# Experiences on Mobile-ATM Deployment in a Developing Country

Amila KARUNANAYAKE[1], Kausn De ZOYSA[1], Sead MUFTIC[2], Feng ZHANG[2]
[1]*University of Colombo School of Computing, Colombo, Sri Lanka.*
*a.karunanayake@gmail.com, kasun@ucsc.cmb.ac.lk*
[2]*Departments of Computer and System Sciences,*
*Royal Institute of Technology, Stockholm, Sweden.*
*sead@dsv.su.se, fengz@dsv.su.se*

**Abstract:** Mobile-Commerce is the latest concept of enabling the financial transactions on mobile phones and hand-held devices. With the rapid development of the society, the M-Commerce applications play a vital role. Mobile-ATM is one such application, enabling the banking services on mobile phones. Even though users have a poor computer literacy, they will be able to use the Mobile-ATM system easily. This kind of application is very useful, especially in rural areas, where accessing financial and banking services is a critical issue due to the distance barriers. Hence this paper discusses the social, economical and technical impact of the Mobile-ATM system, which is developed by the authors. Moreover the paper points out the essential value added services provided by our system with respect to financial transactions services such as security and confidentiality. Although the Mobile-ATM is technically feasible and practically deployed, it is important to have community acceptance. This paper discusses the community acceptance of this system and related issues.

## 1. Introduction

As a result of industrial revolution and globalization, commercial transactions have rapidly increased. However people realized that exchanging a large amount of money is a risky task. As a solution they started using banking facilities for doing money transactions. At present banks provide attractive facilities for more effective money transactions. However, many problems related to bank transactions are still remaining. In developing countries these problems have become worse.

During last two decades researchers have applied information and communication technology concepts to solve banking problems. They introduced E-Commerce and M-Commerce concepts as an alternative to traditional methods. Examples of such solutions are ATM services and credit card/debit card services.

Implementing and using IT-based solutions in developing countries is a big challenge due to poor communication and IT infrastructure. Remarkably, in most of the developing countries like Sri Lanka, mobile telecommunication sector archived a rapid expansion [1] in recent years. Therefore the mobile communication infrastructure can be used as a good deployment platform for the electronic based banking and financial systems.

Mobile banking (M-banking) is one of the newest approaches to the provision of financial services through wireless network, which has been made possible by the widespread adoption of mobile phones even in developing countries. It involves the use of a mobile phone or another mobile device to perform various financial transactions either directly with the recipient (micro-payments) or indirectly, via a client's bank account. The functional capabilities of mobile telephony have been rapid, and have extended usage well beyond the

classical applications (telephone calls and short messaging). There is mounting evidence of positive financial, economic and social impact of those technologies all over the world.

Additionally mobile based solutions can achieve more coverage. On the other hand one of the most important concerns with such transactions is their security. The mobile networks are based on use of poorly secured wireless protocols [2]. Therefore these reasons make mobile financial applications even more vulnerable to fraud and illegal use than similar transactions performed over open networks. Therefore, one of the main prerequisites for successful, large scale and broad deployment of mobile financial services applications is their security.

There are number of commercial systems available for enabling the banking services on mobile devices. Most of these systems are focused on introducing new smart technology in to the banking services. Mobile-ATM [5] is one such system, which is successfully deployed in Sri Lanka. Instead of introducing smart technology to banking services, Mobile-ATM system thinks in a different way. It utilizes some valuable features of mobile networks to address the barriers of accessing banking services in rural areas.

This paper is organized as follows: the next section will discuss the M-Commerce concept and briefly raise security and social requirements. Thereafter the paper describes the Mobile-ATM system and related deployment issues. The latter part of the paper reports from our evaluation methods and results concerning both technical aspects and social.

## 2. M-Commerce

Currently researches on mobile technology are introducing new services to fulfill the growing demand of mobility. One of the attractive services developed in recent years is providing mobile-based banking and financial services. This type of applications/services includes buying over mobile phone, purchasing and redemption of ticket and reward schemes, travel and weather information and writing contracts on the move. This type of mobile applications is categorized as M-Commerce [10] applications. There is a significant growing demand on deploying banking and financial services over mobile networks.

### *2.1 Strengths and Limitations*

The M-Commerce applications are very useful for mobile users in a variety of ways. Any user with a mobile phone can access M-Commerce applications in real time at any place. Also, mobile devices provide security to a certain extent compared to online transaction systems [2]. Furthermore the mobile systems can be expanded to provide local information services by localizing registered users within a specific area with the help of the mobile network operators or positioning techniques such as GIS/GPS. However, there are limitations of mobile devices, as most devices are equipped with limited memory/display and limited processing power. In addition the communication through the air links introduces additional security threats (e.g. eavesdropping).

In fact, M-Commerce applications have the potential to address a major service gap in developing countries that is critical to their social and economic development. However, the success of M-Commerce applications depends on the security of the underlying technologies and the community acceptance of the system.

### *2.2 Security requirements*

Most of the M-Commerce systems are based on the GSM network infrastructure and security features provided by the GSM network. However, using the security features provided by the GSM network is not sufficient for the M-Commerce applications [4].

In M-commerce applications, each party that participates for a particular transaction does not meet each other physically. However, in financial transactions trust should somehow be established between each party [9]. General cryptography concepts can be used to accomplish

the trust between each participant. There are five types of features that are needed for establishing trust:

- *Authentication:* Authentication is the process of proving user identification. One party which involves in transaction needs to make sure that counterparty is the one he interested to communicate with.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original message.
- *Confidentiality:* Ensuring that no one else can read the message except the intended receiver.
- *Non-repudiation:* A mechanism that ensures to prevent that the counter party later on rolls back the transaction.
- *Availability:* System Availability is whether (or how often) a system is available for use by its intended users. This is an integral component of security.

### *2.3 Social requirements*

The Mobile-ATM system targets the rural community [5] in developing countries. So, there are several constraints in developing community acceptable solutions. The poor computer literacy stands against the successfully deployment of such projects. Therefore the mobile user interface should guide users to perform transactions with very simple help statements.

Moreover the existing M-Banking systems use only electronic financial materials (like electronic coins) for the transaction [10]. In most of the developing countries, only very few facilities exist to perform transactions using electronic financial materials. Meanwhile the survey which was conducted shows that most of the people in rural areas do not like to use electronic coins. Therefore M-Banking systems for developing countries should be capable to use actual notes and coins as the transaction medium. Therefore our system should be able to deal with the actual coins and notes.

## 3. Mobile-ATM

Mobile-ATM is a simple M-Commerce application, which provides ATM services. The traditional ATM network [7] can be replaced by the Mobile-ATM system. The key components of the anticipated system are Bank, Customer and the Mobile-ATM agent. Roles of these components will be discussed later in this paper. Both Mobile-ATM agent and the customer should have mobile phones, suitably modified to perform the functions of the Mobile-ATM. The bank has Mobile-ATM server as the front-end, connected to the bank's back-end transaction management system.

### *3.1 System Architecture*

Transactions of the deployed Mobile-ATM system take place are explained below. In order to perform a transaction, a customer with a mobile phone should come to the Mobile-ATM agent, who has another mobile phone. Figure 1 illustrates the overall system design.

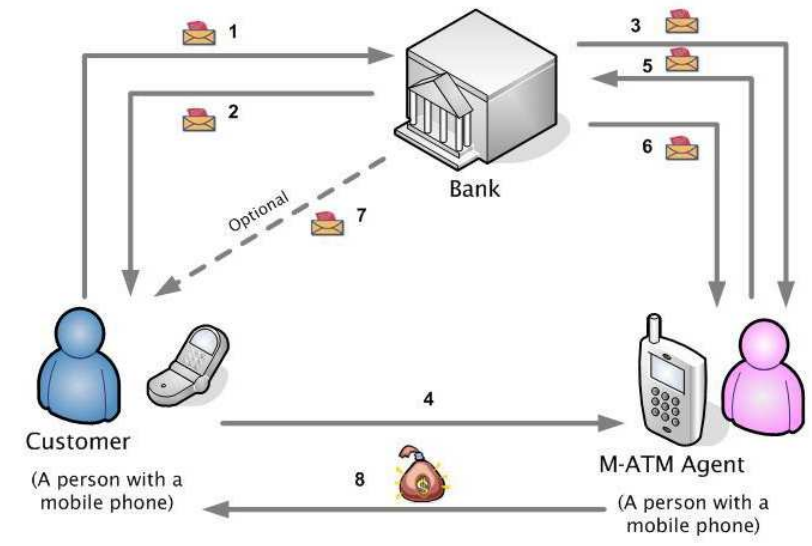



*Figure 1: High level architecture of Mobile-ATM*

1. A customer goes to a Mobile-ATM agent's place and sends a secure SMS to the bank (withdrawal request) with Mobile-ATM agent's (Mobile-ATM) phone number, requested amount.
2. The bank verifies customer's account and sends an authorized SMS message to the customer together with a confirmation number (a random number).
3. At the same time the bank sends a payment authorization SMS to the Mobile-ATM agent (Mobile-ATM) together with a transaction number (a random number which is different from the confirmation number).
4. The customer tells the confirmation number to the Mobile-ATM agent (Mobile-ATM).
5. The Mobile-ATM agent (Mobile-ATM) sends a confirmation SMS to the bank together with the transaction and the confirmation number.
6. The bank transfers the amount from the customer's account to the Mobile-ATM agent's (Mobile-ATM's) account and sends a transaction confirmation SMS to the Mobile-ATM agent.
7. The bank also sends a transaction confirmation SMS to the customer.
8. The Mobile-ATM agent hands in the money to the customer.

Two random numbers are used in any particular transaction to provide non reputability. Moreover it is a good evidence to confirm that the transaction has been fully completed.

### *3.2 System Roles*

The operation of the system can basically be divided into three parts based on the actors in the system:

- *Customer:* A customer can be a person who needs to perform an ATM transaction. He has a bank account and mobile phone. Special program should be installed in customer's mobile phone to operate Mobile-ATM functions.
- *Mobile-ATM Agent:* Like the customer, Mobile-ATM agent should have a bank account and a mobile phone. This mobile phone is also modified to perform functions of the Mobile-ATM in a secured manner. He is an authorized person to perform Mobile-ATM transactions by the bank. Mobile-ATM agent keeps money with his hand and interest to hand over to the customers when there is a request.
- *Bank Organization:* Bank should have Mobile-ATM servers to deal with transactions between customers and Mobile-ATM. The Mobile-ATM servers should be directly connected to the bank's databases. In addition to that, bank maintains the bank accounts of the customer and the Mobile-ATM agent.

### *3.3 System Deployment*

At the customer side there should be a special mobile application which is suitable to operate the Mobile-ATM functions. This application would require customer's PIN number for authenticate purposes. In addition it requires Mobile-ATM agent's mobile phone number and the amount of money to be withdrawn. Finally, application at customer's side sends secure SMS message which includes the Mobile-ATM mobile number, the amount of money to withdraw and customers account number to the bank.

At Mobile-ATM agent's side there should be a mobile application, which is capable of receiving secured SMS messages from the bank. As well as it should be capable of sending transaction number, confirmation number and customer's mobile phone number to bank securely. This application also requires agent's PIN number for authenticate purposes.

Mobile-ATM server is providing registration and authentication services for the Mobile ATM. Furthermore the Mobile-ATM servers are responsible for generating two random numbers (confirmation number and transaction number) for every transaction. There is an algorithmic relationship between the confirmation number and the transaction number. Random number generation program will not generate the same number for another transaction. After the 5th step, in section 3.1, Mobile-ATM servers should be able to identify the two numbers, which belong to the same transaction.

### *3.4 Security Issues*

Since the transaction happens mainly through SMS, security issues related to SMS should be considered by the Mobile-ATM application [3]. Normally in GSM networks, sender and receiver of an SMS is identified by its IMSI [6], which cannot be forged without breaking the GSM/UTM security mechanisms by an attacker [8]. Therefore these SMS messages can be used for authentication (at least towards the network). However, this kind of protection is only available in GSM network and there is no end-to-end security. Therefore either the network operator and its infrastructure must be trusted or an external authentication protocol must be deployed [4]. It is not convenient to trust the network operator and its infrastructure in the context of applications like Mobile-ATM. Therefore, Mobile-ATM provides end-to-end security mechanism instead of depending on the GSM network security.

### *3.5 Security Architecture – Customer side security*

Customer side security is provided based on the symmetric key cryptography. Here we make an assumption that the bank is a trusted entity.

Customer has to enter his PIN number in to the customer side application and the application itself gets the customer mobile phone number and application ID to generate a secure Hash Code. The generated hash code is used as the key for the AES encryption algorithm to encrypt the customer related information at the client side. This information includes the Mobile-ATM agent's phone number, and the amount to be withdrawn. Then, this

encrypted version of information is sent to the relevant Bank. According to the assumption mentioned above, the bank generates a Hash Code using Customer PIN number, Phone number and Application id and keeps it in bank's database, and uses the generated hash key to attempt decrypting the received encrypted message from the customer. If this is successful, it means that the hash key stored in bank database is equal to the hash key generated by the customer. Therefore bank can authenticate the customer. Also encrypted version of the customer message provides the integrity and the confidentiality of the customer information.

### *3.6 Security Architecture – Mobile-ATM agent security*

MOBILE-ATM agent is an authorized person by the bank. The same security architecture described in section 3.5 has been applied here.

At the step 5 of figure 1 the Mobile-ATM agent encrypts the confirmation number (which has been obtained from the customer) and the transaction number. Calculated hash code from Mobile-ATM agent's PIN and application ID is used to generate the encryption key. Then the bank can authenticate the Mobile-ATM agent. This message also provides the integrity and confidentiality of data.

At steps 6 and 7 of figure 1, the bank sends the confirmation note that indicates whether the transaction was completed or rejected. These two messages are encrypted by bank. If these messages are successfully decrypted on the receiving sides, both the customer and the Mobile-ATM agent can verify that the confirmation notes come from the bank. The transaction completes at this stage.

## 4. Evaluation

So far, we have discussed about the technical designs and the special issues of the Mobile-ATM system. This section introduces a detailed technical evaluation and a small user study evaluation. As mention in section 2.3, Mobile-ATM mainly targets for the rural area community. Hence, we believe real world evaluation has more advantages instead of evaluating the system in a lab environment. Therefore, for the evaluation purposes, we have been deployed the Mobile-ATM system in a rural bank, which has a rural customer community.

### *4.1 Technical Evaluation*

The technical evaluation focuses on evaluating the system performances and the scalability. The performance of the deployed Mobile-ATM system has been measured by the time taking to complete a particular transaction. The completion time of a particular transaction consists of the time needed to feed the data to the application, the throughput SMS delivery time and time taken by core banking system to complete the transition. But the time taken to feed the data to the application depends on the computer literacy of the user. Therefore we remove that factor to extract correct measurements about the system performances. For a particular transaction, mainly there are two situations where users should feed data to the application, the withdrawal request and the agent's request. Hence, we have to divide time measurements into two parts.

1. Time period starting from customer sending the withdrawal request and ending with receiving both confirmation SMS and transaction SMS. (T1)
2. Time period starting from agent sending confirmation and transaction numbers and ending with receiving the transaction completion SMS. (T2)

According to Table 1, standard deviation values of T1, T2 and Total are relatively small in comparison to the mean values. That means the spreading of T1, T2 and Total time is in a short time interval. For example, the bulk of the total completion times for transactions are

found between 84s and 104s. Hence we can conclude that the system is stable for most of the transactions.

*Table 1: In-network performances*

| | T1(s) | T2(s) | Total(s) |
|---|---|---|---|
| Mean | 49.677s | 44.34s | 94.021s |
| Standard deviation | 8.216s | 7.311s | 10.534s |

Moreover, we take the first 20 transaction measurements at a location of very high GSM signal strength (at around 250 meters distance from the base station). The latter 20 observations are measured at a location of average GSM signal strength (around 4 Km away from the base station). When these observations interpret in figure 2, we cannot see considerable variation of the total time among first 20 measurements and latter 20 measurements. Thus we conclude that the GSM signal strength does not affect the system performances to a great extent. Hence, the system can be used in rural areas, which has low signal strength.

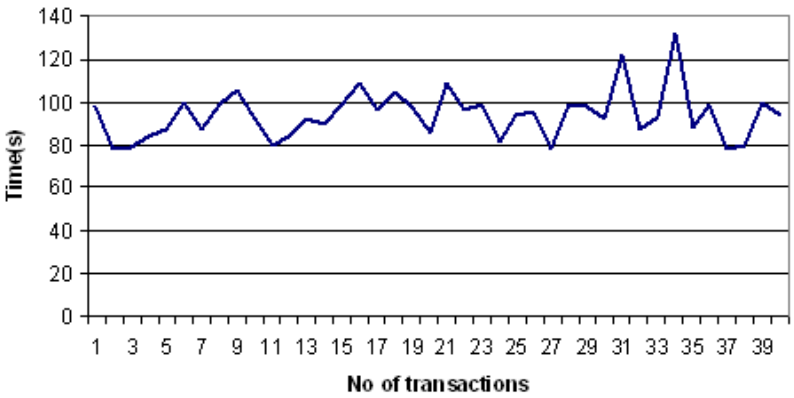



*Figure 2: Transaction performances time*

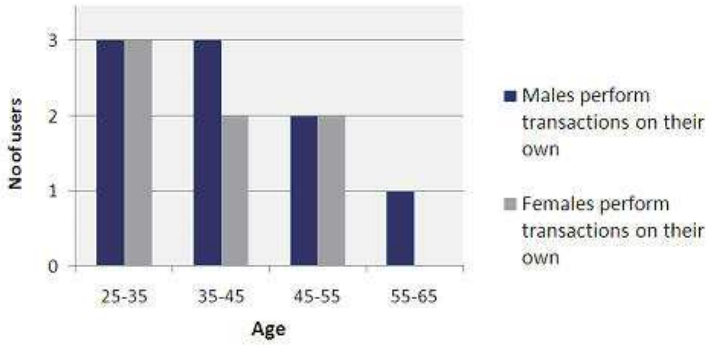
### *4.2 Sociological analysis: A quick pilot study*

As well as introducing a new technology to a social problem, analyzing the social impact of the deployed system is vital. Through a thorough analysis of the social impact, researchers can apply their theoretical proposals in real world problems. When we planned the Mobile-ATM system, we considered that user should have capability to operate a mobile phone. Hence we perform an analysis to test the social factors like age, level of education and sex affect on the usage of system.

Figure 3 illustrates the results of the analysis. The sample take such a way that 6 people are between 25 years to 35, 6 people between 35 to 45 years, and so on. Also from a particular age group there are equal number of males and females. Figure 3 shows that old people cannot do the Mobile-ATM transactions on their own (Mobile-ATM agent has done the customers duty according to the customer's instructions.). Possibly, females are weaker in doing transactions on their own even if it is impossible to draw any final conclusions from

our small sample. So age and possibly sex are two major social factors which stand against the popularity of Mobile-ATM system in rural community.

The above analysis is a quick pilot study that indicates some sociological factors such as differences between age groups and sex which should be investigated more thoroughly but which we have used as a temporary guide for the design of your system.




*Figur3: Users perform transactions on their own*

### *4.3 Privacy Problem*

Another important consideration that we take from users by oral discussions is the privacy of the transactions. Most of the users think privacy is a big issue when they deal with the Mobile-ATM agents. In a real world scenario, the agent is a villager. Most of the customers said, they do not like the agent ask the purpose of money withdrawal. Most probably these situations not occur if customers do their transactions with bank or ATM. Hence the privacy of the transaction is another issue when we deploy the system for practical usage.

## 5. Conclusions

One of the distinguished features of the Mobile-ATM system which makes it different from any other similar system is its security. The Mobile-ATM system provides all the basic security features describe in section 2.2.

Without having any additional cost on the infrastructure, the existing mobile networks can be used to deploy this system. Since most of the people have the knowledge to use mobile phones, customers can familiarize with the system easily.

We have been thinking “out of box” on how to use the mobile technology in a new fashion, instead of using the mobile technology to attract the customers for banking services. According to section 1, the effort taken to bring the Mobile-ATM system into success is acceptance by the rural community in developing countries. Although our evaluation is mainly positive, still there are some barriers standing against the popularity of our Mobile-ATM system.

However, we are confident that this application addresses a major service gap in developing countries that is critical to their social and economic development.

## Acknowledgments

The work present in this paper has been funded by The Swedish Program for ICT in Developing Regions (SPIDER) and University of Colombo School of Computing (UCSC),

Sri Lanka. The content of the paper has been edited by the M4D 2008 conference General Chair, Prof. John Sören Pettersson at Karlstad University.

## References


[1] Annual report. *Central Bank of Democratic Socialist Republic of Sri Lanka*, pages 71–74, 2007.

[2] H. Amcar and R. Kansoy. A mobile telephone based, secure micro-payment technology using the existing ICT infrastructure. *International Conference in Communication and Networking, CHINACOM2007*, 2007.

[3] P. Garner, I. Mullins, R. Edwards, and P. Coulton. Mobile terminated SMS billing – exploits and security analysis. *Third International Conference on Information technology: New Generations (ITNG'06)*, 2006.

[4] L. He and N. Zhang. An asymmetric authentication protocol for m-commerce applications. *Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC03)*, 2003.

[5] A. Karunanayake, K. Zoysa, and S. Mufftic. Mobile-ATM for developing countries. *Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (Mobiarch'08), SIGCOMM, Seattle*, 2008.

[6] K.P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena. Mutual authentication and key agreement for GSM. *International Conference on Mobile Business (ICMB'06)*, 26–27 June, 2006. Page 25.

[7] Z. Li, Q. Sun, Y. Lian, and D. Giusto. An association-based graphical password design resistant to shoulder-surfing attack. *IEEE International Conference on Multimedia and Expo, Chinna*, pages 245–248, 2005.

[8] H. Knospe and S. Schwiderski-Grosche. *Secure mobile commerce*. In C. J. Mitchell, editor, *Security for Mobility*, IEE Press (now IET), pages 325–346, 2004.

[9] D. V. Thanh. Security issues in mobile e-commerce. *First International Conference on Electronic Commerce and Web Technologies*, pages 467–476, 2000.

[10] N. Wishart. *Micro-payment systems and their application to mobile networks*. Washington, DC: *info*Dev / World Bank. Available at: http://www.infodev.org/en/Publication.43.html 2006.