Mobile ATM for Developing Countries

Amila Karunanayake
Department of Computer Science, School of Computing,University of Colombo. Sri Lanka.
a.karunanayake@gmail.com

Kasun De Zoysa
Department of Computer Science, School of Computing,University of Colombo. Sri Lanka.
kasun@cmb.ac.lk

Sead Muftic
Department of Computer and System Science,
Royal Institute of Technology.
Stockholm,Sweden.
sead@dsv.su.se

ABSTRACT

Society benefits from M-Commerce applications to a greater extent. The most attractive benefit of M-Commerce applications is the mobility. Even though users have a poor computer literacy, they will be able to use the M-Commerce applications easily. Additionally, the M-Commerce applications have the potential of reducing the distance barriers. In developing countries, especially in rural areas, accessing financial and banking services is a critical issue. This paper proposes a system called Mobile-ATM to address this problem by incorporating the mobile technology. Also it discusses the limitations of traditional ATM systems, the need of a new M-Commerce application to overcome the limitations and security related issues. In the proposed solution, people can withdraw money from a Mobile-ATM without going to a traditional ATM. The Mobile-ATM system uses even cheap mobile phones, functioning as payment terminals. It will reduce the limitations of traditional ATM and enables confidential and secured ATM transactions.

Categories and Subject Descriptors

K.4.4 [**Computers and Society**]: Electronic Commerce—*Security*

General Terms

Security, Design

Keywords

M-Commerce, Encryption, Authentication, Data Integrity, Confidentiality, Non-repudability, Mobile transaction

1. INTRODUCTION

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

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

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

Additionally mobile based solutions can archive more coverage. On the other hand one of the most important concerns with such transactions is security. The mobile networks are based on the use of poorly secured wireless protocols. 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 a number of commercial systems available for enabling banking services on mobile devices. Thus, most of these systems are based on the GSM network infrastructure and security features provided by the GSM network. Moreover these M-Banking systems use only electronic financial materials (like electornic coins) for the transaction [9]. In many developing countries, only very few facilities exist to perform transactions using electronic financial ma-

MobiArch'08, August 22, 2008, Seattle, Washington, USA.

terials. Therefore M-Banking system for developing countries should be capable to use actual notes and coins as the transaction medium.

Hence, we propose a new money withdrawal/deposit system (ATM system), that would enable people to perform their ATM transactions based on mobile technologies with additional security features.

The proposed Mobile ATM system will reduce some of the barriers of using ATM system and improve security related to ATM transactions.

2. THE ATM SYSTEMS

The traditional ATM system facilitates customers to access their bank accounts in order to make cash withdrawals or deposits and check their account balance. Although it inherits several weaknesses, at present there are thousands of ATMs scattered throughout the world. Such growth reveals that the ATM is a successful new technology that has been adopted by people. ATM is a pay-now payment system and mainly used for small and macro transactions [7]. The existing ATM system functions are explained in section 2.1

2.1 ATM Mechanism

1. A customer goes to an ATM machine and inserts his ATM card.
2. The ATM machine asks PIN number to authenticate the customer.
3. The ATM machine fetches the information stored on ATM card and sends this information with PIN number to banking network via a secured channel.
4. The bank matches this information with its database.
5. If mismatch not found bank will allow the ATM machine to continue the transaction.
6. The bank updates relevant accounts according to the transaction.
7. If a mismatch is found the ATM will withhold the transaction and ask authentication details again.

2.2 Weaknesses

Even though ATM is a very popular electronic transaction system, it associates with several weaknesses. In developing countries these issues become worse. Some of the major problems inherit with ATM are mentioned below.

ATM machines are not evenly scattered all around the country. Therefore users have to travel a large distance to use ATM facilities. In rural areas the situation is worse. Moreover, in most of the developing countries there are no national ATM switches. This means, interbanking ATM facilities are not available.

The initial cost of installing ATMs is very high. Also, ATMs typically connect to the ATM Transaction Processor securely, via either a dial-up modem over a public telephone line or directly via a leased line, which is expensive. In addition to that banking organizations need trained staff to maintain ATM devices. As a result maintenance cost of ATM machines is not economical.

Security, as it relates to ATMs, has several dimensions. There are reports that ATMs have become targets for vandalism. Sometimes thieves are attempting to steal entire ATMs. Shoulder attack [6] is another famous security threat related to ATMs. In order to protect ATMs from these threats, a security guard needs to be employed for every ATM.

Simply, both banks and ATM customers face lot of problems related to ATM.

The proposed system is designed in such a way that it can solve most of these problems and enhance the security of the transaction.

3. M-COMMERCE AND SECURITY

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. These types of applications/services include buying over mobile phone, purchase and redemption of ticket and reward schemes, travel and weather information and writing contracts on the move. These types of mobile applications are categorized as M-Commerce [9] applications. There is a significant and growing demand on deploying banking and financial services over mobile networks.

3.1 Strengths and Weaknesses

The M-Commerce applications are very useful for mobile users in many ways. Any user with a mobile phone can access M-Commerce application in real time at any place. Also the mobile devices provide security to a certain extent than 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 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 an M-Commerce application depends on the security of the underlying technologies and the mobile network bandwidth.

3.2 Security requirements

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 [8]. General cryptography concepts can be used to accomplish the trust between each participant.

Authentication: Authentication is the process of proving user identification. One party which involves in transaction needs to make sure that counter-party is the one he is 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.

4. MOBILE-ATM

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

4.1 System Architecture

Transactions take place the proposed M-ATM system 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.

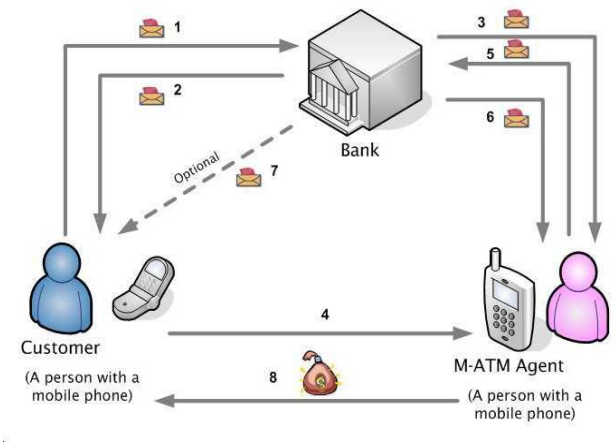

Figure 1: High level architecture of M-ATM

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 (M-ATM) phone number, requested amount.

2. The bank verifies customer's account and sends an authorization 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 (M-ATM) together with a transaction number (a random number is different from confirmation number).

4. The customer declares the confirmation number to the mobile ATM agent (M-ATM).

5. The mobile ATM agent (M-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 (M-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 a particular transaction to provide non reputability. Moreover it is a good evidence to confirm that, the transaction has happened completely.

4.2 System Roles

The operation of the system can basically be divided in to 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 M-ATM functions.
M-ATM Agent: Like the customer, M-ATM agent should have a bank account and a mobile phone. This mobile phone is also modified to perform functions of the M-ATM in a secured manner. He is an authorized person to perform M-ATM transactions by the bank. M-ATM agent keeps money in his hand and interest to hand over to the customers when there is a request.
Bank Organization: Bank should have M-ATM servers to deal with transactions between customers and M-ATM. This M-ATM servers should be directly connected to the bank's databases. In addition to that, the bank maintains the bank accounts of the customer and the M-ATM agent.

4.3 System Deployment

At the customer side there should be a special mobile application, suitable to operate the M-ATM functions. The application requires customer's PIN number for authentication purposes. In addition to that application requires M-ATM agent's mobile phone number and the amount of money to be withdrawn. Finally customer side application sends secure SMS message to the bank with the M-ATM mobile number, the amount of money to withdraw and the customers account number.

At the M-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 the transaction number, the confirmation number and the customer's mobile phone number to bank securely. This application also requires agent's PIN number for authentication purposes.

M-ATM server is providing registration and authentication services for the Mobile ATM. Furthermore the M-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. The random number generation program will not generate the same number for another transaction. After the 5th step, in section 4.1, M-ATM servers should be able to identify the two numbers, which belong to the same transaction.

4.4 Security Issues

Since the transaction happens mainly through SMS, security issues related to SMS should be considered by the proposed application [3]. Normally in the GSM network, sender and receiver of a SMS is identified by its IMSI [5], which an attacker cannot forge without breaking the GSM/UTM security mechanisms [7]. Therefore, these SMS messages can be used for authentication (at least towards the network). However this 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 the 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 M-ATM. Therefore, in this application it motivates to provide end to end security mechanism instead of depending on the GSM network security.

4.5 Security Architecture

4.5.1 Customer side security

Customer side security is provided based on the symmetric key cryptography. Figure 2 illustrates the security architecture. Here we make an assumption that the bank is a trusted entity.

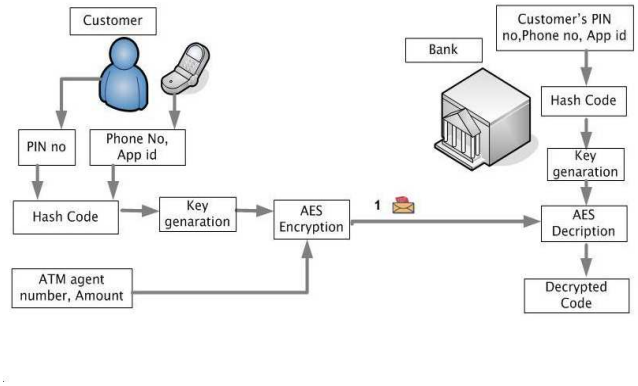

Figure 2: Security between customer and bank-1

Customer enters 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 M-ATM agent's phone number and the amount to withdraw. 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 the Customer PIN number, the Phone number and the 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 a success it means that the hash key stored in the 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.

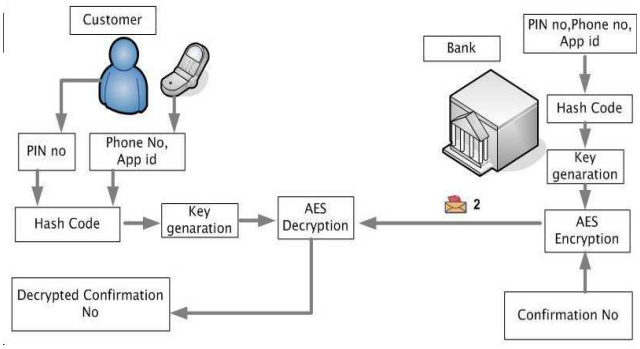

Figure 3: Security between customer and bank-2

The response to customer request is illustrated in Figure 3. Bank encrypts the confirmation number and sends it to the customer. Previously calculated hash code is used to generate the encryption key. If the customer successfully decrypts the message received from the bank, he can verify that the message came from the relevant bank. Because of sending encrypted messages, it provides data integrity and confidentiality.

4.5.2 M-ATM agent side security

M-ATA agent is an authorized person by the bank.

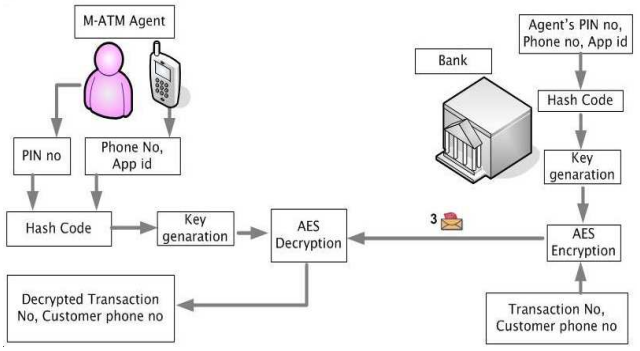

Figure 4: Security between agent and bank-1

As illustrated in figure 4 bank generates a hash code from the M-ATM agent's PIN number, his mobile phone number and his application ID and keeps it in the bank's database. This hash code is used to generate the encryption/decryption key. Then the bank encrypts the transaction number and the customer's phone number. At step 3 in figure 1 bank sends this encrypted message. At the M-ATM agent side, agent enters his PIN number and the application itself gets the mobile phone number and the application ID. The M-ATM agent calculates the hash code from these parameters and generates the encryption key. Therefore the M-ATM agent can authenticate the relevant bank. Using the customer mobile phone number with the message, M-ATM agent can identify the transaction number which belongs to the relevant customer. Because of the message encryption, it provides the integrity and confidentiality of data.

At the step 5 of figure 1, the M-ATM agent encrypts the confirmation number (which has been obtained from the customer) and the transaction number. Calculated hash code in step 5 of figure 1 is used to generate the encryption key.

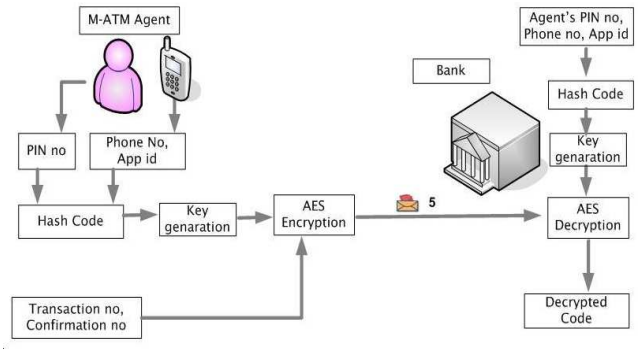

Figure 5: Security between agent and bank-2

Then the bank can authenticate the M-ATM agent. This message also provides the integrity and confidentiality of data. Figure 5 illustrate this architecture.

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

5. DISCUSSION

One of the distinguished features of the Mobile ATM system, that makes it different from any other similar system, is its security.

All participants in the Mobile ATM system are registered through a face-to-face procedure, so that all identities are strongly verified. Identification, financial and authorization data are stored in databases in the encrypted form. Therefore, they cannot be illegally accessed by unauthorized individuals.

According to the section *4.5.1* a customer should enter his PIN number, and the customer side application generates the encryption key based on the PIN. The bank uses the prestored pin number to generate the decryption key. Therefore the Mobile-ATM system provides the authentication. The M-ATM agent authentication takes place in the same way.

All the messages pass through the mobile network are in encrypted form. Thus, the system provides the integrity and confidentiality.

It is very convenient to have non-reputability for the electronic transactions.

According to the section *4.1* the bank generates and sends two random numbers, the confirmation number to the customer and the transaction number to the M-ATM agent. To complete the transaction, the system design enforces customer to disclose the confirmation number to the M-ATM agent. Only after that, the M-ATM agent is authorized to hand over the money to the customer. In the context of the M-ATM agent, the confirmation number received from the customer is a good evidence to verify that the transaction has happened completely. Very similar to the above described scenario, bank transfers money from the customer's account to the M-ATM agent's account after receiving the transaction number and the confirmation number from the M-ATM agent. Hence, none of the parties can rollback the transaction in illegal way. Moreover, the transaction number received from the M-ATM agent is a good evidence to verify that the M-ATM agent has completed the transaction. So, the proposed system provides non-reputability for both customer and M-ATM agent.

At present the Mobile ATM system uses a centralized M-ATM server. Thus, an unavailability of the M-ATM server may hold all transactions. In order to overcome this problem, decentralized M-ATM server architecture should be implemented in future versions.

System uses five mandatory SMS messages for a particular transaction. Commission must be paid to the M-ATM agent. This commission should be paid by the customer. The cost of the SMS messages can be distributed among the customer and the bank. In bank's point of view, it is economically advantageous to pay for the SMS messages instead of deploying traditional ATM machines.

6. CONCLUSIONS

The propose system successfully addresses the issues of difficulties in accessing ATM services in the rural areas of developing countries. It enables more security regard to the ATM transaction. As well as proposed M-ATM system provides legally accepted evidence about the transactions. 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.

The proposed Mobile-ATM system is being implemented in a rural bank in Sri Lanka.

We are confident that this application would address a major service gap in developing countries that is critical to their social and economic development.

7. ACKNOWLEDGMENTS

The work proposed 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.

8. 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 infaastructure. *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 (ISCCŠ03)*, 2003.

[5] Kumar, K. Shailaja, G. Shailaja, A. Kavitha, and A. Saxena. Mutual authentication and key agreement for gsm. *International Conference on Mobile Business (ICMB'06)*, pages 25–26, 2006.

[6] 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.

[7] Schwiderski-Grosche and H. Knospe. Secure m-commerce. 2004.

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

[9] Wishart and Neville. Micro-payment systems and their application to mobile networks. 2006.