Towards secure information systems in online banking. International Conference for: Internet Technology and Secured Transactions, 2009. (pp.1-6).

Teddy Mantoro, holds a BSc, an MSc and a PhD, all in Computer Science. He was awarded a BSc (Ir.) from Department of Informatics Engineering (Computer Science), Faculty of Information Technology, University of Budi Luhur, Jakarta, Indonesia, 1989. MSc from Department of Computer Science, School of Advanced Technology, Asian Institute of Technology, Bangkok, Thailand, 1994 and a PhD from Research School of Computer Science, the Australian National University (ANU), Canberra, Australia in 2006

He is currently working as an associate professor at School of Advanced Informatics, University of Technology Malaysia (UTM), Kuala Lumpur, Malaysia. His research interest is in Ubiquitous Computing, Pervasive Computing, Context Aware Computing and Intelligent Environment. He has authored more than 100 research papers, 4 academic books, several book chapters and has four patents pending to his credits in the area of pervasive/ubiquitous computing.

Media A. Ayu, received her BSc (hons) in Agroindustrial Technology from Bogor Agricultural University (IPB), Bogor, Indonesia and MSc in Industrial Engineering from School of Advanced Technology, Asian Institute of Technology, Bangkok, Thailand. She has graduated with PhD in Engineering and Information Science from School of Engineering, the Australian National University (ANU), Canberra, Australia.

She is currently working as an assistant professor in Faculty (Kulliyyah) of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), Gombak, Kuala Lumpur. She has published more than 50 papers in international conference and journals, several book chapters and academic books. Her research interest is around the area of intelligent environment, smart applications, activity recognition and education technology.

Goenawan Brotosaputro holds a BSc and an MSc in Computer Science. He was awarded a BSc from Department of Informatics Engineering (Computer Science), Faculty of Information Technology, University of Budi Luhur, Jakarta, Indonesia, 1993. MSc from Department of Computer Science, School of Advanced Technology, Asian Institute of Technology, Bangkok, Thailand, 1997.

He is currently a dean at Faculty of Information Technology, University of Budi Luhur, Jakarta, Indonesia and pursue his PhD in Gadjah Mada University. His research area is in digital image processing, feature based image processing and content based image retrieval.

Nur F. Ain and **Noorzalina Ghazali** received BSc degree from Department of computer Science, KICT, International Islamic University Malaysia, 2011. Both of them are currently working as assistant researcher at Integ Lab, Department of computer Science, KICT, International Islamic University Malaysia.