Tactful Management Research Journal
ISSN: 2319-7943
Impact Factor : 2.1632(UIF)

A PRACTICAL APPROACH TO SECURE SMS BASED M-BANKING

Pallavi Wani

Ramanand Arya DAV College, Bhandup (E).

Abstract : M-Banking has emerged as one of the main division of Internet banking. M-banking services consist of information enquiry notifications and alter apps and payment transfer. Mobile based applications are used for connecting customer handset with bank server for all such services. The problem with M-Banking application is that they send data directly to customer in plain text form, compromising with security.

I present SMS based secure M-Banking which enhances security with minimum cost. In this approach the bank hides customer transaction data in secure SMS using Symmetric cryptographic algorithm and sends it to customer application supported handset. Customer application decrypts data in secure manner. The encryption and decryption are characterized by a session key that the legal parties have to posses. So in face of current security issues and the growing number of attacks and consequence frauds, M- banking should be designed to address the security concern.

Keywords: M-Banking, Plain Text, Cipher Text, Session Key, Encryption Decryption.

I.INTRODUCTION

In M-banking schemes; financial services are availed and provided to customer with one click on his mobile handset with supported application. Mobile services are highly adopted in developing countries because of the rapid growth in mobile hardware. It is estimated by the International telecommunication union [ITU] that at the mid of the year 2014, there were nearly 7 billion mobile subscripts worldwide and it is predicted by Portion Research in its “Mobile Fact book 2013" that by the end of 2016 the global subscribers will reach 8.5 billion [1]. There are currently 570 billion mobile phones in India and 100 million are added every year. This shows that the mobile technologies are rapidly being adopted (both logically and globally).

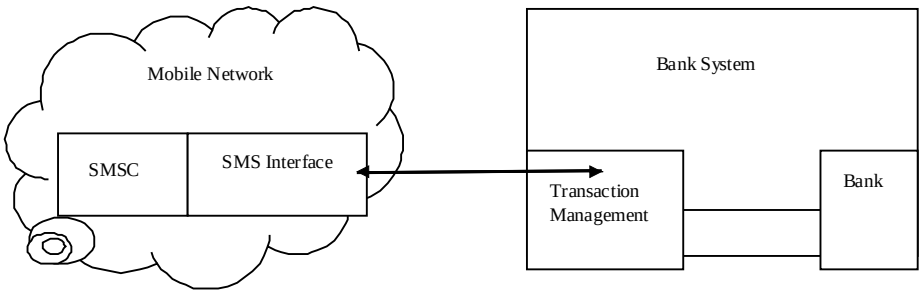
With technology growth, M-Banking is growing popularly over Internet banking. In case of Internet or Online banking you need a computer and Internet connection to access your account and this become a problem during urgency or when don't have Internet connection .However this not problem with M-Banking as network connection is available in remote areas. Using M-banking transferring money or any other transaction can get done with few minutes. M-Banking keeps update with any activity done in account. For example, money withdraws, money transfer, other transaction to account will be informed via SMS.

However there are several changes that meet to be address to completely utilise the benefits of the M-banking like handset compatibly, security, scalability, feasibility. The currently security model for M-banking in use are strongly based on online user identification and authentication method, which also has hacking problem. Mostly all banks in worldwide are sending text SMS directly to the customer handset without any security which can be accessed by any unauthorised person and can use this information for getting access to customer account . Thus there is a need of secure and cost effective solution for M-banking.

II. BASICS OF SHORT MESSAGE SERVICES

SMS is ability to send and receive message to and from mobile telephone. SMS was launched as a part of GSM1 standard. Each SMS is up to 160 characters and can be combination of words, number and punctuation symbols. SMS is a store and forwards service; this means that message sent directly to the recipients but via a network SMS centre.

SMS comprises two basic point to point services as Mobile Oriented Short Message (MO-SM) and Mobile Terminated Short Message (MT-SM). MO-SM are transported from MO capable handset to SMSC where as MT-SM are transported from SMSC to handset.



III .CURRENT SMS BASED BANKING

Presently, the customers have to walking to the bank to submit the registration form by giving their mobile number, account number. Each customer is given a four digit number for authentication. The customer can do the transactions only when the request is received from the registered mobile number along with 4 digits number. The mobile number acts as user id and 4 digits number as password for authentication. This approach is not fully secure because data is transmitted and network operator has full access to data. Due to plain text property SMS is not suitable for authentication. So lacking of privacy, intgrity and security are the main issues involve in SMS banking.

IV. PROPOSED SOLUTION.

Considering current system security issues, I propose SMS authentication method using symmetric cryptographic technique. This application consist of login screen along with get session key option, menu screen for banking services option and encryption and decryption screens for outgoing and incoming secure SMS and send SMS to server.

	Account Info	Payment	Transaction History	Services For You	Rewards
Get Session Key					
Encryption					
Decryption					
Send SMS					
Logout					

Trasaction Details	Billpay3456toac3490
Passaord	****
Encrypt	

Figure [2]

The below figure describes the architecture of the secure transaction, where the bank service sends encrypted messages to the user the used encrypts the message.

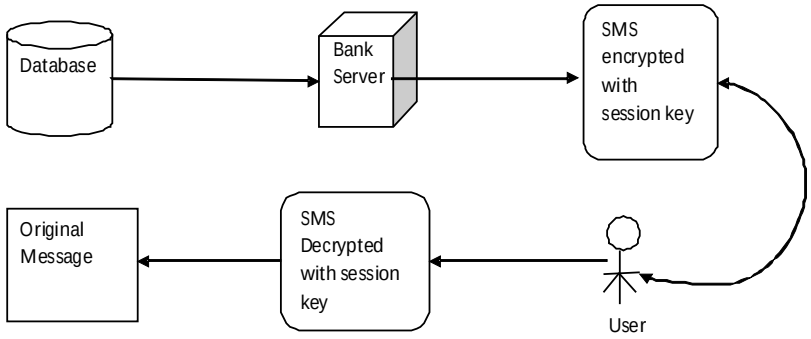


Figure [3]

A.Secure SMS Structure

Account Number | Encrypted Session Key | Encrypted Message

Account Number: It is customer account number in bank which is first field used for authentication. It is stored as P.T so that server can be retrieved the required keys from database. Session key: It is one time randomly generated key from customer password and personal information inputted in bank database during M-banking registration process. Cipher Text: This text is created from the combination of transaction details and password.

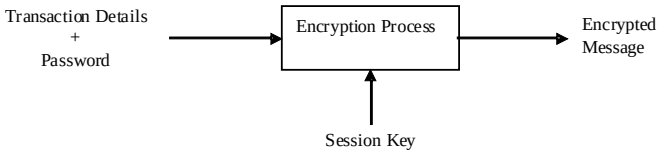


Figure [4]

In this application for making encrypted messages using cryptographic methods based on the IDEA algorithm.

International Data Encryption Algorithm (IDEA) is very secure; IDEA operates on 24 bit blocks using 128 bit key and consist of a series of eight identical rounds and an output transformation. The process for encryption and description is similar. IDEA rounds have a lot of mathematical actions such as multiplier addition an XOR operations more secure.

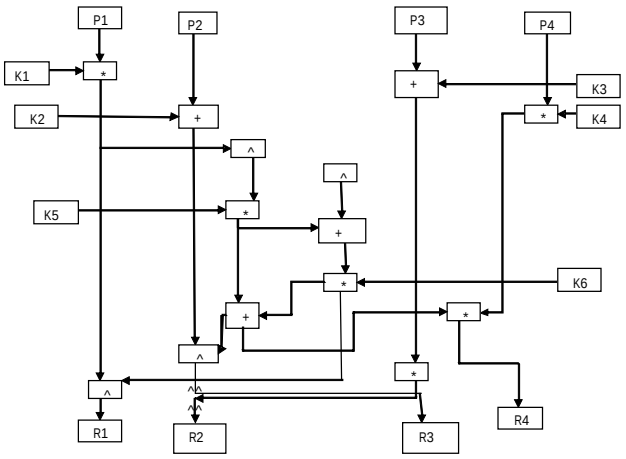


Figure [5]

B. Sending Secure SMS from client Mobile

After registration customer will get mobile applications installed on his mobile. Customer will enter 4 digit password which will be stored in server database in encrypted format wherever customer wish to make any transactions using M-banking, he will run installed application or his handset and provide all necessary details; 6-digit account number, 4-digit password click button to get session key .

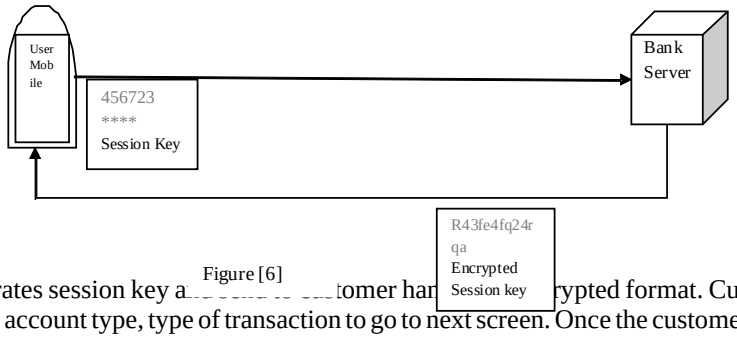


Figure [6]

Sever generates session key a[illegible]tomer har[illegible]rypted format. Customer goes to menu screen chooses account type, type of transaction to go to next screen. Once the customer transaction is complete mobile client application will generate encrypted message fig. [4] Next screen contains 3 entries 1.Accont number 2.Encrypted Message and 3.Encrypted Session Key. Customer will send message to the server as normal message.

C. Receiving & Responding Secure SMS from server

Whenever customer sends any secure SMS, server reads first part, a plain text 6 digit account number & compares it with stared account number at database. If match is not found, it will send message" Wrong Account Number" to customer handset. If account match found server uses 2nd part of SMS i.e. Encrypted Session Key which is decrypted by password of customer stored in server database. If all security checks are proper server application process query of customer is encrypts the result using same session key sends to customer handset.
If decrypted session key not matches with server general session key server send messages "Invalid user" to customer handset.

V. CONCLUSION AND FUTURE WORK

M-banking has various services to its customer: customers are able to interact with their bank account as well as make transactions from anywhere without time restrictions. M-banking has various security threats that need to be resolved to improve privacy aspects. The future of M-banking will be a system where users are able to interact with their banks "worry Free". This paper describes current M-banking problems. I have designed a system allows user to carry out all banking transaction securely. All messages from user mobile are sent in encrypted format to bank server. Bank server decrypts message, process request and encrypts result in SMS server sends message to customer which will be decrypted on his handset. I have designed system using symmetric key IDEA algorithm.

The focus of my future works is to implement and test model in real environment for better power consumptions algorithm like blowfish, AES can be tried out.

VI. GLOSSARY

1.M-Banking: It refers to the use of a Smartphone to perform online banking tasks while away from your home computer, such as monitoring account balances, transferring funds between accounts, bill payment and locating an ATM.
2.Plain Text.: It is information a sender wishes to transmit to a receiver & which is in readable format .
3.Encryption & Decryption: Encryption is the process of translating plain text data into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext.
4.Session Key: A session key is an encryption and decryption key that is randomly generated to ensure the

security of a communications session.

VII REFERENCES

1)mobiThinking. Global Mobile Statistics 2013. 2013 [cited 2013 20 August]; Available from: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers.
2)T N T Nguyen., P Shum., & E H Chua. (n.d.). Secure end-to-end mobile payment System.
3)Dilla Salama Abdul Minaam., Hatem M. Abdul Kadir., & Mohily Mohamed Hadhoud. (n.d.). International Journal of Network Security. Evaluating the effects of Symmetric Cryptographic algorithms on Power, 11.
4)Richard E. Smith. Authentication: From Passwords to Public Keys. Addison Wesley, 2001.
5)Managing the Risk of Mobile Banking Technologies, Bankable Frontier Associates.
6)Kewin Chikomo, Ming Ki Chong, Alpan Arnab, Andrew Hutchison, "Security of Mobile Banking".
7)A. Hiltgen., T. Kramp., & T. Weigold. (n.d.). IEEE Security and Privacy. Secure Internet-banking Authentication, 4, 21-29.
8)Shirali-shahreza, M. (2007). Improving Mobile Banking Security Using Steganography. doi:10.1109/ITNG.2007.108