SMS Based Mobile Banking

Surapaneni Pujitha*, B Veera Mallu**

*(Department of Computer Science And Engineering, K.L University, India
** (Department of Computer Science And Engineering, K.L University, India

Abstract:
M-banking has one of the main division of m-commerce. Mobile banking services consists of information inquiry, notifications and alerts, applications and payment transfer.Mobile based application is used for connecting customer handset with bank server for all such services. Current M-banking applications used by banks are facing security challenges for payment transfer banks are using secure payment gateway and other security measures which increases cost and infrastructure for bank but major day-to-day banking applications are inquiries, notifications and alerts. The problem with current banking applications is that they send data directly to customer in plain text form compromising with security.

We present SMS based secure mobile banking which enhances security with minimum cost. In this approach bank hides customer transaction data is secure SMS using AES symmetric cryptographic algorithm and send it customer application supported handset. Customer application decrypts data in secure manner.

Keywords: M-banking, MD5, AES, MPIN

1.INTRODUCTION:

M-banking system is one which provides all daily banking operations to customer with one click of his mobile handset with supported application. M-banking system has potential to provide access or delivery of very specific and highly necessary information to customer . Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and Integration of other m-commerce services with mobile banking. In M-banking there is no place restriction, it is highly penetration coefficient as growth of mobile phones are more than computers, it is fully personalized and private increasing transaction authenticity and is 100% available all the time with users.

However, there are several challenges that need to be addressed to completely utilize the benefits of the M-Banking like handset compatibility, security, scalability, reliability. Due to increase in use of mobile handsets for many m-commerce applications, Chances of mobile hacking for financial benefits are heavily increased.Currently mostly all banks in India and outside are sending text SMS directly to the customer handset for basic bank services without any security which can be accessed by any malicious person and can use this information for getting access to customer account. OTA (Over-the-air) mobile data can be hacked in network path from bank to customer mobile handset including MPIN, a password use for user identification in M-banking. Thus there is a need of secure and cost effective solution which can be easily provided on all types of handsets. Our objective is to provide cost effective, secure, fast M-banking solution combining features of cryptography.

In this paper we have presented SMS based secure mobile banking with minimum cost using cryptography.

2. M-BANKING CHANNELS:

M-banking can be executed using various channels like SMS, USSD, GPRS, WAP; Phone based Application, SIM Application. All of these channels are used separately or combined for various banking operations

A. Short Message Service (SMS)

SMS is the simplest form of mobile banking. It is largely used for information-based services. SMS has the maximum reach amongest consumers since all the mobile phones support SMS. Short messages are stored and forwarded by SMS centres. These messages have some security issues.

B. Unstructured Supplementary Services Delivery (USSD)

USSD is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signalling channels of the GSM network. USSD provides session-based communication. Turnaround response times for interactive applications are shorter for USSD than SMS. In USSD, the interaction is in the form of a continuous session as opposed to SMS. USSD is available on all handsets.

C. Wireless Application Protocol (WAP) / General Packet Radio Service (GPRS)

GPRS is a packet-switched data service available to GSM users.GPRS enables services such as WAP access, Multimedia Messaging Service (MMS), and Internet communication services such as email and World Wide Web access in mobile phones. WAP is wireless application protocol used over GPRS. It is similar to Internet banking. The consumer's handset needs to be WAP enabled. WAP banking is open to similar threats as Internet banking.

D. Phone-based Application

Phone based applications are developed in various languages like J2ME, .NET having advantages that it can use GPRS, USSD or SMS, MMS to carry the consumer data/instruction in an encrypted format and it is operator independent. These are secure application which resides on supported handset.

E. SIM Application Tool Kit

The SIM Application Toolkit allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card. STK is the most secure method of mobile banking. It allows the bank to load its own encryption keys onto the SIM card with the bank's own developed application.

3. CURRENT M-BANKING

Even though various channels are available for M-banking most of the banks uses SMS as basic and cheap channel for basic banking operations. Currently all banks in India like ICICI, HSBC, SBI etc are not using any encryption techniques in SMS based M-banking system. They are using simple text based SMS for customer queries in which they directly send account information to customer only hiding some digits of account number which can be easily hacked by any hacker or seen by anyone from message inbox. Even though some banks do provide some other channel like GPRS and WAP but cost of implementation is more and these facilities are not available on all types of mobile handset thus there is a need of secure and cost effective solution which can be easily provided on all types of handsets.

A. Issues in M-banking

1) Lack of Standards: The lack of standards gives rise to lot of local and fragmented versions of m-payments offered by different stakeholders. Standards need to address security and privacy concerns of customers as well as interoperability between various implementations.

2) Device constraints: There are technical issues related to the mobile devices .The mobile phones suffers from various constrains like less processing power and memory, bandwidth, short battery life , frequent disconnections, tiny screens, poor resolution and privacy issues.

3) Security Issues: Securing m-Commerce is even more difficult than wired transaction. Device constraints raise the questions as to whether there will be adequate security for users without compromising the ease of use and speed. Current real time M-banking application of various banks uses plain text messages without any security algorithm for sending data hence any malicious user can access customer important data on mobile and used it for malicious purpose thus direct sending of data is not suggestible for M-banking. SMS are prone to spoofing and there are issues related to SMS encryption. However technology manufacturers are developing improved security for applications with authentication and encryption technologies and many claims that the transaction using mobile device is fully secure. There are many techniques for secure M-banking operations but major research work has been done on Cryptography and steganography techniques. Cryptography is a process of converting plaintext data into cipher text using cryptographic algorithms. They insure basic security requirements like authentication, confidentiality, integrity and non-repudiation.

B. Basics of Short Message Service

Short Message Service (SMS) is the ability to send and receive text messages to and from mobile telephones. SMS was launched as a part of GSM1 standard. Each short message is up to 160 characters in length. The 160 characters can comprise of words, numbers, or punctuation symbols. Short Message Service is a store and forward service; this means that messages are not sent directly to the recipient but via a network SMS Centre.

SMS comprises two basic point-to-point services as Mobile-originated short message (MO-SM) and Mobile-terminated short message (MT-SM). Mobile-originated short messages are transported from MO capable handset to SMSC whereas Mobile-terminated short messages are transported from SMSC to the handsets. The figure no. 1 shows a typical organization of network elements in a GSM network supporting SMS.

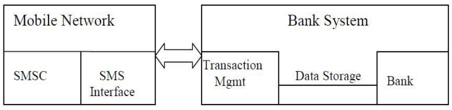


Fig. 1. Basic model of SMS based M-banking

The benefits of SMS to subscribers are convenience, flexibility, and seamless integration of messaging services and data access, delivery of notifications and alerts, guaranteed message deliver, reliable, low-cost communication mechanism, increased subscriber productivity, delivery of messages to multiple subscribers at a time.

The SMSC (Short Message Service Centre) is the entity which does the job of store and forward of messages to and from the mobile station. The SME (Short Message Entity), which is typically a mobile phone or a GSM modem, can be located in the fixed network or a mobile station, receives or sends SMS. The SMSC usually has a configurable time limit for how long it will store the message. SMS Gateway

SMS Gateway is an interface between software applications mobile networks. An SMS Gateway allows interfacing software applications to send and/or receive SMS messages over mobile network.

A GSM Modem modulates outgoing digital signals from a computer or other digital device to signals for a GSM network and demodulates the incoming GSM signal and converts it to a digital signal for the computer or other digital device.

4. PROPOSED SOLUTION:

Current real time M-banking application of various banks uses plain text messages without any security algorithm for sending data in SMS banking hence any malicious user can access customer important data on mobile.

Proposed secure M-banking is based on symmetric cryptographic techniques where common secret key is shared among bank customer and bank server. Proposed Architecture consists of 4 components as Customer Mobile application, Bank Server application, Bank side mobile / GSM Modem, Bank database and wireless OTA [1]. Our solution uses windows mobile as client application platform and .NET framework as server side software. Customer interested in using M-Banking facilities has to make registration only once with corresponding bank. Bank has all necessary details of customer in database. Bank sends Customer–side mobile application developed for windows mobile to user. Application will be installed once on windows mobile supported handset. This application consists of Login screen along with get session key option, menu screen for bank services options, and encryption and decryption screens for outgoing and incoming secure SMS and send message screen to send SMS to server GSM handset /Modem. Application will be updated as and when bank updates it.

Bank will have GSM mobile Handset / GSM modem connected to bank application server. GSM handset will be connected to application server using either Bluetooth or USB cable having SIM card installed in it which has task of receiving, processing and replying customer SMS continuously. GSM handset/ modem are cheaper and can be easily installed but have slow speed for message handling which can be increased by

connecting modem with SMSC centre over internet.

Secure M-Banking server side application is developed in windows compatible environment like VB.NET which can be installed on bank application server. Application is consisting of SMS Service,Information Manage, Account Details Manage, User Request modules to receive and process secure encrypted message from customer mobile. SMS Service module is responsible for retrieving and replying secure SMS automatically whenever they reaches server GSM handset / Modem.

Bank database consists of various tables storing customer details pertaining to his personal information,Account information and transaction information. Bank database stores customer confidential information like his MPIN, Mobile identification pin and encryption keys in encrypted and secure manner.

We have discussed various major types of M-Banking channels as SMS, GPRS, WAP and USSD out of which every channel has own advantages and disadvantages. WAP and GPRS are good and provide session based security but they are handset dependent and also in rural part of India all mobile operators are not providing respective services.USSD is used along with SMS and requires separate infrastructure.

Thus SMS channel is simple, easy to implement, cheaper and widely used channel which is device independent. Current SMS based M-banking service has many drawbacks as SMS is inherently developed in GSM for non-sensitive message transfer among users. Mutual authentication, text encryption, end-to-end security and non-repudiation is not present in design of GSM architecture [16]. Major issues with SMS based banking are SMS Spoofing which is an attack where malicious user sends out SMS message which appears to be sent by original sender. Current SMS architecture allows hiding original sender's address by altering respective field in original SMS header. Also SMS has encryption only during path from base trans receiver station and mobile station.End-to-end encryption is not available.

5. IMPLEMENTATION:

We have implemented proposed solution in .NET platform for windows mobile in windows environment. Customer mobile application in .NET framework runs on supported windows mobile handset for which we have used HTC mobile and bank server application is running in .NET along with any GSM handset connected in Bluetooth / USB mode to it. We have added secure SMS structure which provides extra security

along with satisfying security parameters. This secure SMS will add extra security features like cryptographic and hashing algorithm to satisfy confidentiality, integrity,

authentication and non-repudiation. Our system is based on secure SMS protocol and it uses SMS as media to send and receive encrypted information.

.

A. Secure SMS Message Structure

The secured SMS message is divided into multiple fields's to accommodate for the various security checks required for the protocol. Figure no. 2 shows the structure overview for a secure SMS message. The use of each labelled structure is explained below.

Account Session Key
No (generated from MPIN)
(6 Digit)

Cipher Text Message
(Plain Text+MPIN) Digest

Fig. 2. Secure SMS message Structure

Secure SMS message structure proposed by us consists of 4 fields's as shown in above figure.

Account Number: - It is customer account number in bank which is first field used for authentication purpose. This information is stored in plain test format so that at the server end, information can be retrieved to get required keys from database.

Session key: - It is onetime key randomly generated from customer MPIN inputted in bank server database during M-Banking registration process. This key is stored in 2nd field of message. Customer makes a request to get session key from his handset to bank server. Bank server will reply this with encrypted session keys stored in file, which will be stored on customer handset.

Cipher Text: - This text is created from combination of plain text and MPIN and stored in 3rd filed of message structure. Main idea behind this is to protect data from malicious attacker. As MPIN is most important data and from which session keys are created to be used for encryption and decryption purpose, hence it s send in encrypted manner.

Message Digest: - Message digest is used for checking integrity. Customer message digest is calculated from combination of plain text and MPIN and stored in 4th field of secure SMS. MD5 algorithm is used to calculate message digest on both ends. This received digest will be compared with calculated digest at bank server end , if not found of same size then message will be discarded as fake transaction and no message will be send to mobile handset from which request is sent.

B. Sending Secure SMS from Client Mobile

Whenever customer wish to make any transaction using M-banking, he will run application installed on handset and provide all necessary details. We have used 6 transactions for testing purpose and information collected from user on his handset is used to generate secure SMS. After registration customer will get mobile application installed once on his windows mobile. Customer will enter 4-digit MPIN which will be stored in server database in encrypted format using his password. For non-repudiation purpose we have added concept of one time session key. Server uses customer MPIN to generate session key randomly and again stored them in encrypted format.

Customer runs the banking application and feed details of 6-digit account number, 4-digit MPIN and 4-digit password and click button to get session key. Server sends generated session key to customer handset which will be stored in encrypted format on his handset. Customer goes to menu screen, chooses requires account type and type of transaction he wish to perform and goes to next screen. Mobile client application shows 4 entries on next screen consisting of session key received, generated fixed plain text message depending upon transaction chosen, cipher text created from combination of plain text and MPIN and 4-part secure message. Secure SMS contains account number in plain text, session key in encrypted format, cipher text created from plain text and MPIN and message digest calculated from message. Customer will send message to sever using as normal message.

C. Receiving and Replying Secure SMS from Server Module

Proposed Server is running on computer installed with required software like VB.NET, Windows mobile device centre and SDK, .NET compact framework, MS-access and Server side application. Server side application has four modules as SMS Service, Information Manage, Transaction Manage and User Requests. SMS service module retrieves SMS received at Server side handset and decode it to get original query send by customer. Server application process query, get required data from bank database and then sends it in encrypted format to customer mobile through bank side modem.

Whenever Customer sends any secure SMS containing his transaction query to server side GSM Modem, Server application automatically retrieves secure SMS and deletes it from server attached handset to avoid flooding of message inbox. We have used ActiveX control for this purpose. Bank Server application splits received secure SMS in same 4-parts.

Server reads first part, a plain text 6-digit account number and compares it with database stored account number. If match is not found, it will send message “Wrong Account Number” to customer handset. If account match is found then server uses 2nd part of secure SMS, which is session key send by user to decrypt 3rd part of received secure SMS.

After decrypting 3rd part of SMS, server application gets combination of plaintext as customer original transaction query followed by 4-digit MPIN. Server application compares received MPIN with stored MPIN from server table if a match is not found, will send message “Wrong Pin Number” to customer handset.

Server calculates message digest of 3rd part received using MD5 algorithm and compare it with received massage digest, 4th part of secure SMS to check for message integrity. If match is not found, server generates message on server side “Fake Transaction” and sends nothing to customer side handset as it may be off any malicious user.

If all security checks are proper, Server application process query of customer and get required data from database encrypts data using session key received from customer and sends automatically to customer handset.

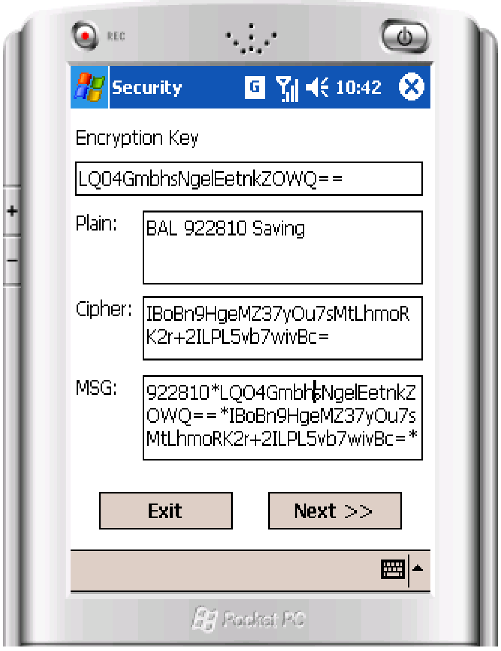
6. EXPERIMENTAL RESULTS:

We have developed two applications for client and server side. Mobile client application is developed using .NET compact framework and VB.NET, installed on windows mobile supported HTC mobile device. This application is used by customer for

various M-banking transactions to send encrypted secure SMS to bank Server and gets back encrypted reply from bank Server. Client and Server side application performs symmetric encryption and decryption using 256-bit AES symmetric encryption algorithm. MD5 algorithm is used for hashing purpose. Server side bank application is developed using VB.NET it uses SMS toolkit, an ActiveX control to retrieve and process secure SMS automatically. Server side application also contains certain modules for database management of customer account and transactions

Normally symmetric cryptographic algorithm don't have non-repudiation as both party shares common secret key but we have used session key concept for maintaining non-repudiation property of encryption. Since Session key is used only once and created randomly, no two users can have common session key and it is created from MPIN, a master key which customer only knows so he cannot deny that he has done transaction.

We have carried out 6 types of transaction including Account Balance, Mini transactions, Cheque Book Request, Cheque Stop request, Pay Bill and Fund Transfer. Following are some sample client application module. The figure no. 3 shows session key, user query in fixed plain text format, cipher text generated from combination of plain text and his MPIN and 4-part secure SMS message generated as per format discussed. This last message is sent to server.



Encryption Key

LQ04GmbhsNgelEetnkZOWQ==

Plain: BAL 922810 Saving

Cipher: IBoBn9HgeMZ37yOu7sMtLhmoRK2r+2ILPL5vb7wivBc=

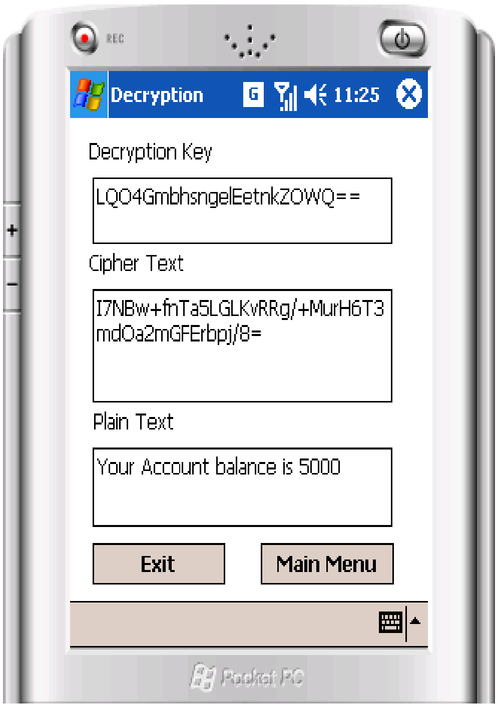
MSG: 922810*LQO4GmbhsNgelEetnkZOWQ==*IBoBn9HgeMZ37yOu7sMtLhmoRK2r+2ILPL5vb7wivBc=*

Fig. 3. Generating 4-Part Secure Message

This secure SMS is retrieved by server side SMS service module. Server application split message and decrypt it to get original transaction query of customer. This query is processed to get response data from database which is firstly encrypted and then send to customer handset.

Customer handset get auto reply from server side in cipher text, which is decrypted on mobile by client side application to get server response in plain text. The Figure no.4 shows response obtained automatically from server for account balance. This reply consists of 3 parts. First part is common session key used by server and client. Second part is cipher text received from server application in secure manner. Third part is plain text message obtained after decrypting secure message received from server. Client mobile application uses 256-bit AES algorithm to decrypt message using common session key.

This message will be hidden from customer and he will only get final query results in plain text format but for result purpose we have shown this screen.



Decryption Key

LQO4GmbhsngelEetnkZOWQ==

Cipher Text

I7NBw+fnTa5LGLKvRRg/+MurH6T3
mdOa2mGFErbpj/8=

Plain Text

Your Account balance is 5000

Fig. 4. Secure Reply from Server

To be a secure system, it must satisfy Confidentiality, Authentication, Integrity and Non-Repudiation Secure SMS system maintains confidentiality using AES cryptography and Non-Repudiation using session key. Here 3-factor authentication is used for authentication and security purpose whereas Message integrity is carried out using MD5 algorithm.

7. CONCLUSION AND FUTURE WORK:

We have implemented a secure SMS based Mobile Banking system. The system allows user to carry out all banking transaction securely from anywhere, anytime. All messages from user windows mobile are sent in encrypted format to bank server. Bank server decrypt message, process query and encrypt result in SMS.Server sends message to customer which will be decrypted on his handset. The evaluation of the system was studied for varying banking transaction and under various security threatening malicious activities were recorded. Performance of the transaction is studied.

We have executed few banking transaction from HTC windows mobile and using VB.Net server side application. We have used LG GSM mobile as server attached mobile device. Experiments shows that secure SMS Mobile banking provides cost effective and secure system with satisfying Confidentiality, Authentication, Integrity and Non-Repudiation using symmetric cryptography. Application can be used on any windows mobile supported handset from anywhere as no GPRS and WAP are required.

We have implemented system using symmetric key AES algorithm. In future better power consumption algorithm like blowfish can be tried out. Steganogrpahy can also be applied for secure M-banking transactions. We can use concept of STK, SIM application toolkit where bank can stored the application and encryption keys on SIM.

REFERENCES:

[1] Przemyslaw Krol, Przemysław Nowak, Bartosz Sakowicz,”Mobile Banking Services Based On J2ME/J2EE”, CADSM’2007.

[2] Yousuf S. AlHinai, Sherah Kurnia and Robert B. Johnston,”Adoption of Mobile, Commerce Services by Individuals: A Meta-Analysis of the Literature”, Sixth International Conference on the Management of Mobile Business .

[3] T N T Nguyen, P Shum and E H Chua,”Secure end-to-end mobile payment System”.

[4] Ashutosh Saxena, Manik Lal Das and Anurag Gupta,”MMPS: A Versatile Mobile-to-Mobile Payment System”, Proceedings of the International Conference On Mobile Business 2005.

[5] Iuon-Chang Lin and Yang-Bin Lin,”An Efficient Steganography Scheme for M-Commerce”.

[6] Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza, ”Text Steganography in SMS”, 2007 International Conference on Convergence Information Technology.

[7] Sandeep Singh Ghotra, Baldev Kumar

Mandhan, Sam Shang Chun Wei, Yi Song, Chris Steketee, ”Secure Display and Secure Transactions Using a Handset”, Sixth International Conference on the Management of Mobile Business.

[8] Jiehua Wang, Song Yuan, “A Novel Security Mobile Payment System Based On Watermarked Voice Cheque”.

[9] M. Shirali-Shahreza, "Stealth Steganography in SMS", Proceedings of the third IEEE and IFIP International Conference on Wireless and Optical Communications Networks 2006.

[10] Kewin Chikomo, Ming Ki Chong, Alpan Arnab, Andrew Hutchison, “Security of Mobile Banking”.