

Mobile Money: M-payment System for India

Sujata P. Deshmukh, Archana M. Naware

*Department of Computer Engineering, Lokmanya Tilak College of Engineering,
Sector-4, Koparkhairane, Navi Mumbai – 400709.*

Abstract— *Mobile Commerce is Electronic Commerce on Mobile a device which is carried out with mobile devices to purchase goods or services using wireless environment. Due to rapid growth of number of mobile phone subscribers in India, mobile phones are proved to be an alternative channel of delivery of banking services. Mobile payments are carried out by SMS based transactional payments, Direct Mobile Billing, Mobile web payments, Contactless Near Field Communication. The users do not need to carry physical money. They do M-Payments to pay school fees, hospital bills, electricity bills, recharge mobiles, pay bus fare, taxi fare using mobile device and internet.*

The system “Mobile Money: M-Payment System for India” proposes a new mobile payment system in which sender sends money to receiver using his mobile phone. The proposed system considers the unbanked population of India. The system uses the vouchers to recharge Mobile Money Account. With this application sender specifies amount and sends to the receiver. Receiver gets the amount from Bank, ATM. Unbanked users can withdraw the amount from Mobile Money outlet or the amount will be credited to phone bill.

Key Terms — *M-commerce, E-commerce, M-Payment*

INTRODUCTION

Electronic Commerce (E-commerce), conducted over mobile communication devices such as mobile phones is Mobile-commerce i.e. M-commerce. M-commerce is evolved from E-commerce which includes all E-commerce transactions, carried out using a mobile (hand held) device [9]. Countless growth of mobile phone subscribers in India causes continuous growth of M-commerce applications which includes the purchase and sale of goods and number of services, net banking, payment of bill, information delivery and so on. Reachability, Mobility and Flexibility are major attributes of M-commerce which have enhanced the application area of M-commerce. Mobile devices are available and reachable everywhere than computers. Therefore, consumers can use M-commerce application easily to perform online transactions. Consumers have greater chances of getting better deals on mobile commerce sites. M-commerce applications have eliminated the need of buyer to go to a physical store because of which M-Commerce applications are time saving and money saving. Consumers access hundreds of products on mobile devices using M-commerce applications and internet. Merchants have a great opportunity to increase the business thru reach and sales using M-commerce applications. With these benefits it have limitations such as device tiny screen of device, weak processors, limited memory, poor resolutions, poor data entry, and lack of WAP-enabled

devices, expensive data speed, and shortage of bandwidth . M-commerce applications for commercial transactions are executed through Mobile Payments (M-Payments) systems. M-Payment is nothing but conducting the commercial transactions online. “Mobile Payment” is defined as information exchange between a merchant and its customers for financial transactions through the use of mobile phones. Mobile Payments are carried out by SMS based transactional payments, Direct Mobile Billing, Mobile web payments, Contactless Near Field Communication. Mobile payment involves debit or credit to a customer’s bank account on the basis of funds transfer instruction received over the mobile phones [11]. Due to quick evolution of M-commerce and number of mobile phone subscribers in India, banks have introduced mobile phones as an alternative channel of delivery of banking services. It includes fund transfer, loan payment (LIC home loans), premium payment (LIC policies), payment of utility bills, recharge mobile phones and so on. Ubiquitous property of M-commerce has changed the utility of the web as a business standpoint. A user can use a mobile phone to pay for a wide range of services and digital or hard goods instead of using cash, cheque or card payment. Thus the life is turned to be cashless with Mobile Payments.

LITERATURE REVIEW

“Mobile Money: M-Payment System for India” introduces a mobile payment system which will be useful for banked as well as unbanked people of India. When any mobile payment system is developed, it is very necessary not to ignore the unbanked people of India. Numbers of authors have suggested number of protocols for mobile payment systems. This literature review is brief discussion of their study and invaluable work in the area of mobile commerce as follow.

Sujata P. Deshmukh et al. (2013) discussed transformation of E-commerce into M-commerce, benefits and challenges of E-commerce and M-commerce. Further authors identified that biometric with unique identification number of the users can be used for transaction security in M-commerce and efforts have already started in India [2]. Tarek M. Mahmoud et al. (2009) proposed a technique in the paper entitled “Hybrid Compression Encryption Technique for Securing SMS” which compresses the SMS to reduce its length, then encrypts it using RSA algorithm to secure the SMS data [3]. Ali Grami et al. (2004) discussed future trends in major aspects of mobile commerce in the paper entitled “Future Trends in Mobile Commerce: Service Offerings,

Technological Advances and Security Challenges”. In this paper future trends in major aspects of mobile commerce are discussed. This paper tells that the highly – personalized, context-aware, location –sensitive, time-critical, pin-point information presentation forms the basis upon which promising M –Commerce applications can be built. Also privacy concerns, trust issues, and security challenges in wireless arena are discussed in this paper [5]. Manoj V. Bramhe (2011) presented the paper entitled “SMS BASED SECURE MOBILE BANKING”. The author presented the approach that bank hides customer transaction data is secure SMS using AES symmetric cryptographic algorithm and send it to customer application supported handset. Customer application decrypts data in secure manner [7]. Seema Nambiar et al. (2004) presented a paper entitled “ Analysis of Payment Transaction Security in Mobile Commerce” and presented an analysis of the security issues in mobile payment. The authors discussed the public key infrastructure as a basis for secure mobile technologies, and studied the features for different security technologies employed in current M-Commerce market [8]. Kwok-Yan Lam et al. (2003) presented a paper entitled “Lightweight security for mobile commerce transactions”. The authors proposed a lightweight mechanism which makes use of a combination of public key cryptography and simple password authentication. This mechanism establishes a symmetric secret key shared only by the mobile handheld device and the wireless protocol gateway [9]. Isern-Deyà, et al. (2011) proposed a micropayment scheme in the paper entitled “Untraceable, Anonymous and Fair Micropayment Scheme”. The scheme is anonymous as the coins do not have user identification. From past transactions user’s identity cannot be traced. Therefore the system is untraceable. Authors have eliminated the use of public key cryptography and used the concept of partially blind signature [1]. ICICI Bank and MCSL, a Vodafone group company group presented “MPESA” a mobile money transfer service for Vodafone subscribers. MPESA is proved to be helpful for customers for saving cost of travel expenses, ease of transacting whenever/wherever, reduced risk of carrying cash. MPESA service suffers when the connection between Safaricom and the customer’s bank fails. MPESA delays in processing the transactions because of verification at bank as well as Safaricom. Customers face troubles when withdraw money from bank account as bank gets delayed notification to credit customer’s bank account. Further, a borrower should have saving account as well as loan account in the bank [14]. In Budapest, Taxi fare is paid using Master card application. Smart phone is used to scan the QR code in the car to get car details. The amount announced by the driver and mPIN is entered by the customer. Taxi driver and Taxi Company receives payment confirmation message. Then driver issues invoice for the fare. The customer should be a banked customer [15].

M-PAYMENT SYSTEMS IN INDIA

Banks are using M-Payment systems as an alternative way of quick, safe payment system. There are numbers of

Mobile Payment services available in India as discussed below.

A. State Bank freedoM: State bank freedoM is SBI’s mobile banking service. Funds transfer (within SBI or other Bank’s account), Interbank Mobile Payment Services (IMPS) : Fund Transfer, Merchant Payments 24 x 7, Enquiry Services (Balance Enquiry / Mini statement), Cheque Book request, Demat Enquiry Service, Bill Payment (Utility bills, Credit Cards, Insurance premium), Mobile Top up, M-Commerce (DTH Recharge of TataSky, BigTV, SunDirect, DishTV, Digital TV and Videocon d2h connections, SBI Life insurance premium, etc.), Booking of train tickets over the IRCTC portal through IMPS are some of the services offered by this application [16].

B. iMobile: iMobile is the mobile banking service offered by ICICI. The customers can do Funds Transfer, bill payment, balance enquiry, Cheque Book Request, stop Cheque Request, Cheque Status Enquiry, open Fixed Deposit, open Recurring Deposit [17].

C. HDFC Bank Mobile Banking Application: HDFC bank offers HDFC Bank Mobile Banking Application for Android, Nokia, iPhone, blackberry, windows. It offers the customers to check account balance, transfer funds, to pay utility bills and much more. With this application the customers can access about 60 transactions anywhere, anytime. HDFC offers SMS banking for the customers [18].

D. Airtel-Money: This service is jointly offered by Airtel and Axis bank. The customers can load cash in Airtel Money account, make payments, send money, find retailers, donate money to NGO, recharge mobile prepaid account, recharge 2G data, recharge digital TV, pay postpaid bill, landline bill and pay utility bill amounts [19].

These are recent M-Payment systems in India. There are business rules such that account type of the customers required for subscription to mobile banking, transaction limit per day for each of the M-Payment services which is regulated by RBI.

SECURITY CHALLENGES OF M-PAYMENT SYSTEMS

There is a need to secure the M-Payment systems as the system can be attacked to steal the information. Different possible attacks to M-payment system are discussed below.

A. Man-in-middle Attack: Network authenticates the users.

The user does not authenticate network so the attacker can use a false BTS with the same mobile network code as the subscriber’s real network to take off himself and perform a man-in-the-middle attack [24].

B. Replay Attack: The attacker can misuse the previously exchanged messages between the subscriber and network in order to perform the replay attacks [24].

C. Message Disclosure: Since encryption is not applied to short message transmission by default, messages could be intercepted and snooped during transmission. In addition, SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages could be viewed by users in the SMSC who have access to the messaging system [24].

- D. *Spamming*: Though SMS are a practical publicity channel, many people have had the trouble of receiving SMS spam. The bulk SMS broadcasting utilities available makes it easy for virtually everyone to send out mass SMS messages [24].
- E. *Denial of Service (DoS) Attacks*: DoS attacks are sending frequent messages to a target mobile phone because of which mobile phone of the victim becomes inaccessible [24].
- F. *SMS Phone Crashes*: If susceptible mobile phones receives malformed message, it may crash and phone becomes unworkable [24].
- G. *SMS Viruses*: Mobile phones are getting more powerful and programmable and hence the potential of viruses being spread through SMS is also increasing [24].
- H. *SMS Phishing*: SMS phishing is a combination of SMS and phishing. It is similar to an Internet phishing attack. Attackers try to fool mobile phone users with fake text messages. When users attend the fake message, they may connect to a website which is delivered in the SMS message. Thus the user is trapped by downloading a malware application into their mobile phones [24].

SECURITY CHALLENGES OF M-PAYMENT SYSTEMS IN INDIA

In India M-Payment is carried out using SMS, direct mobile billing systems, mobile web applications. There is a need of end to end security to the system. Information should be encrypted at end to end in the transactions [13]. mPIN is used for authentication in mobile applications. The security to the username, password and mPIN should be given so that it cannot be beaked. Security to the information should be given when it is transferred from end to end in the system. Another approach to achieve transaction security is biometric identity with unique identification number for the users of the mobile commerce application. India has already started the efforts to achieve this [2].

The huge population of India is unbanked and economically poor. The M-Payment systems should be developed compatible for not only high configurations mobile phones but also for low configuration mobile phones such that poor population can also use the M-Payment applications on their low configuration mobile phones. In India people have different mother tongue language. Thousands of people do know only their mother tongue language. So there should be an option to select language for transactions in M-Payment systems in India. Awareness programs for M-Payment systems should be conducted by bank sectors to give guidelines to the customers. M-Payment systems in India are limited to Indian Currency. In M-Payment systems currency should be transformed from one type of currency into another under the rules and regulations of RBI.

CRYPTOGRAPHY AND SECURITY TO M-PAYMENT SYSTEM

The information to transfer on electronic communication channel such as internet is transformed into unreadable format. This is known as cryptography. The unreadable format of information or data is called as cipher text. The private key is used for deciphering the text. Converting unreadable information into readable form is called deciphering. Private Key is required to decipher the text. Email messages, credit card information, online banking and corporate data are made secure using cryptography. Cryptography which uses only a single key to be shared by sender and receiver of information is called as Symmetric Key Cryptography. Cryptography which uses public key to cipher the information and private key to decipher the information is known as Asymmetric Key Cryptography. Symmetric key algorithms run faster than asymmetric key algorithms and the memory requirement of symmetric algorithms is lesser than asymmetric encryption algorithms [11]. More processing power is required for asymmetric key encryption to encrypt and decrypt the information. Secure channel is required to exchange secret key in symmetric key cryptography Secret key should be exchanged in such that it should remain secret. Key management should be proper as different key is required for each different communicating party. It may result in problem to manage and ensure the security of all keys. In symmetric key cryptography authentication and origin of messages is not guaranteed. DES, triple DES, AES , Blowfish are known symmetric encryption techniques. Diffie–Hellman key exchange, Digital Signature Algorithm, RSA are known asymmetric encryption techniques.

PROPOSED SYSTEM

The people do not have computers, bank accounts but they have mobile phones. So there is a need for secure online transactions which can be carried out on mobile phones without the need of bank account and credit cards/debit cards. The proposed M-payment system eliminates the use of credit cards/debit cards. Fig. 1 shows the block diagram of Mobile Money: M-Payment System for India. The entities involved in the Mobile Money Application are as follow:

- A. *User 1*: User 1 is registered user of the application who will send money to the receiver.
- B. *User 2*: User 2 is registered user of the application who will receive money from the sender.
- C. *Mobile Money Application Server*: It will receive request and sends response to the end users. It will have centralized control on all activities.
- D. *Network service Provider*: It will provide mobile network to the subscribed users.
- E. *Bank*: It will maintain details of the users who have bank accounts.
- F. *Vouchers*: Vouchers are used to recharge Mobile Money Account.

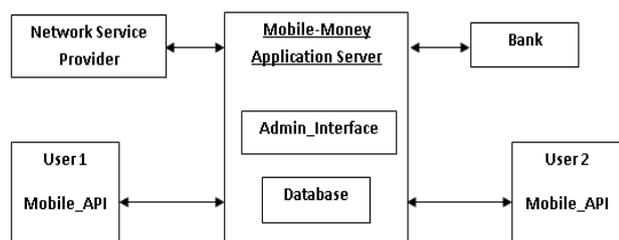


Fig. 1 Mobile Money: M-Payment System for India.

In the proposed system user will do registration for this application at bank or Mobile Money outlet or network service provider's office. After KYC verification user will get username and password by post or in hand. The user will be able to login the application on mobile phone using his/her username and password. In the proposed system hashing is used to secure the password of the user. One time password is generated for each successful login which adds one layer of security to the system. The money will be transferred in the form of coins in this application. Mobile Money account will be loaded by adding coins and unloaded by debiting the coins. The application will be used to pay school fees, bus tickets, payments of bills and to pay for a cup of tea. Mobile money account will be recharged using bank account, prepaid account or postpaid account and vouchers. In the proposed system coins can be encrypted using public key cryptography such as RSA. Further blind signature concept can be implemented to hide user identification of a coin. Performance of the application will be very slow as public key encryption techniques are slower than secret key encryption technique [1]. To make the application faster RSA combined with padding and compression technique can be implemented. Encryption to username and password will secure the system from Phishing attack. Encryption to coins will secure the system from man in middle attack.

CONCLUSION

Thus the paper discusses electronic commerce on mobile phones i.e. M-Commerce, applications of M-Commerce, benefits and limitations of M-Commerce. M-Payments systems are used to pay school fees, bus fare, electricity bill, hospital bill. There is no need for a user to carry cash. There are different ways such as SMS based transactions, Direct Mobile Billing to do M-Payments. Different M-Payment systems and security challenges of M-Payment systems in India are discussed. Cryptography for security of M-Payment systems and limitations of using cryptography on mobile devices is discussed. M-Payment systems in India offered by banks make use of credit/ debit cards or net banking. Unbanked people are totally ignored for these services. There is a need of M-payment system which will eliminate the use of credit/ debit cards or net banking. The paper proposes the system "Mobile Money: M-Payment System for India". In this M-Payment System the money sender will be able to send money to the receiver using mobile phones. The system will be anonymous and untraceable. Use of vouchers and elimination of net banking and credit/debit card will make the system useful for unbanked population of India.

REFERENCES

- [1] Isern-Deyà, Andreu Pere, Payeras-Capellà, M. Magdalena, Mut- Puigserver, Macià, Ferrer-Gomila, Josep L., "Untraceable, Anonymous and Fair Micropayment Scheme", The ninth International Conference on Advances in Mobile Computing and Multimedia, 5-7 December 2011, Ho Chi Minh City, Vietnam.
- [2] Sujata P. Deshmukh, P. Deshmukh, Prashant Deshmukh, G. T. Thampi, "Transformation from E-commerce to M-commerce in Indian Context", IJCSI, Vol. 10, Issue 4, No 2, July 2013.
- [3] Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz, "Hybrid Compression Encryption Technique for Securing SMS", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), pp. 473-481.
- [4] Elias Haddad and Brian King, "A Simple Secure M-Commerce Protocol SSMCP*", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007 , pp. 220-229.
- [5] Ali Grami and Bernadette H. Schell King, "Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges", Second Annual Conference on Privacy, Security and Trust, October 13-15, 2004, Wu Centre, University of New Brunswick, Fredericton, New Brunswick, Canada (2004).
- [6] Scarlet Schwiederski-Grosche, Heiko Knospe, "Secure m-commerce", it.iitb.ac.in.
- [7] Manoj V. Bramhe presented a paper "SMS BASED SECURE MOBILE BANKING", Manoj V, Bramhe / International Journal of Engineering and Technology Vol.3 (6), 2011, 472-479.
- [8] Seema Nambiar, Chang-Tien Lu and Lily R. Liang, "Analysis of Payment Transaction Security in Mobile Commerce", IEEE International Conference, 8-10 Nov. 2004.
- [9] Kwok-Yan Lam, Siu-Leung Chung, Ming Gua, Jia-Guang Sun, "Lightweight security for mobile commerce transactions", www.sciencedirect.com/science/article/pii/S0140366403001889
- [10] Sonal Gupta, "EMCV: Enhancing the Security of the Mobile Commerce using Voice Features ", IJCA Journal, Volume 44-Number 16, 2012.
- [11] Monika Agrawal, Pradip Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", IJCSSE, Vol. 4 No.05 May 2012.
- [12] Mercy W. Buku and Michael W. Meredith, "SAFARICOM AND M-PESA IN KENYA: FINANCIAL INCLUSION AND FINANCIAL INTEGRITY", Washington Journal of Law, Technology & Arts, Volume 8, Issue 3, Mobile Money Symposium 2013.
- [13] V. Devadevan, "Mobile Banking in India-Issues & Challenges", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013
- [14] Mukesh Sadana, George Mugweru, Joyce Murithi, David Cracknell and Graham A.N. Wright, "MicroSave Briefing Note # 94 Riding the M-PESA Rails: Advantages & Disadvantages" May 2011.
- [15] "Mobile Payment in Budapest Taxis", www.cellum.com/pdf/Case_Study-Taxi-EN.pdf
- [16] https://mobile.onlinesbi.com
- [17] http://www.icicibank.com/mobile-banking/index.html#
- [18] "Payment Systems in India: Reflections on some recent trends and future challenges", http://www.rbi.org.in/scripts/BS_SpeechesView.aspx?id=839
- [19] http://www.hdfcbank.com/personal/ways-to-bank/bank-with-your-phone/mobilebanking
- [20] http://www.airtel.in/money/index.html#
- [21] Ashok Kumar Nanda, Prof. Lalit Kumar Awasthi, "SMS Security Using NTRU Cryptosystem for M-Commerce", Vegas International Academic Conference as Vegas, Nevada USA, 2011, p 297.
- [22] Niels Christian Jul and Niels Jorgensen presented a paper "Security Issues in Mobile Commerce using WAP" 15th Bled Electronic Commerce Conference-Reality: Constructing the e-EconomyBled, Slovenia, June 17 - 19, 2002 .
- [23] http://www.geocities.ws/nelam21582/#overview
- [24] Nina Godbole, Sunit Belapure, Cyber Security", Wiley India, New Delhi.
- [25] www.wikipedia.org
- [26] www.google.com