M-Wallet: An SMS based payment system

Nitika Rai*, Anurag Ashok**, Janhvi Chakraborty**, Prajakta Arolker**, Saumeel Gajera**

*(Associate Professor, Department of Information Technology, St. Francis Institute of Technology, Mumbai-103
Email: nitika75@yahoo.com)
** (Student, Department of Information Technology, St. Francis Institute of Technology, Mumbai-103
Email: anurag16890@gmail.com, janhvi800@gmail.com, prajakta1990@gmail.com, saumeel2007@gmail.com)

ABSTRACT

This paper describes an efficient alternative to the traditional and current payment systems. With the advent of m-commerce, the payment systems are also being moved to the mobile devices. The current mobile payment systems are generally tied to a network provider or work only on smart phones. The transaction usually takes place via a mobile app and a GPRS / Wi-Fi connection may be required. M-Wallet is an alternative mobile based payment solution that aims at replacing the current payment solutions like credit cards; debit cards and cash with a simple Short Messaging Service (SMS) based solution that would work on all mobile phones irrespective of the network carrier and the manufacturer. Transactions can also take place between consumers that have subscribed to the service and merchants irrespective of their subscription

Keywords - **m-commerce, m-payment,**

I. INTRODUCTION

Electronic payment systems [1] like credit and debit cards are an attractive alternative from the perspective of cost and convenience. However, the security of credit and debit cards depends upon the ability of the merchant to authenticate the card by comparing signatures and the ability and honesty of the merchant in protection of the sensitive information required for carrying out the transaction. The new trend in electronic payments is mobile payment schemes – those in which at least one part of the transaction is carried out using a mobile device.

The number of mobile phones in use far exceeds any other technical devices that could be used to market, sell, produce, or deliver products and services to consumers. Mobile commerce especially mobile banking is popular in countries where most of their population is unbanked. By 2012, it is estimated that there will be 1.7 billion people with a mobile phone but not a bank account [2]. Mobile payment is being adopted all over the world in different ways. Combined market for all types of mobile payments is expected to reach more than $600B globally by 2013, [3] which will be the double of the current figure, [4] while mobile payment market for goods and services excluding contact less NFC transactions and money transfers is expected to exceed $300B globally by 2013. [5] Some mobile payment solutions are also used in developing countries for micro payments. [6]

The current emerging mobile payment services are Google wallet, Nokia's mobile money and the Interbank Mobile Payment Service (IMPS) with the latter two prevalent in India. Google Wallet works via near-field communication (NFC) which means it requires a NFC-enabled phone in order to use the service. Nokia India Pvt. Ltd. has launched Mobile Money service in partnership with Union Bank of India and Yes Bank. But this service works only on handsets manufactured by Nokia. Interbank Mobile Payment Service (IMPS) is a pilot service that allows transfer of money between bank accounts of registered users in the participating banks. But the transactions are carried out with simple PIN based security that can be easily defeated by replay attacks or mobile number spoofing. [7]

M-Wallet provides a mobile payment system that will be available on all mobile devices that support basic features like text messaging, yet be secure from spoofing of mobile numbers and replay attacks. M-Wallet transactions are totally based on text messages and provide mobile apps only for added convenience. A user specified PIN allows

only authorized access. Mobile number spoofing and replay attacks is eliminated as each transaction is protected with a unique one time key sent to the user's registered mobile number.

II. HEADINGS

A. Entities

An M-Wallet mobile payment involves the participation of a consumer, merchant and the M-Wallet system. It also includes the provision of M-Wallet outlet for recharge transactions. In the payment scenario, the consumer intends to pay the merchant electronically through the M-Wallet system. In recharge transactions, the consumer wishes to add funds to his M-Wallet account by using the services of the M-Wallet outlet.

A consumer is a registered user of the M-Wallet system and intends to use it to pay for a service or product bought from a merchant. A merchant, depending on whether digital content or physical goods and services being purchased is someone or some organization that sells products to the consumer and is the intended recipient of the funds. The M-Wallet system is the entity responsible for the execution of the payment process. It controls the flow of transaction between the mobile consumer and the merchant. The M-Wallet outlet is a point wherein a user can add funds to his/her virtual M-Wallet account by paying the required amount.

B. Registration

A user can register for this service by sending an SMS to the M-Wallet system using his mobile number which is verified and this mobile number acts as a unique ID for the user. A unique pin is generated and sent to the user which can be later changed by the user for additional security. The M-Wallet then creates a virtual account for the user with zero initial balance. According to RBI guidelines an open prepaid payment instrument requires fulfillment of Know your customer (KYC) norms. The account is fully activated only when the KYC documents are submitted at an M-Wallet outlet.

C. Transactions

The transactions that take place in the M-Wallet system are recharge, withdrawals, payments and recurring payments. A recharge transaction takes place when a user adds funds into his M-Wallet account through an outlet of the M-Wallet system or a bank using National Electronic Funds Transfer (NEFT). A user can withdraw funds from his M-Wallet account to his bank by sending a withdrawal request which is processed by the M-Wallet system through NEFT. Also withdrawal is available at M-Wallet outlets for users who cannot avail banking services. A payment transaction is consumer initiated. The payment process verifies the consumer and gathers details of the payment from the consumer and processes it accordingly. Recurring payments automate the process of payment transactions that have to be executed according to schedule.

D. Recharge:

The virtual account needs to be recharged before it can be used for payments. The M-Wallet system supports two types of recharges. First one is recharge through participating outlets which can range from a pharmacy to a bakery. This is to facilitate consumers who do not have access to banking services. The outlet can recharge the accounts through their registered mobile devices by sending an SMS to the M-Wallet system containing the details of the recharge. The other mode is through a bank transfer which gives added convenience to those who have NEFT enabled bank accounts. The procedure is depicted in Fig 1.

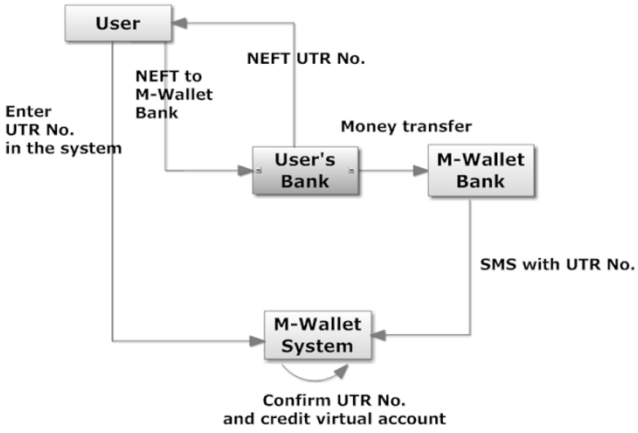

Figure 1. Recharge using NEFT.

E. Payment:

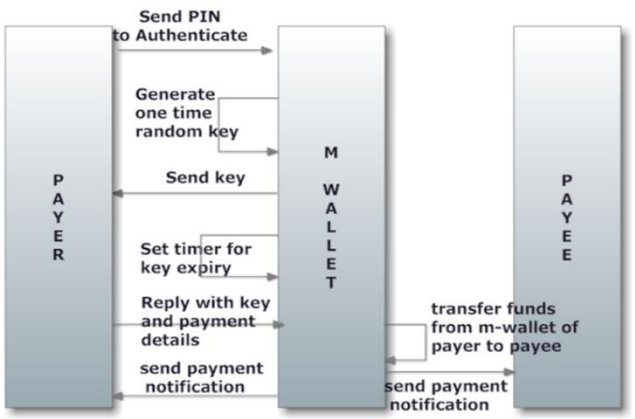

Figure 2. Payment Process.

After the consumer has recharged his virtual account he can use the funds in the account to make payment for various transactions. The payment process depicted in Fig. 2 is initialized by sending an SMS to the M-Wallet system with the PIN for the authentication. The M-Wallet system generates a one-time random key for the next transaction with a timeout and sends it to the consumer. The consumer has to reply within the timeout with the key, payment details like the mobile number of the merchant, the amount to be paid to the merchant and an optional reference text that can be used by the merchant to identify the transaction. If successful, the consumer's M-Wallet account gets debited and merchant's M-Wallet account is credited with the specified amount and confirmations along with reference text are sent to both the consumer and the merchant. The merchant is charged a percentage of the transaction amount as service fee which the merchant may pass on to the customer or bear it himself.

The merchant in payment transaction need not be an M-Wallet user. A temporary M-Wallet account is created for the merchant if he is not an M-Wallet user and this account is maintained till the user registers for M-Wallet or decides to withdraw the funds in the temporary account. The account needs to verified by using the mobile number as unique identity to withdraw the funds.

F. Redemption:

The funds in the virtual account can be redeemed for money by direct bank transfer or redemption at an M-Wallet outlet. The user can request a bank withdrawal by sending a SMS to the system. The request will be processed and payment will be made to the bank account specified. The user can also use outlet redemption to redeem funds up to a certain maximum limit. A request needs to be made for outlet redemption in advance.

G. Miscellaneous features

The M-Wallet system gives the user the facility of check his account balance by sending a SMS. Also the user can get details of all payments made and recurring payments scheduled over SMS. Flexibility in registration is provided to M-Wallet consumers where-in the consumer can update the existing M-Wallet account to the new SIM number by registering the new number using the SIM of the old number and the PIN. If at any point an M-Wallet consumer believes that his account has been compromised, he can freeze his respective account via customer service or the M-Wallet web portal or sending an SMS.

H. Reserve Bank of India Rules and regulations:

M-Wallet falls into the category of Open System Prepaid Payment Instruments in Reserve Bank of India's (RBI) draft for Draft Guidelines for issuance and operation of Prepaid Payment Instruments in India. [8]. These payment instruments can be used for purchase of goods and services and also permit cash withdrawal. According to the guidelines a mobile prepaid system like M-Wallet can be implemented by any bank which has which have been permitted to provide Mobile Banking Transactions by the Reserve Bank of India. The guidelines on Know Your Customer/Anti-Money Laundering/Combating Financing of Terrorism guidelines issued by the Reserve Bank of India to banks, from time to time also apply to prepaid payment instruments. Hence M-Wallet requires fulfillment of Know Your Customer norms. It also states that all prepaid payment instruments issuers shall disclose all important terms and conditions in clear and simple language. The outstanding balances of M-Wallet shall be part of the net demand and time liabilities of the bank for the purpose of maintenance of reserve requirements. This position will be computed on the basis of the balances appearing in the books of the bank as on the date of reporting.

I. Security

The popular standard used for mobile communication is Global System for Mobile communications (GSM. M-payment rides on the underlying infrastructure of GSM which is insecure as it does not have a provision for mutual authentication) which make way for attacks like man-in-the-middle-attack and replay attacks [9]. The default data format for SMS messages is plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable. Therefore a more secure algorithm is needed. The SMS security mechanism relies on GSM/UMTS signaling plane security mechanism. SMS may be eavesdropped by the man-in-the-middle attack as no encryption is applied to SMS message transmission.

The first step of a payment transaction in M-Wallet is authentication by sending a PIN by SMS. The PIN is sent in plaintext and also saved in users sent items. This poses a security risk and hence the M-Wallet system provides an optional J2ME application that will encrypt the PIN before sending it to the M-Wallet system. The default java.util.Random has some weakness and hence cannot be used for generating encryption keys [9]. Hence java.security.SecureRandom is required for generating random keys. The IEEE paper on SSMS - A secure SMS messaging protocol for the m-payment systems provides an elliptic curve-based public key solution that uses public keys for the secret key establishment of a symmetric encryption. It also provides the attributes of public verification and forward secrecy. It efficiently makes the SMS messaging suitable for the m-payment applications where the security is of great concern. However J2ME may not be available on all devices and hence text SMS can also be used wherein the user is responsible for deleting his sent items. In this case the GSM layer provides confidentiality.

The mobile number of the sender can also be spoofed if a direct connection to the short message service center (SMSC) can be made. In order to eliminate this, the user is required to reply within a specified timeout period with a one time random key. This one time random key is sent to the user via SMS and hence will be received only by the authorized user on his mobile number.

J. Limitations

The M-Wallet system is vulnerable to SMS delays and loss. Loss of message will lead to a transaction failure while a delayed SMS may increase the time required for the transaction to complete. However, it is expected that this vulnerability will affect only a small number of transactions as studies indicate only 0.4% of the SMS deliveries fail due to lack of resources [10]. Also the use of delivery reports will help track the delayed and lost messages.

III. RELATED WORK

Safaricom, the leading mobile operator in Kenya, launched one of the most successful implementations of a mobile money transfer service, M-PESA. M-PESA is a SMS-based system that enables users to deposit, send, and withdraw funds using their mobile phone. Safaricom accepts deposits of cash from customers with a Safaricom cell phone SIM card and who have registered as M-PESA users. Formally, in exchange for cash deposits, Safaricom issues a commodity known as "e-float", measured in the same units as money, which is held in an account under the user's name. This account is operated and managed by M-PESA, and records the quantity of e-float owned by a customer at a given time. [11]

The choice of bearer channel used to deliver mobile money transaction receipts in an important decision in the launch of the service since it impacts usability and security. Safaricom chose to use the SIM Toolkit (STK) with SMS delivery. With STK the user has an application on the SIM card which is accessed from the phone's menu. This offers very high levels of security and usability. However M-PESA is dependent on the Safaricom network and requires a SIM change as the M-PESA application is programmed using the STK.

IV. EVALUATION

Table 1. Comparison with other E-payment systems

Parameters	**Credit and Debit Cards** **Online / Offline**	**Airtel Money / Nokia Money**	**M-Wallet**

Security	CVV and CCV	Relies on USSD which may be insecure	one time random key
Convenience	Requires credit card terminal	Registration Required	No registration or device
Time	less for offline and more for online	Fast since it uses USSD	Usually 15-20 seconds. Delays possible due to SMS
Verification process	signature on the card	PIN	PIN and one time key
Bank account	Required	Not Required / Required	Not Required
Dependence on network provider/ bank/ mobile manufactu-rer	Independent	Dependent	Independent
Ease of Use	Easy / Not Easy	Easy	Easy ,only sending and receiving of SMS
Requirement for Payee	Card terminal /merchant a/c, SSL	Registration	No requirement

V. CONCLUSION

As the costs of mobile phone technology have fallen and as the technology have been adapted to support financial services, mobile banking innovations have begun to spread across and within poor countries. The low cost and the widespread unmet demand for financial services as captured by low rates of bank access means that mobile banking has the potential to reach remote corners of the socio‐economic, as well as geographic spectrum.

This potential can be realized, through M-Wallet, the SMS based mobile payment system. M‐Wallet is an innovation that clearly dominates its money‐transfer predecessors on virtually all dimensions. It is faster, safer and network independent. It has been designed in adherence to all the guidelines laid down by the RBI.

In developing markets, M-Wallet will allow people to use financial services in a more efficient way and sometimes the only way - at more affordable costs, and can greatly improve standards of living. In developed markets, M-Wallet will be more of an extension of the existing payment infrastructure that allows people to deal with their financial needs in a timely and convenient way.

REFERENCES

[1] James F. Chen et al *Electronic payment system and method* US Patent 5590197. 31 Dec 1996.

[2] Consultative Group to Assist the Poor. *Mobile Banking: Overview*. [ONLINE] Available at: http://www.cgap.org/p/site/c/template.rc/1.11.14910/. [Accessed 06 February 12].

[3] Wirelessintelligence.com. 2008. *Deployment Tracker | Mobile Money Live*. [ONLINE] Available at: http://www.wirelessintelligence.com/mobile-money. [Accessed 06 February 12].

[4] Howard Wilcox. 2008. *Press Release: Juniper Research Forecasts Total Mobile Payments to Grow Nearly Ten Fold by 2013.* [ONLINE] Available at:http://www.juniperresearch.com/viewpressrelease.php?pr=106.[Accessed 06 February 12].

[5] Bonsoni.com. 2011. *Research shows mobile phone payment double by 2013*. [ONLINE] Available at: http://www.bonsoni.com/blog/research-shows-mobile-phone-payment-double-by-2013/. [Accessed 06 February 12].

[6] Howard Wilcox. 2008. *Press Release: Mobile Payment Transaction Values for Digital and Physical Goods to Exceed $300bn Globally Within 5 Years, According to Juniper Research.* [ONLINE] Available at:http://www.juniperresearch.com/viewpressrelease.php?id=128&pr=97. [Accessed 06 February 12].

[7] National Payments Corporation of India. 2011. *Interbank Mobile Payment Service.* [ONLINE] Available at:

http://www.npci.org.in/aboutimps.aspx. [Accessed 07 February 12].

[8] Reserve Bank of India. 2009. *Draft Guidelines for issuance and operation of Prepaid Payment Instruments in India*. [ONLINE] Available at: http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1902. [Accessed 02 February 12].

[9] Agarwal S., Khapra M., Menezes B. and Uchat N. (2007), *Security Issues in Mobile Payment Systems.*

[10] Xiaoqiao Meng, Petros Zerfos, Vidyut Samanta, Starsky, H.Y. Wong, Songwu Lu, *Analysis of the Reliability of a Nationwide Short Message Service* IEEE Infocom, May 2007

[11] International Finance Corporation (2009, March). *M-Money Channel Distribution Case – Kenya* [Online] Available at: http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool6.7.CaseStudy-M-PESAKenya+/$FILE/Tool+6.7.+Case+Study+-+M-PESA+Kenya+.pdf