Innovative Secure Mobile Banking Services

doi:10.3991/ijim.v5i1.1516

Mousa Al-Akhras[1], Rizik Al-Sayyed[1], Marwah Alian[2] and Doaa Qwasmi[1]
[1]The University of Jordan, Amman, Jordan
[2]Isra University, Amman, Jordan

***Abstract*—Due to the widespread use of computer technologies in almost all aspects of life, organisations that are connected to the Internet started extending their services to their customers to include new applications and services that satisfy their customers' desires to make better businesses. One of these emerging applications is mobile banking. The term mobile banking (or m-banking) describes the banking services that the user can perform via a mobile device ubiquitously at anytime and from anywhere. In order for users to access their accounts, they need a mobile device and network connectivity. Therefore, sitting in front of a computer is not a requirement anymore; accessing accounts can occur while users are waiting their turn at the dentist clinic or relaxing at the beach!**

This paper explores the opportunities of using mobile technology in the electronic banking (e-banking) sector to enhance existing banking services by moving toward m-banking using mobile devices and wireless media that can provide opportunities for ubiquitous access to the banking services as mobile technologies can be used at anytime and from anywhere. The technical problems encountered while using the mobile devices presents some technical difficulties and challenges for the m-banking.

In this paper we introduce a mobile system that demonstrates the flexibility gained out of this technology and covers the major aspects of such kind of applications. The proposed system covers two parts: the customer services (user interface) and the security aspects. In the user interface part, banking facility is provided to the user through the mobile device to implement banking transactions. The model provides customers with the services: billing payments, transferring of funds, viewing of customer's accounts and transactions, allowing the user to change his/her password and request a cheque book. The application takes into consideration security aspects, it satisfies the following security requirements: Authentication, Confidentiality and Authorisation.

This paper introduces the advantages and disadvantages of using mobility in the banking sector. Furthermore, this paper also presents the security, suitability and feasibility aspects of using m-banking in terms of technology and usability.

***Index Terms*—Customer Relationship Management, CRM, Electronic Banking, e-banking, Mobile Banking, m-banking, Security, Ubiquitous.**

I. INTRODUCTION

The pioneer work of Mark Weiser on ubiquitous computing [1], has paved the way for more focus among researchers on taking advantage of these technologies in several application areas in the commercial and business domains. Available ubiquitous technologies such as wireless communications, positioning services, and sensor network technologies will have an immense impact on various areas of business. Customer Relationship Management (CRM) as a technology-based strategic implementation for company relations with customers is becoming a business function and its scope has been expanded via utilising the existing ubiquitous technologies [2, 3].

The initial wave of applications aimed to deliver CRM through electronic media was named electronic CRM (e-CRM) [4]**.** It began to use the Internet to change the ways in which companies reach customers. Later, the concept of mobile CRM (mCRM) [5] which uses mobile medium such as mobile phones or Personal Digital Assistants (PDAs) for managing customer relationships was presented. The term ubiquitous CRM (uCRM) refers to the process of providing the customers with the right service anywhere and at anytime in a proactive manner.

Several businesses have been affected by the above waves of CRM development. One of the main businesses to be affected by this development is the banking sector. The widespread use of Internet-enabled mobile phones and PDAs makes the transformation of banking services to mobile devices a successor to Internet Banking or electronic banking (e-banking), and this created a new subset of electronic banking, called mobile banking (m-banking) [6].

Internet Banking gives the customers the ability to access their bank accounts anytime. Customers can check out their account details, perform transactions like transferring money from one account to another, get their bank statements, and pay their bills all while they are at their homes, offices, or at any place equipped with an Internet facility. The biggest limitation of Internet banking is the requirement to have a PC with an Internet connection. M-Banking, however, reduces this requirement to only a mobile device [7].

M-Banking is defined as the use of mobile devices such as a mobile phone to perform banking transactions or to access financial services. With mobile banking, clients that may be in the most remote location and have a mobile phone with network connectivity, can access their accounts anytime and from anywhere in what is termed ubiquitous computing [8].

As m-banking is the successor for e-banking, it is divided into two main areas; First: mobile brokerage which covers securities transactions with mobile devices. Second: mobile banking which covers account management with mobile devices [6].

The simplest form of mobile banking services enables users to receive information about their account balances

through Simple Messaging Service (SMS). But in a broader sense, the new Wireless Access Protocol (WAP) and Java-enabled mobile devices that use General Packet Radio Service (GPRS) support a wider variety of banking services such as fund transfers between accounts, stock trading, and confirmation of direct payments via the phone's micro browser [9]. M-Banking is being deployed using mobile applications developed on one of four channels: Interactive Voice Response (IVR), SMS, WAP and Standalone Mobile Application Clients [7].

The rest of this paper is organised as follows. Section II introduces a related literature review. Section III introduces mobile banking services for the proposed model. Section IV introduces the security aspects in mobile banking in general. Section V presents the security aspects in the proposed mobile banking system. Section VI details the components and services of the proposed mobile banking system. Implementation details are presented in section VII. Section VIII draws conclusions and presents possibilities for future work.

II. LITERATURE REVIEW

The Global System for Mobile Communications (GSM) association indicated that there were over 3.6 billion GSM subscribers in the world before the middle of the year 2008 [10] and about 1.2 million new daily connections [11]. According to this fast growth, it is predicted that the number of subscribers will exceed 4 billion by the end of the year 2010 [11]. Financial services, especially mobile banking services are greatly affected by this growth. According to Green Research [12], "the number of active users of mobile banking and related financial services worldwide is forecasted to increase from 55 million in 2009 to 894 million in 2015". This increase will have great impact on the type of m-banking applications required by different types of customers. When the GSM association began the Mobile Money Transfer programme in 2007, the target was to make the transfer of funds services easier for workers and to introduce mobile financial services as a new application [13].

In the developing countries, only a few banks are offering m-banking services. However, the Philippines, South Africa and Kenya have successfully introduced these services. Some of these servicers for example include Globe Telecom's GCash from the Philippines and Safaricom's M-PESA from Kenya. They both use a text-based SIM (SIM stands for Subscriber Identity Module, a small memory chip) Application Toolkit implementation to provide their services. In South Africa, Nedbank and Standard bank offer their services through WAP [14].

Barati and Mohammadi proposed a model to solve the consumer resistance to innovation by integrating Tense Aspect Modality (TAM) with an innovation resistance theory and with another variable named as "social and cultural factor". In order to facilitate the acceptance of m-banking, they also considered other conditions such as the familiarity of the mobile device, the usage time and technology use skills that were based on Unified Theory of Acceptance and Use of Technology (UTAUT) [15].

Shammot and Al-Shaikh surveyed the branch managers of 59 Jordanian commercial banks, and grouped the data into: branch location, gender, and years of experience. They found from the feedback of managers who work in the capital of Amman that customers who use m-banking are highly comfortable with the process and have easy access to WAP. In addition, male managers feel that using m-banking is highly influenced by personal contact and that the procedure to obtain m-banking access from a bank is an easy task. Furthermore, managers with less than 8 years experience feel that using m-banking provides monitoring and follow reports related to work more than those with 15 years experience or more, due to the fact that managers with less than 8 years experience are more open to newer technology than older managers [16]. This observation can also be noticed in learning new technology by new generations as compared to older generations which makes m-banking more attractive to the coming generations.

Mallat et al. indicated that the final decision of whether to adopt one or several mobile applications or none at all is the customer's decision. Financial institutions and operators can cooperate together to provide mobile payments, dividing the responsibilities according to their core competencies. The roles and tasks are not necessarily fixed, but are subject to change and evolution [17].

III. MOBILE BANKING SERVICES

Sun Microsystems Inc. mentioned some applicable guidelines when defining service requirements [18]. Such guidelines include, make it easy, make it small and fast, fail fast-scale fast, bank-grade security overall, and mobile commerce as the main goal.

By designing an m-banking application in a simple way, it can be understood and used with the limitations of mobile phones. On the other hand, generalised solutions can suffer from poor implementations and interfaces, which cause slow and cumbersome usage. Any m- banking application must be easy, fast, and intuitive; in order to be used on customer handsets. Users should be able to easily find an m-banking application among those available on the handset, and authenticate and execute the transaction within a small number of keystrokes.

Fail fast-scale fast means that banks must be able to quickly identify and try out new applications, scaling them if they work and removing them if they do not. Consumer confidence in the provided service is a major factor of its adoption. End-to-end bank-grade security is a requirement for every banking application. That means comprehensive security must be built and deployed into overall security architecture, not added on to each application [18].

Developers of m-banking applications must indicate clearly that mobile commerce is supported. That means a customer's ability to conduct mobile commerce transactions, in other words, the ability to perform mobile payments, account information and services, and more [18].

Banks that offer mobile access are mostly supporting many services like: account information, payments and transfers, investments, support, coverage, and content services [7].

The most common services available today in most large U.S banks are: account alerts, security alerts and reminders, account balance updates and history, customer service via mobile, branch or ATM location information, bill payments by secure agents and mobile client applications, funds transfers, transaction verification, and mortgage alerts [19].

M-banking extends existing online services such as account information, funds transfer, bill payment, and mini statements by making them accessible from any mobile device. Combining other mobile services such as customer alerts on account activities provides an improved customer experience and increased customer loyalty.

Some characteristics of the mobile use were identified by Pousttchi and Schurig [6] such as: mobile application uses a mobile device, connection is provided by a mobile network operator, using mobile data transmission is expensive, sensitive data is transmitted, and disruption of the usage is possible at any time.

With regards to these characteristics, four use cases were introduced by Pousttchi and Schurig [6], they developed 15 requirements to mobile banking applications which can be classified into four categories: technical, usability, design and security [6].

Technical requirements are as follows: using application must be possible with both kinds of mobile devices (a mobile phone and a PDA), the application should automatically adapt to the conditions of the mobile device, using the application must be possible for customers of any mobile network operator, and the amount of transmitted data should be kept to the minimum.

Usability requirements include: the possibility to work offline with the application, a simplified method of data input, resumption of usage at the same point after disruption which means that the application should allow the user to resume his/her usage at the same point where it was disrupted, without a complicated re-log-in procedure, and a "One-Click"-Request of important data for quick access to information.

In order to make m-banking a real alternative to e-banking, several design requirements must be satisfied such as: the possibility to personalise the application, the possibility to scale the application, the possibility to get announcements on important events, and a wide range of functionality, similar to those in e-banking,

Finally security requirements are classified into three parts: the transmission of the data has to be encrypted. Before usage, access to the data must be authorised, and authorisation has to be simple [6].

IV. SECURITY ASPECTS IN MOBILE BANKING

System security is a major factor that is considered to be a technical issue. However, a security system lays the user authentication. When users are involved, security is more than technical: it needs to be practical and usable [20]. Security is achieved only by means of a combination between the user and the technology [21]. Users are considered as the weakest link in the security chain, and users are often blamed for the failure of system security [22].

Security design has two aspects; technological and usability. Security systems in most cases are not designed to be convenient to the user's needs or to user's mental limitation. Although the goal of a security system is to have mechanisms to protect the system, it is also important that the mechanisms are usable by legitimate users who are authorised to use the system [8].

Martino and Perramon [23] proposed an authentication resistant method focused specifically on the e-banking scenario. The protection was based on the mutual authentication process, of which details have been studied thoroughly. In addition, security is provided against a compromised client environment, like virus or spyware infections on the client side, as such malware could be used to steal banking customers' account access information.

Narendiran et al. [24] proposed a security architecture for mobile banking and a prototype solution for securing sensitive data over wireless networks through a Mobile Information Device Profile (MIDP)-enabled device. Narendiran et al. also proposed an end-to-end security framework using Public Key Infrastructure (PKI) for mobile banking.

Chong proposed the design of two mobile authentication techniques: combinational graphical passwords and gesture passwords. These techniques were implemented as prototypes. The prototypes along with a Personal Identification Number (PIN) authenticator were evaluated by users, and the results revealed that users were more proficient and preferred to use PINs for mobile banking authentication than the other two systems [8].

Pousttchi and Schurig classified the security requirements into three categories, first: the transmission of the data has to be encrypted. Second: access to the data must be authorised before usage. Third: authorisation has to be simple [6].

Authentication refers to "the process of confirming or denying an individual's claimed identity" [25]. Password authentication is the most commonly used verification method and most users have adapted to use passwords for authentication.

M-Banking services are offered through different platforms, but the underlying services remain the same. PIN authentication is used by all implementations as a login method, regardless of the platform. Before conducting a transaction, a client is required to login with a PIN. Only a valid PIN code will grant the client access to the service [8].

V. SECURITY ASPECTS IN THE PROPOSED MOBILE BANKING SYSTEM

Security aspects were carefully considered in the proposed m-banking system to satisfy the security requirements as described in section III.

A. Authentication

The proposed system uses three components to ensure appropriate level of authentication, these are: username and password technique, National ID technique where the client must input one or more of his/her national ID digits chosen randomly, and an account ID technique in which the client has to input one of his/her accounts for each service s/he attempting to execute, also blocking to his/her profile is applied if s/he had wrong trial more than three times.

The client has to enter their username and password in order to access the system then his/her information will be encrypted and sent to the server side to check if it is correct or not. If it is not correct, the system displays an alert "invalid user name or password" and the system gives the client another chance to enter the correct information. The client has three trials then if the third trial was failed an alert is displayed to instruct the customer to return to the customer's branch. If the customer attempts to access the

system after this alert before visiting his/her branch, the system becomes inaccessible.

After successful username and password authentication, the system asks the client to enter his/her national ID, the client does not need to enter the whole national ID, but s/he will be instructed to enter one, two, or three digits from his/her national ID chosen randomly by the system; such as: First, third and last digit, first three digits, or last three digits.

If the client enters an incorrect combination of digits, the system will inform him/her that it is an invalid combination and the question will be asked again, possibly with other combination of digits. If the answer is correct, the next step will be to select the service and the system shows a welcome message with the client's name and a list of services. Figure 1 shows a flowchart for these steps.

B. Confidentiality

The proposed system encrypts the transmitted data using a substitution cipher which is a method of encryption in which single (simple substitution), double or triple of letters of plaintext are substituted by other letters, numbers or symbols in the cipher text. Substitution over a single letter (simple substitution) is adopted in the proposed system. Simple substitution can be demonstrated by writing out the alphabet in some order to represent the substitution.

The cipher alphabet may be shifted or reversed like with the Caesar cipher, a type of substitution cipher, which replaces each plaintext letter with one fixed number of places down the alphabet (a type of substitution cipher the alphabet is rotated 13 steps like ROT13 algorithm). The rotation steps could be set to a specific number. In the proposed system we adopted the shift of 7 steps so that A in the plaintext becomes H. Caesar cipher of plain text with a rotation of 7 steps as adopted in the proposed system is shown as follows:

Plaintext alphabet:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher text alphabet:

HIJKLMNOPQRSTUVWXYZABCDEFG

According to this substitution MOUSA as plaintext is replaced by TVBZH.

C. Authorisation:

After the customer obtains authentication to the system, an appropriate authorisation level is assigned where the user only gains access to his/her profile and his/her account details. This is achieved by entering an account number. The system asks the user to input the account number before the use of every service because if the customer forgets to turn off the application on his/her phone, a physical intruder may be able to use the available services of the customer account. Therefore, requesting an account number before any action protects the account from illegal utilisation. Additionally, a user may have several accounts, and s/he needs to decide on which account the current transaction should be performed.

VI. MOBILE BANKING COMPONENTS AND SERVICES

Several components interact with each other through well-defined interfaces. One of the main components is the erver that is located on the bank side. That server

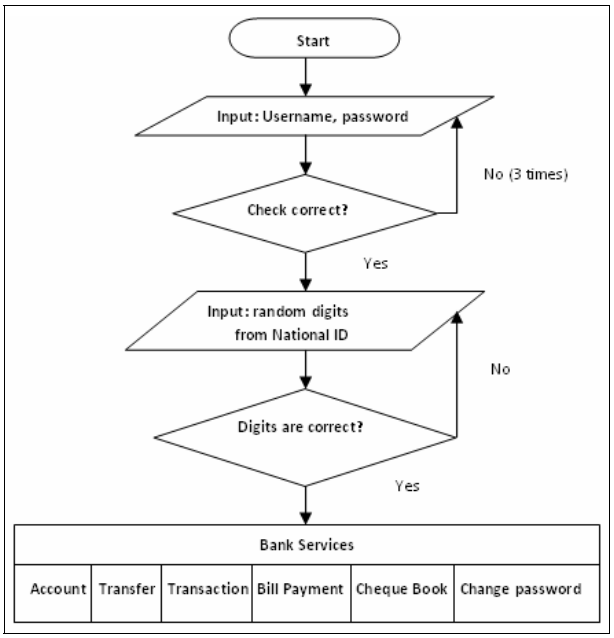


Figure 1. Checking Authentication.

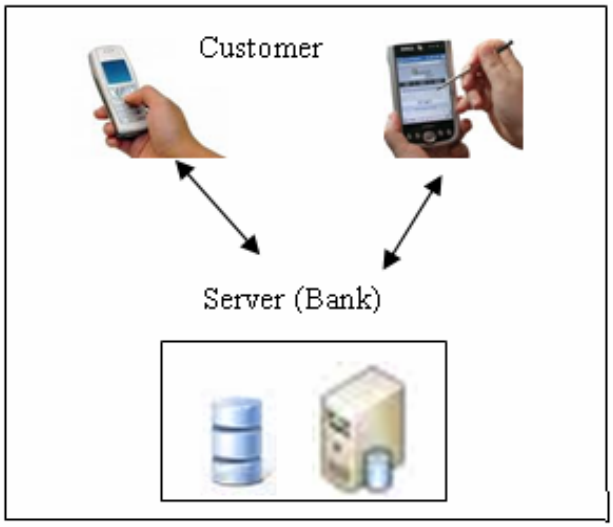


Figure 2. Mobile Banking System Architecture.

contains the bank database and offers mediation between the database component from one side and to the client component on the other side. The system architecture is depicted in Figure 2.

Server component (Bank)

Server side processes any received information and sends the results. Also, database is installed on the server side.

A. Client (Customer)

In the Client side there is no processing. The client (customer) sends requests and receives results. Java 2 Micro Edition (J2ME™) is used to program the application on the client side.

B. Database

In order to implement the proposed system, information about customer, account and submitting are required. We

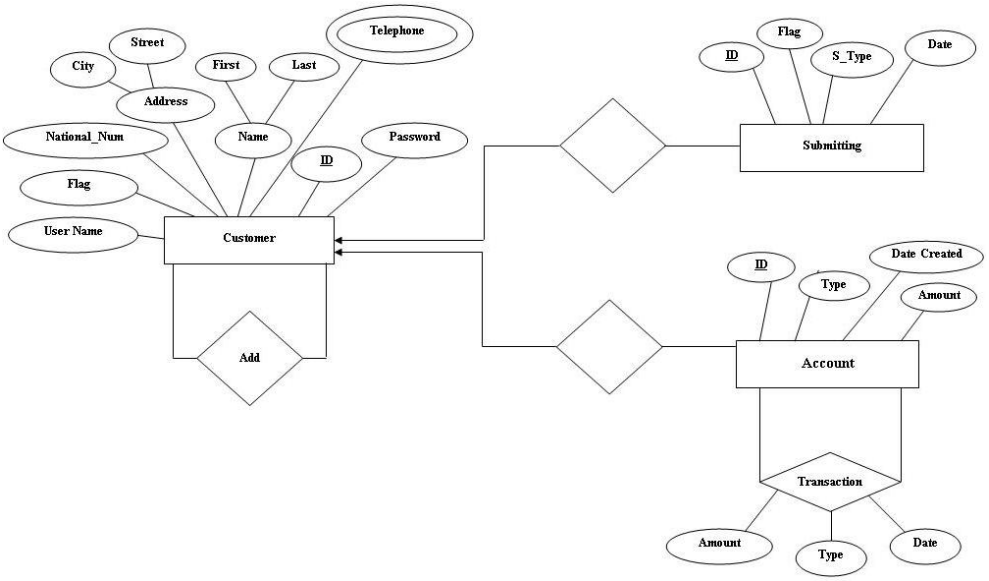


Figure 3. ER diagram for tables used in the proposed m-banking system.

organised such required information into three tables represented as ER diagram with relationships between them as shown in Figure 3. Table 1 describes the customer table, Table 2 describes the account table, and Table 3 describes the submitting table, along with attributes that link them together. In submitting table the system stores information to allow the user access to the system or to review the bank through the flag with the date of operation and submitting type. It is stored every time the user attempts to access the system.

C. Services

The system offers several services to the customers. These services are shown in Figure 4. Such services include, view of accounts, money transfers, transaction views, bill payments, ordering of cheque books, and changing passwords.

View Account: In this service the customer can see general information about the account (type, date creation, amount).

Transfer: Using this service, the customer can transfer money from one of the customer's accounts to another.

Transaction: This service enables the customer to view their latest account transaction(s) in detail such as type of transaction, and date.

Bill payment: Using this service the client can pay bill invoices to utility companies such as electricity, water and gas.

Cheque Book: Allows clients to send requests to order a cheque book from the bank.

Change password: Allows the client to update or change his/her password.

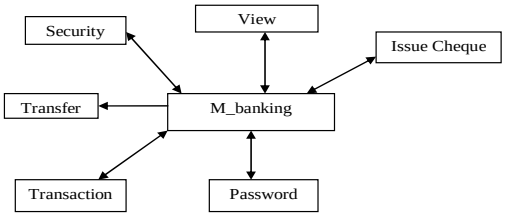


Figure 4. The proposed system block diagram.

TABLE I.
CUSTOMER TABLE

Attribute	Description
ID	Identification Number (Primary key)
User Name	Customer username that s/he enters as first step in using the system
Password	Password that the customer use in order to use the system
Name	Customer's name (first name and last name)
National No	Customer national ID number
Address	Customer address (City and Street no)
Flag	To indicate the role of the customer: (0: manager, 1: employee, 2: user)
Telephone	Customer's telephone number

TABLE II.
ACCOUNT TABLE

Attribute	Description
ID	Account Identification Number (Primary Key)
Type	Type of the Account (checking account, or saving account)
Amount	Represents balance amount
Date Created	The date when the customer account was created
Customer ID	To indicate which customer owns this account (Foreign Key)

TABLE III.
SUBMITTING TABLE

Attribute	Description
ID	Submitting Identification Number (Primary Key)
S_Type	Submitting Type
Flag	To indicate whether the user is allowed to access the system or s/he has to review the bank
Date	The date when the submitting occurs
Customer ID	To indicate which customer performed this submitting (Foreign Key)

D. Use Cases

Figure 5 shows the use case diagram and the actors of the proposed system.

In the following, we introduce eight use cases that have been developed in the proposed m-banking system. The use cases are not exhaustive, but are representative. In each use case the desired information and/or the conditions of the usage are displayed. For each use case we identify actions that the user has to do in this particular situation.

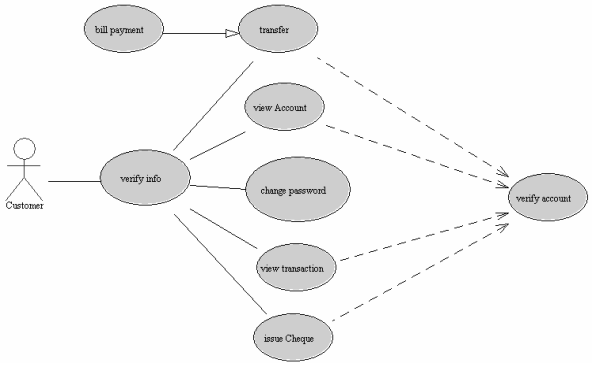


Figure 5. The use case diagram and the actors in the proposed m-banking system.

1) Use case 1: Verify Information:

The customer enters his/her user name and password, and the system verifies this information. The system then requests him/her to enter 1, 2, or 3 digits from his/her national ID number for more security. If the entered digits are correct then the customer can use the provided services and select any one of them. This use case is shown in Figure 6.

2) Use case 2: Verify Account

In many services in order to do some operations the customer must enter his/her account number. This is important for security reasons and as customers may have more than one account, this step allows the customer to decide on which account the current transaction is to be performed. The system verifies the account number, and checks if that account belongs to the currently logged in customer. If it is correct, the system continues to provide the service to the customer as shown in Figure 7.

3) Use case 3: View Account

The customer enters his/her user name and password, then enters digits from his/her national ID. If they are correct, the system requests him/her to enter an account number, and the server will check if it is correct or not as described in the previous use case. If it is correct, the server will send account information such as account type, date of creation, and current balance. Otherwise, an alert will be sent by the server: wrong account and it will allow the customer to try to log in again up to three times. After three failed attempts, the account will be locked and the server will ask the customer to go back to his/her branch to unlock the account. This use case is shown in Figure 8.

4) Use case 4: Fund Transfer

The customer enters the system according to use case 1. If successful, the customer can select the transfer service and then the customer has to enter one of his/her accounts from which s/he needs to transfer money. Also, s/he enters the account that will receive the money s/he needs to transfer, with the amount to be transferred. The system checks the two accounts and if both of them are correct and there is sufficient fund in the first account, the system will complete the transfer operation. Otherwise, the system returns back to the transfer form.

If one of the accounts the user entered was not for him/her, the system shows an alert "Error Account" and it allows the customer to correct the error up to three trials. After three failed attempts, the system displays a message asking the user to return to the branch. Then the system returns to the main form. The above sequence is depicted in Figure 9.

5) Use case 5: Transaction

The customer enters the system according to use case 1. If successful, the customer can select the transaction service. Then, the customer has to enter his/her account, transaction type and the duration, which is designed to allow the customer to choose from three options: last five transactions, last three transactions, or last transaction.

After entering the desired choice, the system checks if the customer's account is correct or not. If it is correct, transaction(s) details will be displayed such as: transaction type, transaction amount, and transaction date. If the account number is incorrect, the system shows a message to inform the customer that s/he entered an invalid account and the customer has to try again, but if s/he failed to enter a correct account number for three times, the system displays a message asking the customer to return to his/her branch. The system then displays the main form as shown in Figure 10.

6) Use case 6: Bill Payment

The user is in a mobile situation and intends to make a payment by bank transfer from his/her account to a utility company account. The customer enters the system according to use case 1. If successful, the customer can select the bill payment service. Then s/he must enter his/her account, select the company name and enter the amount and type of the bill. The system continues to process this operation. If the entered account was wrong, the system displays a message to the customer "Error Account" and if the customer enters wrong account for three times, the system displays a message telling the customer to return to his/her branch then return to the main form as shown in Figure 11.

7) Use case 7: Issue Cheque Book

The customer enters the system according to use case 1. If successful, the customer can select the cheque book issuing service. The system then asks the customer to enter three pieces of information: Account number, number of required cheque books, and number of pages per book. The system will check if the account number is correct or not. If it is correct, the request is sent to the bank server to process it. But, if the account is wrong, the system displays an alert "Error Account" to the customer and if the customer has made three wrong trials, the system will return to him/her a message to return to his/her branch and view the main form of the application as shown in Figure 12.

8) Use case 8: Change password

The customer enters the system according to use case 1. If successful, the customer can select change password service. Then the customer enters his/her old password,

new password, and confirmed new password. The system will check if the old password is correct and if the new and confirmed passwords are identical and differ from the old one or not. If the entered information is correct, then the system displays a message to tell the customer that the operation is successfully completed. Then the system sends the customer back to the main form to use the application using the new password as shown in Figure 13.

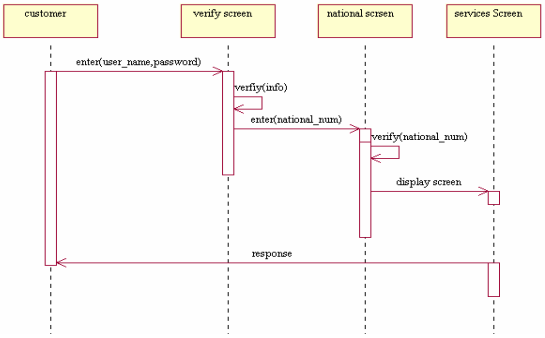


Figure 6. The sequence for verifying customer information

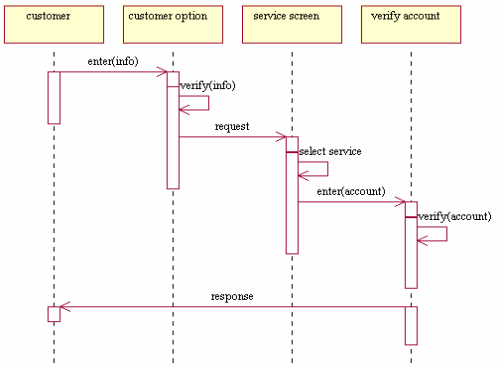


Figure 7. The sequence for verifying a customer account.

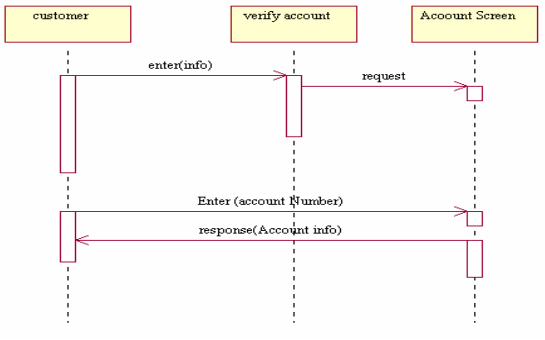


Figure 8. The sequence for viewing an account.

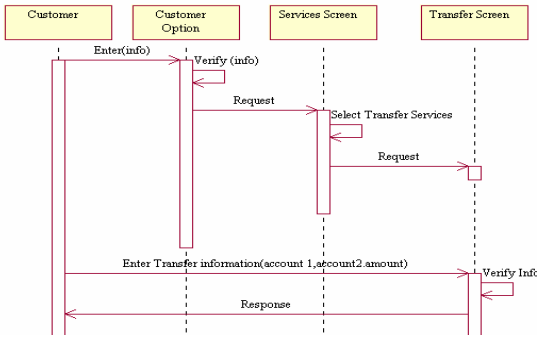


Figure 9. The sequence for fund transfer.

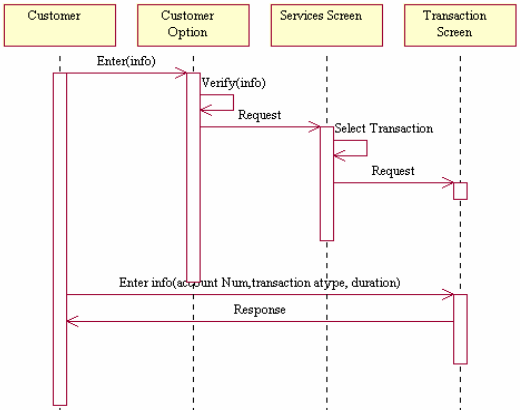


Figure 10. The sequence for transaction.

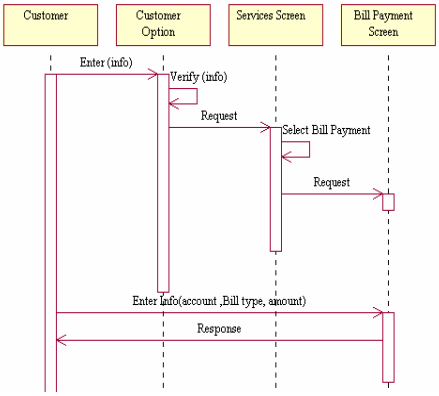


Figure 11. The sequence for bill payment.

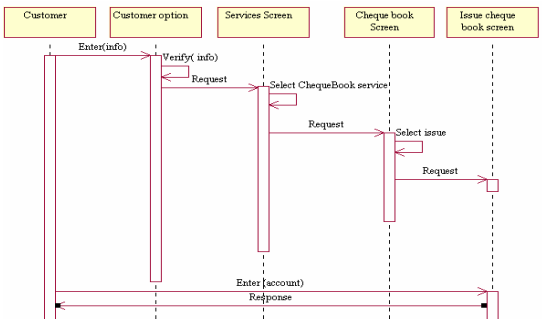


Figure 12. The sequence for issuing a cheque book.

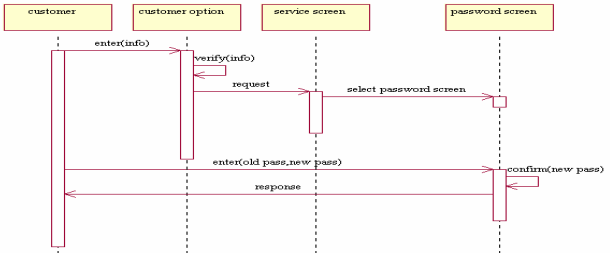


Figure 13. The sequence for changing a password.

VII. IMPLEMENTATION DETAILS

JAVA is used to program the server side and derby database is installed and used in this application as it offers a lightweight database.

Sun Microsystems developed Java 2 Platform Micro Edition (J2ME™) technology aimed at a specific area of computing industry which is for the combined needs of: consumer and embedded device manufacturers who build a diversity of information devices, service providers who wish to deliver content to their customers over those devices, and content creators who want to make compelling content for small, resource-constrained devices.

Although J2ME offers a subset of features offered in Java 2 Platform Standard Edition (J2SE™), but it maintains the basic features that Java technology offers like:

- Built-in consistency across different products such as its capability of running anywhere, anytime, and on any device.
- The power of a high-level object-oriented programming language with a large number of development libraries (packages)
- Portability of code.
- Safe network delivery.
- Upward scalability with J2SE and Java 2 Platform Enterprise Edition (J2EE).

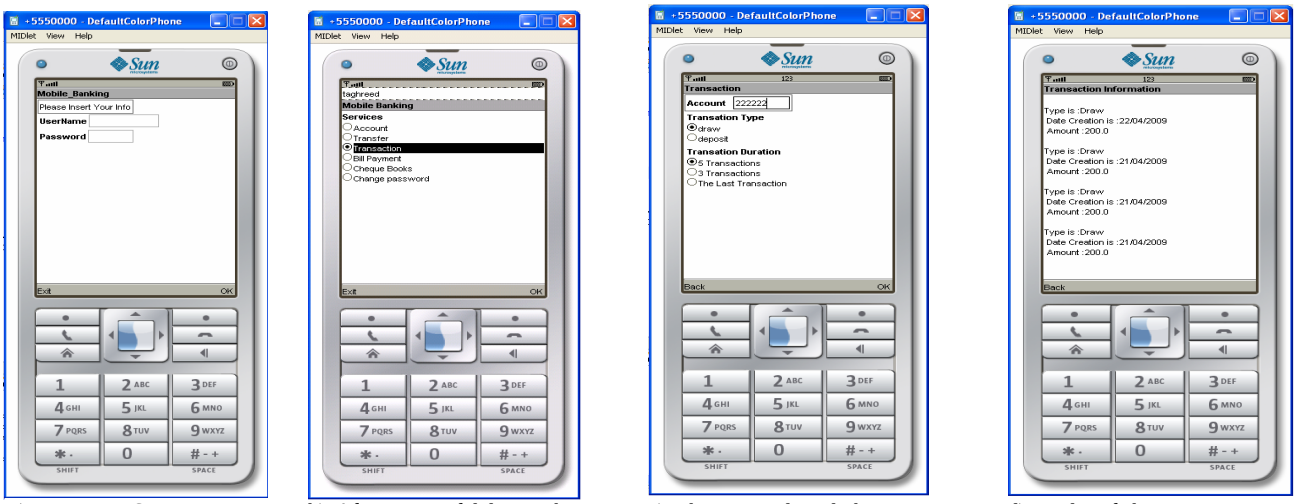
The J2ME architecture was made modular and scalable to support this kind of flexible deployment, also it supports minimal configurations of the Java virtual machine and Java Application Program Interfaces (APIs) that provide and capture just the essential capabilities of each kind of device.

Because of the large range of different type of devices in the J2ME market place, Sun has split the J2ME in configurations; Connected Limited Device Configuration (CLDC), and Connected Device Configuration (CDC) [26].

J2ME profile addresses the specific demands of a "vertical" market segment such as banking or payment applications. Because of this, profiles may include libraries that are more device-specific than the libraries provided in a configuration.

For developers, a profile is just a collection of Java APIs and class libraries residing on top of a configuration and providing domain specific capabilities for devices in a specific market segment.

Sample screenshots from our implementations are shown in Figures 14. The captions under the figures make them self explanatory.



a) First Login Step

b) After successful login, the user selects a specific service.

c) The user selected the transaction service then asked to enter the account number.

d) results of the transaction service for the last 5 transactions

Figure 14. Screenshots from the proposed m-banking implementation.

VIII. CONCLUSIONS AND FUTURE WORK

In the preceding sections we analysed the relevant services and security aspects in a mobile banking (m-banking) system. We proposed a system for m-banking and identified relevant m-banking use cases of the proposed application. Based on these we derived a set of security aspects, which we employed later in the proposed m-banking system.

One major goal of banks is to expand the big success of electronic banking (e-banking) to m-banking in order to improve users' reachability. However, it is important to keep in mind that any usage of m-banking is done with the application of the rules of mobile commerce.

REFERENCES

[1] Weiser, M., The Computer for the 21st Century, *Scientific American Special Issue on Communications, Computers, and Networks*, no. 265, pp. 94–104, September 1991.

[2] Alawairdhi, M., Yang, H. and M. AL-Akhras, BlueCRM: A New Trend of Customer Relationship Management Systems, *12th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2008. FTDCS '08,* pp. 226-232, 21-23 October 2008.

[3] Prahalad, C.K., Ramaswamy, P.B. Katzenbach, J.R., Lederer, C. and S. Hill, Harvard Business Review on Customer Relationship Management. Harvard Business School Press, January 15, 2002.

[4] Shoniregun, C.A., Omoegun, A. Brown-West, D. and O. Logvynovskiy, Can eCRM and trust improve eC customer base?, Proceedings of *IEEE International Conference on e-Commerce Technology, 2004*. CEC 2004, pp. 303-310, 6-9 July 2004.

[5] Sinisalo, J., Salo, J., Karjaluoto, H. and M. Leppäniemi, Managing customer relationships through mobile medium – underlying issues and opportunities, Proceedings of the *39th Hawaii International Conference on System Sciences*, pp.1-10, January 2006.

[6] Pousttchi, K. and M. Schurig, Assessment of Today's Mobile Banking Applications from the View of Customer Requirements, Proceedings of the *37th Hawaii International Conference on System Sciences*, pp. 1-10, 5-8 January 2004. doi:10.1109/HICSS.2004.1265440

[7] Infogile Technologies, Mobile Banking - the future [Online White Paper]. Available: http://www.infogile.com/pdf/Mobile_Banking.pdf, published: August 2007, last access 7/10/2010.

[8] Chong, M.K. Usable Authentication for Mobile Banking, M.Sc. thesis, University of Cape Town, South Africa, 2007.

[9] Laukkanen, T., Comparing Consumer Value Creation in Internet and Mobile Banking, Proceedings of the *International Conference on Mobile Business*, pp. 655-658, 11-13 July 2005. doi:10.1109/ICMB.2005.28

[10] GSM Association. Subscriber connections - Q2 2008. [Online]. Available: http://thazza.mobi/upl/tbl3/gsma_stats_q2_08.pdf, last access 30 October 2010.

[11] GSM Association. 20 facts for 20 years of mobile communications. [Online]. Available: http://www.scribd.com/doc/12975203/20-facts-for-20-years-of-mobile-communications, last access 30 October 2010.

[12] Green Technology. Research and Markets: The Number of Active Users of Mobile Banking and Related Financial Services. [Online]. Available: http://green.tmcnet.com/news/2010/04/23/4747452.htm, last access 30 October 2010.

[13] GSM Association. Global money transfer pilot uses mobile to benefit migrant workers and the unbanked. [Online]. Available: http://www.gsmworld.com/newsroom/press-releases/1984.htm, last access 20 October 2010.

[14] Medhi, I., Ratan, A. and K. Toyama, Mobile-Banking Adoption and Usage by Low-Literate, Low-Income Users in the Developing World, Proceedings of the *3rd International Conference on Internationalization, Design and Global Development*: Held as *Part of HCI International 2009*, pp. 485-494, San Diego, CA.

[15] Barati, S., and S. Mohammad, An Efficient Model to Improve Customer Acceptance of Mobile Banking, Proceedings of *the World Congress on Engineering and Computer Science 2009*, Vol. II WCECS 2009, October 20-22, 2009, San Francisco, USA

[16] Shammot, M. M. and M. S. Al-Shaikh, Adoption of Mobile Banking Services in Jordan, *Scientific Journal of King Faisal University (Humanities and Management Sciences)*, vol. 9, no. 2, 1429H, 2008.

[17] Mallat, N., Rossi, M., and V. K. Tuunainen. Mobile banking services, *Communications of the ACM, vol. 47, no.* 5, pp. 42-46, May 2004. doi:10.1145/986213.986236

[18] Sun Microsystems Inc. The road to mobile banking. [Online White Paper]. Available: http://sun.systemnews.com/127/2/Financial/20550, published June 2008, last access 30 October 2010.

[19] Mobile marketing association. Mobile banking overview. [Online]. Available: http://www.mmaglobal.com/mbankingoverview.pdf, last access 30 October 2010.

[20] Tognazzini, B., Design for usability. Cranor, L. F. and Garfinkel, S. (ed.) Security and Usability: Designing Secure Systems that People Can Use, pp. 31-46. Sebastopol, CA: O'Reilly, 2005.

[21] Renaud, K. and A. De Angeli, My password is here! An investigation into visuo-spatial authentication mechanisms. Interacting with Computers, vol. 16, no. 6, pp. 1017-1041, December 2004. doi:10.1016/j.intcom.2004.06.012

[22] Schneier, B. Secret and Lies. John Wiley & Sons, 2000.

[23] San Martino, A. and X. Perramon, Defending E-Banking Services: Antiphishing Approach, *Second International Conference on Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08*, pp. 93-98, 25-31 August 2008

[24] Narendiran, C. and Rabara, S.A. and N. Rajendran, Performance evaluation on end-to-end security architecture for mobile banking system, *1st IFIP Wireless Days, 2008. WD '08*, pp.1-5, 24-27 November 2008.

[25] Jansen, W. A., Authenticating users on handheld devices, In Proceedings of the *Canadian Information Technology Security Symposium*, May 2003, Wayne Jansen.

[26] Steiner, U. J2ME: Introduction, Configurations and Profiles. University of Zürich, [Online]. Available: http://www.ifi.uzh.ch/~riedl/lectures/Java2001-j2me.pdf, last access 30 October 2010.

AUTHORS

Mousa T. AL-Akhras is a member of IEEE and he was elected as a secretary for general activities of the IEEE executive committee, Jordan Section, region 8 for the years 2010-2011. He was also elected as a vice-chair for Computational Intelligence/ Computer Joint Societies Chapter, Jordan section for the years 2010-2011. He is also a member of IEEE CIS & RAS Societies. Mousa received his B.Sc. and M.Sc. degrees in Computer Science from the University of Jordan, Jordan, in 2000 and 2003, respectively. He received his Ph.D. degree from De Montfort University, UK, in 2007.

He is currently working as an assistant professor in the Computer Information Systems Department, King Abdullah II School for Information Technology (KASIT) at the University of Jordan, Amman, 11942 Jordan (http://www.ju.edu.jo/). Dr.AL-Akhras main research interests include problems in the area of Artificial Intelligence and particularly Artificial Neural Networks (ANN). His research interests include Voice over IP, Multimedia Communication, Robotics, Genetic Algorithm, Fuzzy Logic, and statistics. He is also interested in the area of electronic learning (e-learning) and mobile learning (m-learning). Mousa is in the organising and technical committees for a number of local and international conferences. Also, he serves as a reviewer and a member of the editorial board in a number of local and International Journals. He is a member of the Jordan Society for Scientific Research (JSSR). He also serves as a judge in the national and Arabic robot contest (First Lego League), (e-mail: mousa.akhras@ju.edu.jo).

Rizik Al-Sayyed is currently with the University of Jordan, King Abdullah II School for Information Technology, Business Information Systems Department. Dr. Rizik holds the B.Sc. (The University of Jordan 1984), M.Sc. (Western Michigan University 1995), and Ph.D. (Leeds Metropolitan University 2007) all in Computer Science. His areas of interest include: Wireless Networks, Database Design and Programming, Network Simulation, Mobile Computing, Design and analysis of algorithms and Web Design and Programming (e-mail: r.alsayyed@ju.edu.jo).

Marwah Alian received her B.Sc. degree in Computer Science from Hashimite University in 1999. After graduation, she worked as programmer then as a teacher in many high schools in Jordan then she received the M.Sc. degree in Computer Science from The University of Jordan in 2007 with a thesis titled as: The Shortest Adaptive Learning Path in eLearning Systems. After graduation she became a member in the technical team of a project called Science Education Enhancement and Development (SEED) supported by Japanese International Cooperation Agency (JICA). Since 2008 she became a member of Computer Science Department in Science and Information Technology Faculty at Isra University. Ms.Marwah research interests include e-learning Systems, Adaptive Learning, Mobile Learning, and Mobile applications. She has several publications in the areas of e-learning, adap-

tive e-learning, and data mining (e-mail: marwa@ipu.edu.jo).

Doaa Qwasmi received her B.Sc. from the University of Jordan, Amman, 11942, Jordan in 2009 from the Computer Science department. Doaa has interest in the subject of computer networks. After graduation Doaa has joined Umniah mobile operator, she is working in the Department of wired and wireless networks (ADSL & UMAX, commercial name for WiMAX), her responsibilities also include teaching computer skills within the program of computer skills with Umniah for the community and students (e-mail: doaak2001@yahoo.com).

Submitted, November 20, 2010. Published as resubmitted by the authors December 12th, 2010.