Using RFID to Enhance Mobile Banking Security

Zakaria Saleh
MIS Department, IT faculty
Yarmouk University
Irbid, Jordan
zzaatreh@yu.edu.jo

Izzat Alsmadi
CIS Department, IT faculty
Yarmouk University
Irbid, Jordan
ialsmadi@yu.edu.jo

***Abstract*— Mobile banking is introducing a new generation of location-independent financial services using mobile terminals. This facilitates allowing users to make payments, check balances, transfer money between accounts and generate statements of recent transactions on their cellular phones. While providing , anywhere, anytime banking to the user, the service should be secure and security needs to be implemented at various levels, starting from the SIM card security, mobile software security, and secure customer access to banking services. Banks rely on users having their mobile phones with them all the time. Hence, as a mean for security measures, banks can send alerts, anytime, in order to provide an enhanced security and services. This paper analyzes the security issues in Mobile Banking, and proposes an improved security to the mobile banking services using RFID.**

Key words: Mobile banking, security, RFID, Wireless communication, Pervasive Computing, smart cards, and contactless payment, wireless security, and e-commerce.

I. INTRODUCTION

Mobile banking is set to reform the way people manage their money, and while Internet banking brought banks to the desktop, the Mobile banking is bringing it right into users' pockets. However, in an age of uncontrolled cyber crime, security is the primary concern. The remarkable increase in cellular phone usage has been followed by an increase in mobile fraud. Many users are concerned about the security aspect when carrying out financial transactions over the mobile network.

Mobile is often the only means of access available for millions of users in many countries. A report published by IMS [62] on Mobile Applications and Services indicates that mobile penetration in many developing markets is far higher than that of banking or fixed line infrastructure. However, lack of security is seen as the biggest deterrent to the widespread adoption of mobile financial services. KPMG LLP examined trends in the use of mobile technology of more than 4,000 people in 19 countries worldwide, where the 91 % respondents said they had never tried banking through a mobile device, and 48% (those respondents who have not conducted banking through a mobile device) cited security and privacy as the primary reason. This research will investigate the current security within mobile banking while focusing on users' authentication, and propose a model that will further enhance access security using RFID.

What is mobile banking?

The Mobile Banking environment requires both a Bank and a Mobile Network Operator (MNO) to deliver a Transactional or informational banking service to a consumer through the mobile phone. The implementation of wireless communication technologies may result in more complicated information security problems [23]. In developing countries, the role of the mobile phone is more extensive than in developed countries, as it helps bridge the digital divide. Even with initiatives like the One Laptop per Child (OLPC), the mobile penetration in many developing markets is far higher than that of banking or fixed line infrastructure [62]. People carry their mobile phones at all times, and services beyond voice communication are expected by users all over the globe. Users desire the same kind of services they get through an Internet-connected PC to be available through their mobile phone.

Mobile banking allows users to perform everyday banking functions using the mobile phone. All the major banks offer some type of mobile service for bill payment, funds transfers, checking balances, and receiving alerts [19]. Financial institution use mobile banking in one of different modes:

- Mobile Text Banking: In their simplest form, mobile banking services enable enables users to retrieve information

about bank accounts from a mobile phone using Short Message Service (SMS) .

• Mobile Web/Client Banking: Using a mobile phone's data connection, this service provides users with an interface and a login with password feature.

Mobile Text Banking

SMS Based applications may be the simplest form of mobile banking implementation [18]. The solution is not intuitive and has no aesthetic value but is as simple as sending an SMS. SMS is used primarily as an informational banking tool as opposed to transactional banking. However, SMS can provide a pro-active functionality to send brief text messages to customers ensuring that the relevant information is provided to the user at the "right" place, at the "right" time [21]. The reason being that transactional banking requires certain levels of security, and while SMS is encrypted using the standard GSM encryption across the air, the SMS message is store in plaintext format, and the current SMS banking design has neglected the fact that some employees working for the cellular service provider can have access to the transmitted message at the service stations. Therefore using plaintext SMS message to send security details is not sufficiently secure [20]

Mobile Web/Client Banking

Mobile Web/Client Banking is a browser-based application, where users would access the Internet from a mobile phone. It usually offer 24/7 real-time access to users accounts right from a Web-enabled cell phone, allowing users to access account information, pay bills, transfer funds, or find a in some cases nearby ATM or Branch from the handheld mobile device[24]. The service requires no special software. However, For Mobile Web/Client Banking, the phone would have to support web browsing [22], which usually requires a "data" support plan as part of the mobile service.

The Radio Frequency Identification (RFID) system at the very simplest level, Radio Frequency Identification (RFID) system consists of a tag (or transponder) and reader (or interrogator) with an antenna. Tags can be passive with no power source or active. The technology allows for the transmission of a serial number wirelessly, using radio waves. A typical RFID transponder (tag) which can be passive (no battery) or active (with battery) consists of an antenna and an integrated circuit chip which is capable of storing an identification number and other information [16]. The reader sends out electromagnetic waves. The tag antenna is tuned to receive these waves. A passive RFID tag draws power from the field created by the reader and uses it to power the microchip's circuits. The chip then modulates the waves that the tag sends back to the reader, which converts the new waves into digital data. RFID systems use many different frequencies, but generally the most common are low-frequency (around 125 KHz), high-frequency (13.56 MHz) and ultra-high-frequency or UHF (860-960 MHz). Microwave (2.45 GHz). The RFID operating frequencies and associated characteristics are illustrated in table 1[17].

TABLE I: RFID OPERATING FREQUENCIES AND ASSOCIATED CHARACTERISTICS.

Band	Low frequency	High frequency	Ultra high frequency	Microwave
Frequency	30–300kHz	3–30MHz	300 MHz–3GHz	2–30 GHz
Typical RFID Frequencies	125–134 kHz	13.56 MHz	433 MHz or 865 – 956MHz 2.45 GHz	2.45 GHz
Approximate read range	less than 0.5 meter	Up to 1.5 meters	433 MHz = up to 100 meters 865-956 MHz = 0.5 to 5 meters	Up to 10m
Typical data transfer rate	less than 1 Kbit/s	About 25 Kbit/s	433–956 = 30 Kbit/s 2.45=100 Kbit/s	Up to 100 Kbit/s
Typical use	Animal ID Car immobilizer	Smart Labels Contact-less travel cards	Specialist animal tracking Logistics	Moving vehicle toll

A smart phone with RFID tag for ATM communication: Experiments and Analysis; RFID enabled cell phones

A paper published in RFID journal in 2004 [33] predicted that within 5 years, 50% of cell phones will include RFID chips to use Near Field Communication (NFC), a two-way technology. The service was supposed to automatically connect cell phones with services in a similar fashion that occurs between airplanes and air traffic controllers on earth. NFC technology uses short-range RFID transmissions that provide easy and secure communications between various devices [33]. The important element in this proposal is the automatic peer to peer communication between RFID equipments without user involvement. The cell phone can be connected to RFID enabled applications such as websites, ATMs, restaurant outlets, GPS, etc. Files or video transfer is also possible similar to the current Bluetooth technology. In order to make this work, an NFC chip embedded in a phone can act as an RFID reader when the phone is on and a passive smart label or RFID tag when the phone is off.

There are two main ways to integrate RFID with a wireless smartphone: "A smartphone with RFID tags" and "a smartphone with an RFID reader" [34]. The first one is a typical cell phone that has embedded or attached an RFID chip with some identification information programmed on it. Its antenna is also equipped with RF antenna to be able to communicate with the RFID readers when they are within

the range. The RFID tag information is sent to the reader and the reader can write information back to the phone.

On the other hand, the second type contains an RFID reader that can collect data from various RFID tags with also an RF antenna.

However, the technology is not going very smooth. The limited UHF bandwidth and dense reader problems are still major issues to adoption

NFC and ISO 14443 13.56 standard for NFC and RFID enabled phones

Near Field Communication (NFC) is a standards-based, short-range wireless connectivity technology that enables simple and safe two-way interactions among electronic devices [61].An ISO standard (14443) is proposed for NFC RFID enabled phones operating at 13.56 MHz in close proximity with a reader antenna. 14443 has certain features that make it particularly well-suited to applications involving sensitive information such as contactless credit cards as data transmitted is encrypted and the transmission is very short. Physical contact between the reader and the transponder is not necessary. Even a line of sight is not required. A tag may be attached to a package in the form of a smart label, worn on a person hand, attached to a ring of keys or carried in a purse along with conventional credit cards.

Some of the sought goals from using NFC RFID enabled phones are: Making payments using contactless card readers, reading account or status information from any equipment that has RFID such as stores items, discounts from smart posters or smart billboards, etc, store tickets to access transportation gates, parking garages or get into events, and many others.

II. LITERATURE REVIEW

Recently, there are many examples for RFID enabled applications. For example, Objecs company (iwww.objecs.com) has developed three, cell-phone readable tablets suitable for gravestones that once touched can read information about the diseased. In 2005, Wal-Mart announced its decision to require its suppliers to be ready to track goods using RFID tags. Other fields of applications for RFIDs are: Transport and logistics: toll management, tracking of goods, security and access control: tracking people (students etc.), controlling access to restricted areas, supply chain management: item tagging, theft-prevention, medical and pharmaceutical applications: identification and location of staff and patients, asset tracking, counterfeit protection for drugs, manufacturing and processing: streamlining assembly line processes, agriculture: tracking of animals, quality control, public sector, sports and shopping [38]. There are some other applications that are expected to be used with RFID enabled smartphones. Examples of such applications include: web information retrieval, data transmission, automated messaging, voice services, device integration, presence indication, and mobile payments and money transactions.

The focus on this literature review will be on FRID applications in cell phones and more particularly for banking applications. A smartphone with an RFID reader can be placed on a tag located on an equipment and use the wireless network to browse through the Internet [35]. Similar to wireless sensors, RFID enables phones can collect data at real time for many applications such as automatic material, items, weather status tracking, etc.

Currently, there are many phone companies such as Nokia, Motorola, Apple, Minec who are designing or developing RFID enabled phones [35, 36, 37]. In 2004, Nokia introduced its first RFID enabled phone 5140. Figure shows the user interface for Nokia 3220 that is also RFID enabled.

Figure 1. Cell phone screen with RFID tag feature

Mobile payment with RFID enabled phones is already available in some regions of the world. For example, in Japan and Germany, train users can pay their tickets using their enabled phones. Similar approaches are applied for airline check-in services. In France, Carrefour embraces RFID payments by card and phone.

In the following paragraphs, we will mention some papers that discussed using wireless phones in the security of mobile banking which is the focus of this subject. Some papers discussed mobile banking security, evaluations and metrics in general and examples of threats. [42, 44, 49, 50, 51, 53, 54, 56, 57]. Narendiran et al discussed using PKI security framework for mobile banking [40]. Shahreza discussed using stenography for improving mobile banking security [41]. Hossain et al [43] discussed enhancing security of SMS for financial and other services [43]. Manvi et al, Itani et al, and Krol et al proposed using J2EE and J2ME for enhancing mobile banking security [45, 47, 58]. Hwu et al proposed an encrypted identity mechanism for financial mobile security [46]. Ghotra et al proposed using Secure Display Devices (SDD) with phones for secure financial transactions [48]. Zhu et al and Rice et al proposed a framework for secure mobile payments based on cryptography [52, 55]. Henkel et al discussed the idea of

secure remote cash deposit [59]. Finally, in a similar goal to this paper, Arabo proposed utilizing phones for securing ATM transactions [60]

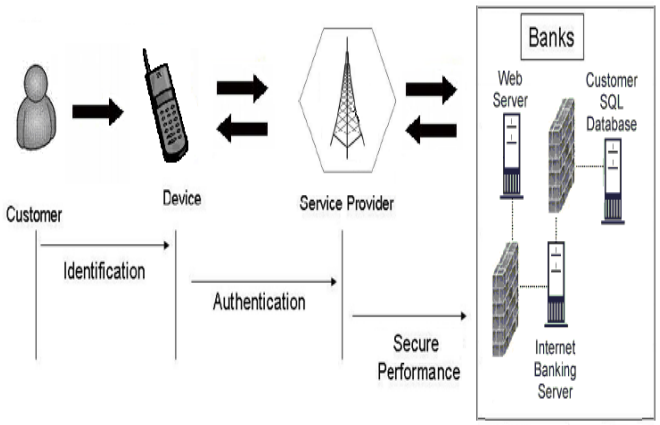

Figure 2: Mobile Banking Security System

III. THE PROPOSED SOLUTION FRAMEWORK

A. *Mobile Banking Security System*

Figure 2 shows a typical mobile banking system using cell phones. In mobile banking as with online and traditional banking methods, security is a primary concern. Banks announce that all standard "Distance" Banking security features are applied at login including multifactor authentication by soliciting multiple answers to challenge questions. However, this may be considered strong authentication but, unless the process also retrieves 'something you have' or 'something you are', it should not be considered multi-factor. Nevertheless, Data security between the customer browser and the Web server is handled through Secure Sockets Layer (SSL) security protocol. SSL protects data in three key ways: 1) Authentication to ensure that a user is communicating with the correct server; 2) Encryption to make transferred data unreadable to anyone except the intended recipient; 3) Data integrity and verify that the information sent by users was not altered during the transfer (usually If any tampering has occurred, the connection is dropped) [6]. There are no bouts that banks have taken every precaution necessary to be sure that information is transmitted safely and securely. The security of mobile banking application is addressed at three levels (see Figure 2). The first concern is the security of customer information as it is sent from the customer's mobile phone to the Web server. The second area concerns the security of the environment in which remote access to the banking server and customer information database reside. Finally, security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web site.

Mobile Banking gives users instant connectivity to their accounts anytime, anywhere using the browser on their mobile device, allowing users to access account details, history and check account balances, which increase convenience for the consumer, while reducing banking costs. Value-added services are the key for long-term survival online banking. However, given the uncertain nature of the transmission environment, there are security shortfalls in the present mobile banking implementations such as security problems with GSM network, SMS/GPRS protocols and security problems with current banks mobile banking solutions [63].

Services have security and privacy barriers that causes resistance and slows down the adoption, a recent study shows that 91 % of the respondents said they had never tried banking through a mobile device, and 48% of those who have not conducted banking through a mobile device indicated that security and privacy are the primary reason . A lot still prefer traditional telephone banking or ATMs and service terminals [1]. Thus, bank managers could enhance adoption of mobile banking services by concentrating their marketing efforts on factors under those barriers.

B. *Proposed Framework Modification*

Banks providing mobile services need to work on reducing security risks and improving customers' trust. Therefore, in an attempt to help banks achieve a high level of trust of mobile banking, this study has developed a module that shall further tighten security of mobile banking, and reduce the associated risk (see Figure 3), by adding a Radio-Frequency Identification (RFID) reader to the mobile banking system, on the end user's mobile phone.

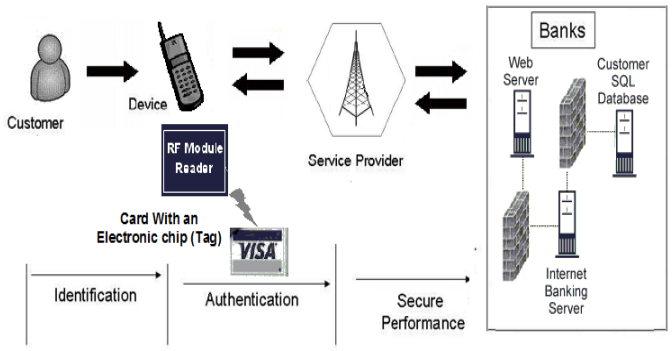

Figure 3: Proposed Module to Increase Mobile Security

- **Proposed hardware changes: Cell phones with RFID tags**

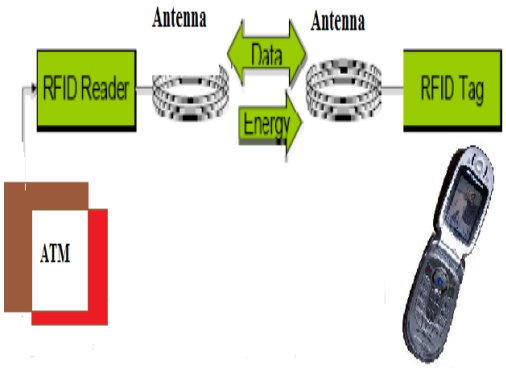

Figure 4. Connecting cell phone with ATMs through RFID

RFID tags, that are composed of an antenna connected to an electronic chip. Figure 4 shows a simple design to connect cell phones with the ATM system. When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna. The RFID reader transmits radio-frequency queries, tags respond by sending back information they enclose. Finally, a Mobile phone hosting a specific RFID application pilots the reader and processes the data it sends. RFID does not require a line-of-sight reader. This whole process is depicted in Figure SSS.

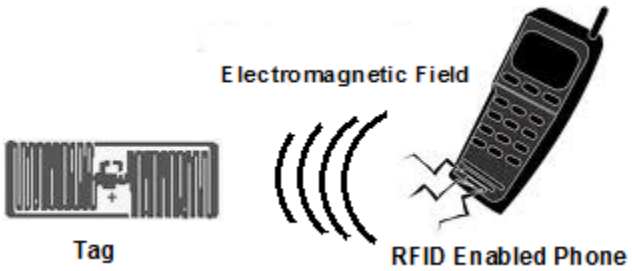

Figure 5. RFID enabled phones.

- **Proposed software changes, Programming the cell phone**

The major modification proposal for phones is hardware. Once, the phone is NFC RFID enabled, accompanied software can be included to be able to synch the phone with the RFID reader. Other expected tasks will depend whether we want the RFID tag in the phone to be active or passive, or if we want it to send and receive signals or just be a passive receiver or responder (Figure 5).

- **Programming the ATM and the banking system**

ATM user interface should be modified to include adding a new security rule for login. Figure 6 and 7 show the proposed use login use case for ATM that include verifying customers identity with their RFID tag along with the card number and PIN.

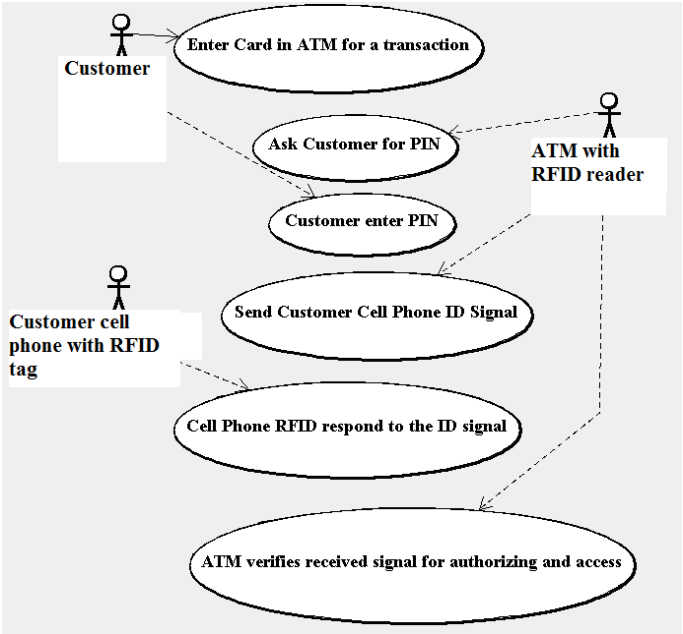

Figure 6: Use case of proposed modification on ATM access authentication

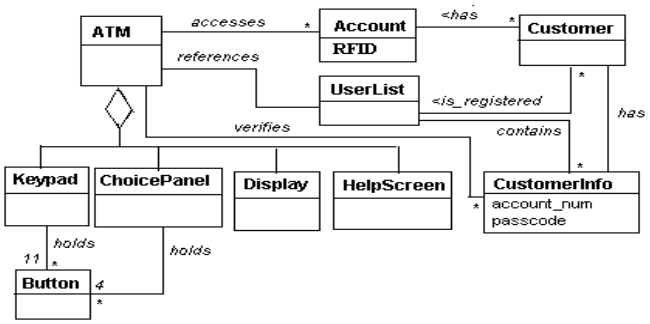

Figure 7. Typical ATM display model, with RFID attribute added to customer accounts

The banking system should be also modified to be able to deal with users RFID tags creation, cancelation, update, verification, etc. Eventually this can be incorporated with the database management system where the tag ID will be added as an attribute to users' accounts.

C. Conclusion and Future Work

In this paper, we proposed utilizing NFC RFID enabled phone for mobile banking security. This proposal is expected to solve problems with identity or credit card thefts. Users will be required to have their smart phones with them to be able to process ATM transactions. This is convenient as

users usually have their mobile phones with them all the time. Technology can help facilitating this service without breaking bank or users' privileges or security.

REFERENCES

[1] Berger, S. C., and Gensler, S. (2007) "Online Banking Customers: Insights from Germany". Journal of Internet Banking and Commerce, , vol. 12, no.1.

[2] Betts, W. (2000). Defying denial of service attacks. Network Magazine, 16(5), 36-41

[3] Greenberg, P. A. & Caswell, S. (February 1, 2001). Online banking fraud raises more security concerns. E-Commerce Times, ,. Retrieved August 14, 2003, http://www.ecommercetimes.com/perl-/story/?id=2390

[4] Cheung, C. and M. Lee (2000). "Trust in Internet Shopping: a proposed model and Measurement Instrument". Proceedings of the Americas Conference on Information Systems, pp. 681-689

[5] Dandash, O., Le, P. D., and Srinivasan, B. (2007) "Security Analysis for Internet Banking Models". Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, July 30, 2007-Aug. 1 2007 Page(s):1141 - 1146

[6] Freier A., Karlton P., and Kocher P. (1996). "SSL 3.0 Specification". draft-freier-ssl-version3-02.txt, Netscape Communications

[7] Foster, A. (2002) "Federal Officials Issue Alert on Security of College Networks." Chronicle of Higher Education, July 5, 2002, A32.

[8] Read, B. (2002). "Delaware Student Allegedly Changed Her Grades Online." Chronicle of Higher Education, August 2, 2002, A29.

[9] Saleh, Z. I. (2003). "An Examination Of The Internet Security And Its Impact On Trust And Adoption Of Online Banking ", Unpublished PhD Dissertation, Capella University

[10] Sarma, S. "Integrating RFID" Queue, Volume 2 Issue 7, ACM Press, 2004.

[11] Stewart, D. Pavlou and S. Ward (2001). "Media Influences on Marketing Communications," In Media Effects: Advances in Theory and Research, J. B. a. D. Zillmann (Ed.), Erlbaum, Hillsdale, N. J.

[12] Koufaris, M.and Hampton-Sosa, W.(2005). "The Effect of Web Site Perceptions on Initial Trust in the Owner Company" International Journal of Electronic Commerce Vol 10,No 1, Pages 55-81

[13] Laukkanen, P., Sinkkonen, S., Laukkanen, T., and Kivijärvi, M.(2007). "Consumer Resistance and Intention to Use Internet Banking Services. EBRF 2007 conference, 25-27 September 2007. Finland

[14] Want, R. "RFID Magic" Queue, Volume 2 Issue 7, ACM Press, 2004.

[15] Woodforest (2007). "Frequently Asked Questions". Retrieved August 12, 2007 <http://www.woodforest.com/default.aspx>.

[16] Galehdar, A. Thiel, D & O'Keefe S (2007). "Antenna Efficiency Calculations for Electrically Small, RFID Antennas" IEEE Antennas and Wireless Propagation Letters, VOL. 6, 156-159.

[17] IET (2006). Radio Frequency Identification Device Technology (RFID) Factfile. The Institution of Electrical Engineers.
http://www.iee.org/Policy/sectorpanels/control/rfid.cfm

[18] Mallat, N, Rossi, M, & Tuunainen, V. (2004). "Mobile Banking Services". Communications of The ACM, Vol. 47, No. 5. 42-46

[19] Adler, J.(2009)"Is Mobile Banking Getting Connected?". DIGITAL TRANSACTIONS.NET, VOL 6 No. 6. P 28-33

[20] Chong M (2006). "Security of Mobile Banking:Secure SMS Banking ". Data Network Architectures Group. University of Cape Town, South Africa

[21] Rajnish Tiwari, R. Buse, S. & Herstatt C. (2006)"Mobile Banking As Business Strategy: Impact Of Mobile Technologies On Customer Behaviour And Its Implications For Banks". Portland International Conference on Management of Engineering and Technology (PICMET) 2006, 8–13 July 2006, Istanbul, Turkey.

[22] Kuwayama, J. (2008) "New Mobile Banking Products Present Opportunities And Challenges". Printed in Wisconsin Community Banking News June 2008.

[23] Jin Nie Xianling Hu (2008). "Mobile Banking Information Security and Protection Methods". Computer Science and Software Engineering, 2008 International Conference on, 12-14 Dec. 2008, 587 – 590

[24] Deb M. (August 2009)."Keep Your Finances Literally at the Tip of Your Fingers". Bank of America Mobile Banking, REVIEW – Retrieved on March 2010 from www.appshouter.com/iphone-app-review-–-bank-of-america-mobile-banking/

[25] Mohammed A Qadeer, Nadeem Akhtar, Shalini Govil, Anuja Varshney, A Novel Scheme for Mobile Payment using RFID-enabled Smart SIMcard, 2009 International Conference on Future Computer and Communication

[26] Jiahao Wang1, 2, Edward C. Wong2, Terry Ye3, PGMAP: A Privacy Guaranteed Mutual Authentication Protocol Conforming to EPC Class 1 Gen 2 Standards, IEEE International Conference on e-Business Engineering, 2008.

[27] Jiahao Wang1, 3, Terry Ye2, Edward C. Wong3, Privacy Guaranteed Mutual Authentication on EPCglobal Class 1 Gen 2 Scheme, The 9th International Conference for Young Computer Scientists, 2008.

[28] Ching-Nung Yang, Jie-Ru Chen, Chih-Yang Chiu, Gen-Chin Wu, and Chih-Cheng Wu, Enhancing Privacy and Security in RFID-Enabled Banknotes, 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications.

[29] D. Malocha, N. Kozlovski, B. Santos, J. Pavlina, M. A. Belkerdid and TJ Mears, II, ULTRA WIDE BAND SURFACE ACOUSTIC WAVE (SAW) RF ID TAG AND SENSOR, Military Communications Conference, 2009. MILCOM 2009. IEEE.

[30] Anand Oka and Lutz Lampe, Distributed Scalable Multi-Target Tracking with a Wireless Sensor Network, IEEE Communications Society, 2009.

[31] Xu Guangxian, The Research and Application of RFID Technologies in Highway's Electronic Toll Collection System, Wireless Communications, Networking and Mobile Computing, 2008.

[32] Mohamed Gamal El Din, Bernd Geck, and H. Eul, Adaptive Matching for Efficiency Enhancement of GAN Class-F Power Amplifiers, IEEE MTT-S International Microwave Workshop on Wireless Sensing, 2009.

[33] Claire Swedberg, Developing RFID-Enabled Phones, RFID Journal, July 9th 2004.

[34] Dora Karali, Integration of RFID and Cellular Technologies1, Technical report/ white paper UCLA-WINMEC-2004-205-RFID-M2M.

[35] Nokia's RFID Kit, http://www.nokia.com/cda1?id=55739.

[36] RFID Journal, Nokia Unveils RFID Phone Reader, March 17, 2004, Gerhard Romen

[37]. Minec Web Site: http://www.minec.com/

[38] Christoph Seidler, RFID Opportunities for mobile telecommunication services, ITU-T Lighthouse Technical Paper, 2005.

[39] Elham Ramezani, Mobile Payment, 2008.< http://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-mobile-payment-Ramezani.pdf>.

[40] C. Narendiran1 S. Albert Rabara2 N. Rajendran, PUBLIC KEY INFRASTRUCTURE FOR MOBILE BANKING SECURITY, Proceedings of the World Wireless Congress, WWC`2008

[41] Mohammad Shirali-Shahreza, Improving Mobile Banking Security Using Steganography, International Conference on Information Technology (ITNG'07).

[42] Jin ,Nie, Xianling,Hu, Mobile Banking Information Security and Protection Methods, 2008 International Conference on Computer Science and Software Engineering

[43] Md. Asif Hossain1, Sarwar Jahan, M. M. Hussain, M.R. Amin, S. H. Shah Newaz, A Proposal for Enhancing The Security System of Short Message Service in GSM. 235-240, ASID ISBN: 978-1-4244-2585-3", 2008.

[44] C.Narendiran, S.Albert Rabara, N.Rajendran, Performance Evaluation on End-to-End Security Architecture for Mobile Banking System, Wireless Days, 2008. WD '08. 1st IFIP

[45] S. S. Manvi, L. B. Bhajantri, Vijayakumar.M.A, Secure Mobile Payment System inWireless Environment, 2009 International Conference on Future Computer and Communication

[46] Jing-Shyang Hwu, Rong-Jaye Chen, and Yi-Bing Lin, An Efficient Identity-based Cryptosystem for End-to-end Mobile Security, IEEE

TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, SEPTEMBER 2006

[47] Wassim Itani and Ayman I. Kayssi, J2ME End-to-End Security for M-Commerce, Wireless Communica- tions and Networking - WCNC 2003

[48] Sandeep Singh Ghotra, Baldev Kumar Mandhan, Sam Shang Chun Wei, Yi Song, Chris Steketee, Secure Display and Secure Transactions Using a Handset, Sixth International Conference on the Management of Mobile Business (ICMB 2007)

[49] Mahesh .K. harma , Dr. Ritvik Dubey, Prospects of technological advancements in banking sector using Mobile Banking and position of India, 2009 International Association of Computer Science and Information Technology

[50] Jongwan Kim, Chong-Sun Hwang, Applying the Analytic Hierarchy Process
to the Evaluation of Customer-Oriented Success Factors in Mobile Commerce, Services Systems and Services Management, 2005. Proceedings of ICSSSM '05.

[51] Toshinori Sato, and Itsujiro Arita, In Search of Efficient Reliable Processor Design, Proceedings of the 2001 International Conference on Parallel Processing,

[52] Y. Zhu and J. E. Rice, A Lightweight Architecture for Secure Two-Party Mobile Payment, 2009 International Conference on Computational Science and Engineering.

[53] Matthew Freeland, Hasnah Mat-Amin, Khemanut Teangtrong, Wichan Wannalertsri,
Uraiporn Wattanakasemsakul, Pervasive Computing: Business Opportunity and Challenges, Management of Engineering and Technology, 2001. PICMET '01.

[54] Zhenhua Liu and Qingfei Min, and Shaobo Ji, An Empirical Study on Mobile Banking Adoption: The Role of Trust, 2009 Second International Symposium on Electronic Commerce and Security

[55] J. E. Rice and Y. Zhu, A Proposed Architecture for Secure Two-Party Mobile Payment, IEEE PacRim09

[56] Toshinori Sato'y, and Itsujiro Arital, Evaluating Low-Cost Fault-Tolerance Mechanism for Microprocessors on Multimedia Applications, Proceedings of the 2001 Pacific Rim International Symposium on Dependable Computing.

[57] Shan chu, and Lu yao-bin. The effect of online-to-mobile trust transfer and previous satisfaction on the foundation of mobile banking initial trust, 2009 Eighth International Conference on Mobile Business.

[58] Przemyslaw Krol, Przemysław Nowak, and Bartosz Sakowicz, Mobile Banking Services Based On J2ME/J2EE, CADSM'2007.

[59] Joseph Henkel, and Justin Zhan. Remote Deposit Capture in the Consumer's Hands, IEEE 2010.

[60] Abdullahi Arabo, Secure Cash Withdrawal through Mobile Phone/Device, Proceedings of the International Conference on Computer and Communication Engineering 2008.

[61] Patrick Henzen, Near Field Communication Technology and the Road Ahead, NFC Forum, 2007.

[62] IMS (2009). "900M Users for Mobile Banking and Payment Services in 2012 - 29 May 2008". Research Published July 8, 2009.

[63] Chikomo, K., Chong, M., Arnab, A. & Hutchison A. (2006). "Security of Mobile Banking". Technical Report CS06-05-00, Department of Computer Science, University of Cape Town.