Location Based Services in M-Commerce: Customer Trust and Transaction Security Issues

Archana Sharma *asharma269@rediffmail.com*
Research Scholar
Mewar University
Rajasthan, 312901, India

Vineet Kansal *director.ec@its.edu.in*
Director
ITS Engineering College
Ghaziabad, 201308, India

R. P. S. Tomar *rpstbd@gmail.com*
Director, MCA
Institute of Professional Excellence & Management
Ghaziabad, ,201010, India

Abstract

It is understood by studies that wireless data services is crucial for users to access location-based services. As in location-dependent services, the data value for a data item depends on geographical locations. In general, the Location Based Services includes the services to identify the location of a person or object like searching of the nearest Banking, Cash Machine Receiving Alerts, Location Based Advertising etc. With the rapid adoption of mobile devices as a primary interface to network of services, there is a considerable risk with respect to authentication and authorization. To guard against risk, trustworthy authentication and secure communication are essential especially in Location Based Services. The purpose of this study is to identify security risks in mobile transactions specially in location based services like mobile banking. Current mobile banking authentication is challenging and identified as a major security risk. Identify the factors why customer distrusts mobile banking. Furthermore, identifying security issues between mobile devices and mobile banking systems. Finding which approach is more suitable and secure for mobile banking transaction between customer and bank.

Keywords: Customer Trust, WAP Security, LBS, M-Commerce, Authentication.

1. INTRODUCTION

With the growth of the mobile devices market and the rapid & sustained advancement in mobile device technology, the demand for multimedia services like games, videos, music along with multimedia content has drastically increased, moreover Smart phones and Mobile Internet users are growing rapidly and India is expecting to double its base of smart phones and Mobile Internet subscribers by the end of 2015 according to Telecom Regulatory Authority of India (TRAI) report.

Year	Jan.	Feb.	March	April	May	June	July	August	Sept.	Oct.	Nov.	Dec
2002	0.28	0.35	0.41	0.28	0.29	0.35	0.36	0.49	0.37	0.53	0.72	0.8
2003	0.64	0.6	0.96	0.64	2.26	2.2	2.31	1.79	1.61	1.67	1.9	1.69

2004	**1.58**	**1.6**	**1.91**	**1.37**	**1.33**	**1.43**	**1.74**	**1.67**	**1.84**	**1.51**	**1.56**	**1.95**
2005	**1.76**	**1.67**	**0.73**	**1.46**	**1.72**	**1.98**	**2.45**	**2.74**	**2.48**	**2.9**	**3.51**	**4.46**
2006	**4.69**	**4.28**	**5.03**	**3.88**	**4.25**	**4.78**	**5.28**	**5.9**	**6.07**	**6.71**	**6.79**	**6.48**
2007	**6.81**	**6.21**	**3.53**	**6.11**	**6.57**	**7.34**	**8.06**	**8.31**	**7.79**	**8.34**	**8.32**	**8.17**
2008	**8.77**	**8.53**	**10.16**	**8.21**	**8.62**	**8.94**	**9.22**	**9.16**	**10.07**	**10.42**	**10.35**	**10.81**
2009	**15.41**	**13.82**	**15.64**	**11.9**	**11.58**	**12.04**	**14.38**	**15.08**	**14.98**	**16.67**	**17.65**	**19.1**
2010	**19.9**	**18.76**	**20.59**	**16.9**	**16.31**	**17.98**	**16.92**	**18.18**	**17.1**	**18.98**	**22.88**	**22.62**
2011	**18.99**	**20.2**	**20.21**	**15.34**	**13.35**	**11.41**	**6.67**	**7.34**	**7.9**	**7.79**	**2.97**	**9.47**
2012	**9.88**	**7.44**	**8**	**1.85**	**8.35**	**4.73**	**-20.61**	**-5.13**	**-1.74**	**-2.39**	**-13.63**	**-25.88**
2013	**0.4**	**-1.97**	**5.35**	**6.33**	**8.95**	**12.12**	**9.9**	**11.42**	**7.99**	**5.78**	**20.47**	**18.11**
2014	**7.02**	**10.05**	**1.15**	**2.95**	**2.71**	**4.77**	**3.8**	**5.6**	**5.88**	**6.28**	**1.71**	**2.14**

TABLE 1 : TRAI Report, 2014- Progressive Growth(in Millions) Monthly in Mobile Subscribers in India[1].

In particular, the reality of increased mobile penetration coupled with a changing mobile threat landscape and a fragmented mobile technology market has led to deep concerns about security and privacy risks. Mobile users are ever more concerned about the security of their data and private information on their mobile devices. In general M-Commerce is defined as any type of transaction of an economic value by using Mobile Telecommunications Network and at least one mobile device and mobile transactions include buying or selling of goods / services, transferring ownership or rights, transferring money and the positioning technologies, such as the Global Positioning System (GPS), allow companies to offer goods and services to the user specific to his current location specially in Location Based Services. Location Based Services can be, thus, offered to meet consumers' needs and wishes for localized content and services like bank services for the execution of financial services through mobile device are called Mobile Banking.

Despite the fact that M-Commerce is getting a great deal of global attention, mobile consumers are coping with some difficulties to engage in this new type of commerce. In Mobile Banking, trust is considered to be the most important factor. The reason is that the transaction of money is occurring online. Trustworthiness is the belief that the business partner can be trusted and will act according to the business rules. Acceptance of Technology and willingness of transacting money depends upon the customer trust. Customers lack in trust on mobile banking because of some issues in its process like cost, security, convenience of customer in adopting mobile banking etc.

2. FACTORS AFFECTING THE ADOPTABILITY OF M-COMMERCE

As number of drivers are engaged in M-Commerce payment services and providing mobile payment solutions through their services. Still most of the M-Commerce services in India are still relatively in the piloting phase. However, the M-Commerce adoptability challenges can be classified into four major issues which dramatically affect the mobile transaction adoptability such as:

Regulatory factor	**:**	RBI guidelines for prepaid devices
Socio-cultural factor	**:**	Customer trust issues
Technology factors	**:**	Security issue and network complications
User Convenience	**:**	Satisfaction, user interface, interoperability

This research major focus on the customer trust and security issues due to different technology standards. Though customer can get details about account, transfer money to account etc. and the interact with the database of the bank, thus data at mobile device with customer and as on database at the server must be secured. Thus, security is an important issue for the customer trust.

To transfer money or for making any transactions customer distrust the mobile device for this purpose. The security is a major concern for the customer's satisfaction. Customer's main concern in using mobile devices for mobile banking is the authentication method used to ensure that the right person is accessing the services like transaction etc. A third party payment gateway is involved in this mobile payment scheme; they give service between two or more banks so the customers need to trust on unknown third-party payment gateway and also need to pay an extra service charge.

3. ANALYSIS OF FACTORS AFFECTING THE DISTRUST IN ADOPTABILITY OF M-COMMERCE

In Location Based M-Commerce services especially in Mobile Banking, the service provider provides services to mobile users like their locations with a certain level of granularity to maintain a degree of secrecy. Some factors affect the adoptability of M-Commerce in Location Based Services according to the Mobile user.

FACTORS OF DISTRUST	**REASONS**
Reliability	Frequent network disconnection increases the communication time and the communication cost. Most of the time due to network slow speed, transaction may incomplete.
Security	In case of message lost, transaction will fail. There is no encryption applied at SMS, so hacker can hack the contents of SMS message.
Customer Satisfaction	Due to reliability and security dissatisfaction, mobile customer prefer the internet banking and don't use the mobile banking to transfer the money.
Fraud	Although the mobile banking services are improving still there are number of frauds occur. Thus there is need of secure system to minimize the fraud chances.

TABLE 2: Factors of distrust of M-Commerce.

With the above analysis of Mobile customer dissatisfaction of M-Commerce especially Mobile Banking, it has been observed that transaction security and network technology for mobile transaction are the two main issues in M-Commerce. As the Security includes, Data transmission which should be securing so that no hacker should be able to hack the data, for this purpose a secure connection is needed where authentication and authorization are two important aspects. Authentication means only authorized persons are allowed to access the data and authorization means it should be simple and fast so that quick access should be available for the data.

4. AUTHENTICATION PROCESS

Under authentication process, it identifies a particular device allowed to use for their services. Thus it is an important factor for accessing Mobile Location Based Services as trustful and secure service as security and privacy are especially important for mobile device.

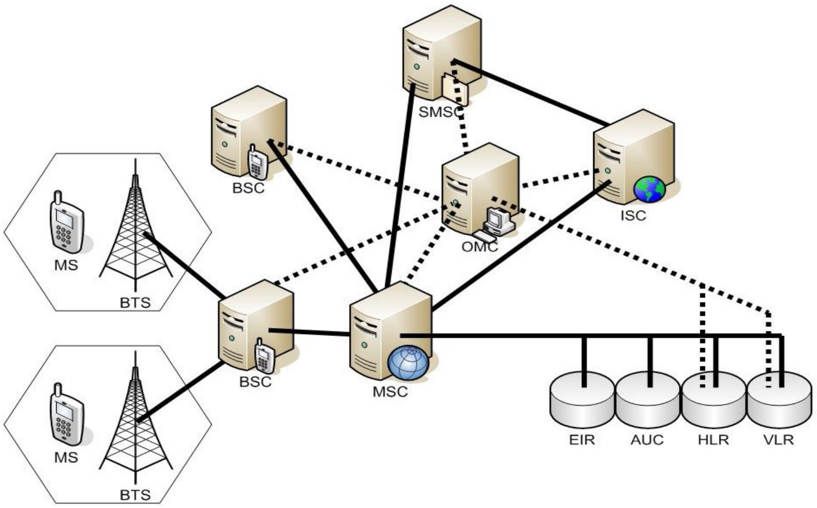

FIGURE 1: GSM Architecture.

As technology developed GSM and cell phones became more and more popular and more services were provided, such as SMS, Wireless Application Protocols, HSCSD, and GPRS.

GSM is responsible for the security of the Mobile Station when linked to a network [2][3].

i. IMSI confidentiality.
ii. IMSI data confidentiality on physical connections.
iii. Connectionless user data confidentiality.
iv.Signaling information element confidentiality.

Here the Home Location Register is the database for subscriber parameters like Subscriber ID (IMSI and MSISDN), current subscriber VLR i.e Current location, current forwarding number, subscriber status, authentication key and its functionality and the master database of all subscribers in GSM system. Thus the HLR maintains the database of Mobile Subscriber and generates and stores authentication information for mobile subscriber. The authentication process in general secure data stored on the SIM card is calculated and compared with the data field in HLR database. A random number is sent to the mobile from the AUC. This number is calculated together authentication key (KI) stored in SIM card by authentication algorithm, which is held in SIM card. The full authentication process takes place as the first time a subscriber attempts to make a call. However, for subsequent calls attempted within a given system control time period, or within a single system provider's network, authentication may still be available. When a subscriber changes its location and comes in roaming, meaning changing of VLR (Visitor Location Register) due to mobility, the new serving VLR fetches some information about the subscriber from HLR and old VLR removes the entries of the mobile subscriber that changed the VLR. Thus HLR can be considered as permanent database, while the VLR is considered as temporary database.

5. SECURITY RISK AND ISSUES IN AUTHENTICATION PROCESS IN LOCATION BASED SERVICES

In general, login method is used in mobile transaction for authentication in location based services like mobile banking but many security issues such as Id theft and password theft are major challenges in this method due to secrecy reveal threats and this results in customer's distrust on the security service provider despite of following the security mechanism in the mobile transaction by identifying the customer's phone number, SIM card number, pin number etc. Although the facility of mobile banking attracts the customer due to its mobility as he can access the bank anywhere and in any situation and its services like customer can transfer his money from one account to another account faster in a user-friendly environment with checking the current status of his account, still the adoptability of mobile banking is quite less with the assumptions that the mobile banking systems brings inconvenience to the users assuming and cannot prevent direct or indirect attacks. Since SMS based mobile banking is a convenient and easy way for accessing bank , the mobile user prefer to use SMS Banking but SMS is not suitable for authentication and is susceptible to misuse including redirection, hijacking and spoofing, as in spoofing attack where attacker can send messages on network by manipulating sender's number due to insecurity of transaction, most of the organizations are not adopting mobile transaction through SMS . So lacking of privacy, integrity and security are the main issues involve in authentication process specially in case of SMS banking [4].

6. TECHNOLOGIES FOR MOBILE TRASNACTIONS

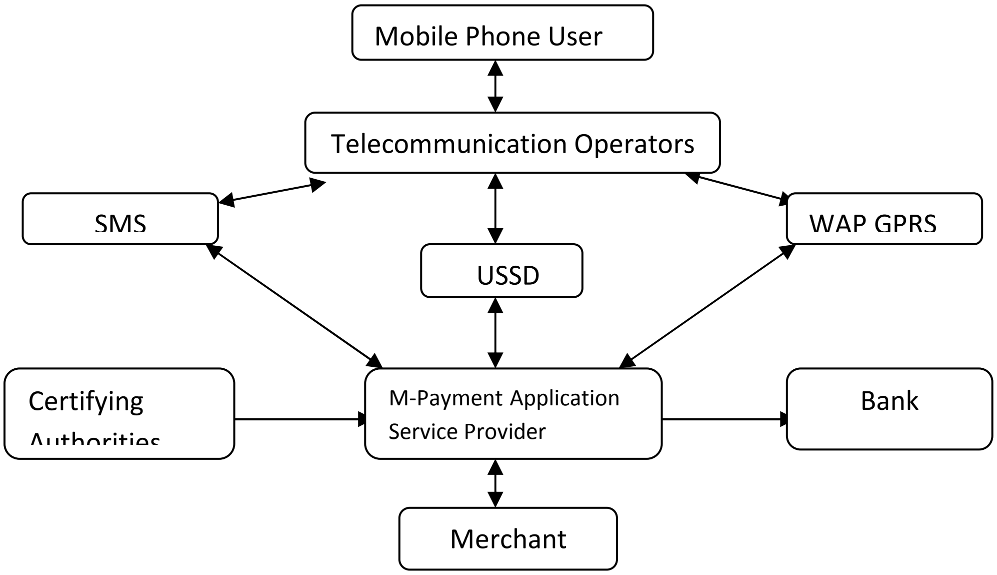

FIGURE 2: Mobile Transaction Technologies.

6.1 Short Message Service (SMS)

SMS is a text message service that enables short messages (140-160 characters) and can be transmitted from a mobile phone. These short messages are stored and forwarded by SMS centers. SMS messages have a channel of access to phone different from the voice channel [4]. SMS can be used to provide information about the status of one's account with the bank (informational) or can be used to transmit payment instructions from the phone (transactional).

6.2 Unstructured Supplementary Services Delivery (USSD)

Unstructured Supplementary Service Data (USSD) is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signaling channels of the GSM network. USSD provides session-based communication, enabling a variety of applications. USSD is session oriented transaction-oriented technology while SMS is a store-and-forward technology. Turnaround response times for interactive applications are shorter for USSD than SMS.

6.3 WAP/GPRS

General Packet Radio Service (GPRS) is a mobile data service available to GSM users. GPRS provides packet-switched data for GSM networks. GPRS enables services such as Wireless

Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access in mobile phones.

6.4 Phone-based Application (J2ME/BREW)

The client m-payment application can reside on the mobile phone of the customer. This application can be developed in Java (J2ME) for GSM mobile phones and in Binary Runtime Environment for Wireless (BREW) for CDMA mobile phones. Personalization of the phones can be done over the air (OTA).

6.5 SIM-based Application

The Subscriber Identity Module (SIM) used in GSM mobile phones is a smart card i.e., it is a small chip with processing power (intelligence) and memory. The information in the SIM can be protected using cryptographic algorithms and keys. This makes SIM applications relatively more secure than client applications that reside on the mobile phone. Also, whenever the customer acquires a new handset only the SIM card needs to be moved. If the application is placed on the phone, a new handset has to be personalized again.

6.6 Near Field Communication (NFC)

NFC is the fusion of contactless smartcard (RFID) and a mobile phone. The mobile phone can be used as a contactless card. NFC enabled phones can act as RFID tags or readers. This creates opportunity to make innovative applications especially in ticketing and couponing [5].

6.7 Comparison of medium of communication in M-Commerce Technology

S. No.	Elements	SMS Based		GPRS Based	USSD Based	NFC
		SIM Based SMS	Phone Based SMS			
1	Data Carrier	SMS	SMS	GPRS	Text Message through USSD gateway	channels
2	Data Storage	SIM Memory	Phone Memory	Not Stored	Not Stored	Linked with user mobile
3	Card present/ card not present TXN	Card Present	Card Present	Card not Present	Card not Present	Card not Present
4	User Interface	Menu based	Menu Based	Interactive	Interactive	Interactive
5	Security	Firewall	Firewall	Firewall	No security feature deployed	Firewall
6	Time parameter	Not instant	Not instant	Instant	Instant, no time gap	Instant

7	Java application based solution	No	No	Yes	No	Yes

TABLE 3: Comparison of M –Commerce Technology.

7. MOBILE TRANSACTION SECURITY

Mobile payment, a major component of M-Commerce, is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services. Comparing to E-commerce, mobile payment has particular security and privacy challenges due to the differences between their underlying technologies. The major difference is that the transport of payment involves wireless service providers. The ability to address the issue is a major factor affecting the customer confidence, market penetration, and long-term success of M-commerce applications.

Security is an essential consideration for mobile payment which can be challenged during sensitive payment information handling or transmission. Four properties have always been essential for secure transaction, including authentication, confidentiality, integrity, and non-repudiation[6].

Authentication: Authentication is concerned about verifying the identities of parties in a communication and confirming that they are who they claim to be.

Confidentiality: Confidentiality is about ensuring that only the sender and intended recipient of a message can read its content.

Integrity: Integrity is concerned about ensuring the content of the messages and transactions not being altered, whether accidentally or maliciously.

Non-Repudiation: Non-Repudiation is about providing mechanisms to guarantee that a party involved in a transaction cannot falsely claim later that she did not participate in that transaction.

7.1 Location Based Mobile Financial Transaction Security Issues

A mobile user is more likely to need the location information when roaming under another provider whose network may or not may not have the same location performance, further, it needs to add more issues like privacy and security issues, ownership of location information, service interoperability, vendor support. This potentially makes certain mobile users vulnerable to security and privacy issues. Mobile financial transaction requires a strong level of security support. In location based mobile financial transactions, in general mobile user uses SMS and WAP based banking services.

7.1.1 SMS Banking

In SMS banking, mobile user can find out the details about their account balance and will get their desired data. Despite of few features like simple, convenient, cost efficient and fast exchange of messages, the challenges that are to be overcome for wide acceptance of SMS based payment transaction[6], as there is no encryption technique can be applied for sending and receiving SMS, the data are not secure while transmitting through SMS.

Short Message Service is a store and forward service where 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[7].

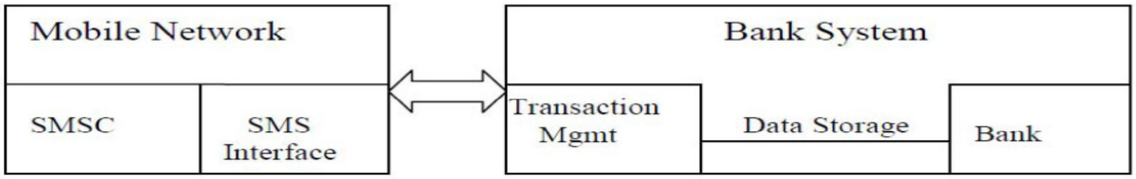

FIGURE 3: Organization of network elements in a GSM network supporting SMS.

The benefits of SMS to mobile users integration of messaging services and data access, delivery of notifications and alerts, guaranteed message deliver, reliable, low-cost communication mechanism, which increases the mobile user productivity.

The SMSC (Short Message Service Centre) job's to store and forward of messages to and from the mobile station. The SME (Short Message Entity), in general is a mobile phone or a GSM modem, which can be located in the fixed network or a mobile station, SMSC usually has a configurable time limit for how long it will store the message. 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 [8].

7.1.1.2 Security Challenges in SMS Banking Transactions

In general, initially in GSM network architecture, mutual authentication, text encryption, end to end security, no repudiation were omitted and SMS usage was intended for the mobile users [9]. 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. Beside this implementing complex cryptography is difficult, hacker can get password from the stolen device.

7.1.2 WAP Based Mobile Transactions

WAP is daily need of mobile users. Using WAP it's easy to mobile users to access internet and other networking services through mobile. It gives anyone access to an indefinite amount of information at any time and is expandable. But it is uncertain i.e. if connected then we can use it. WAP enables wireless communication and M-Commerce where Internet data moves to and from wireless devices like digital mobile phones, internet, PDA etc. WAP-enabled phones can access interactive services such as information, location-based services, corporate information and interactive entertainment and supports Bluetooth enabled mobiles. Through WAP mobile customer can realize more functionality of internet banking. Encryption process is currently used for secure data transmission between bank and users but the problem is that this encryption process is not good enough for the protection of sensitive data between bank and customer. If we take internet banking it is realized that there are powerful computer systems and well defined complex encryption process to ensure the security. Mobile device have low computational capacity and hence are unable to apply complex cryptographic system [10].

Indian Bank offers "WAP Based Mobile Banking" to mobile customers who have GPRS enabled facility on their mobile handset. The mobile customer can access their account details through WAP based mobile banking. WAP Mobile Banking offers various account related enquires, transfer of funds (Intra-bank & Inter-bank through NEFT) at customers' convenience at 24 x 7 basis. The WAP Mobile Banking is secured through login password (MPIN) and OTT (as two-factor authentication) for funds transfers. The present mobile banking implementations that are using WAP have proven to be very secure, but there exist some loopholes which could lead to insecure communications. Some of these loopholes include: There is no end-to-end encryption between client and bank server. There is end-to-end to encryption between the client and the Gateway and between the Gateway and the Bank Server.

7.1.2.1 Security Challenges using WAP in Mobile Banking Transactions

The end to end security is necessary requirement of current mobile transaction. It means that if user uses his/her mobile device for mobile banking then the data transacted are secure at the bank end and not at the user end, thus leaving the data vulnerable to attacks. Through WAP it is some time difficult to provide end to end security. The reason is that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile banking in WAP [11]. WAP is vulnerable to hacker's attacks due to its protocol translation and compression of contents which is insecure.

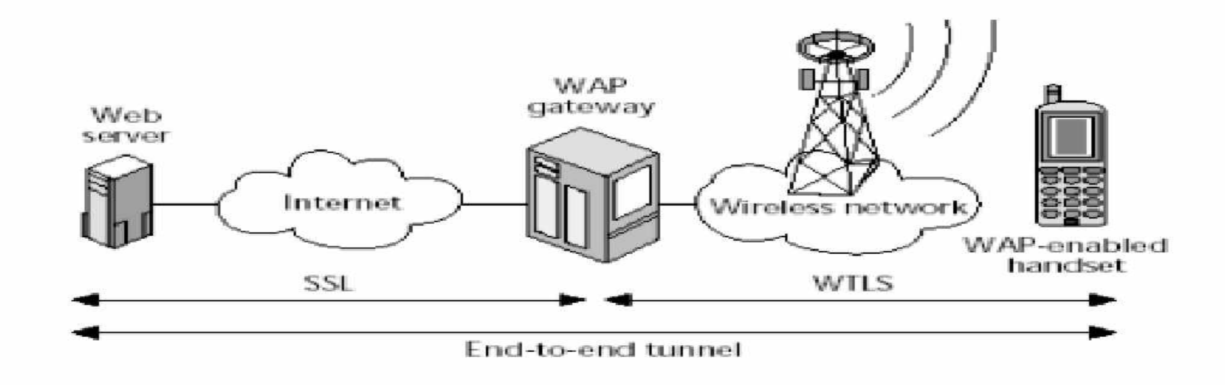

FIGURE 4: Wireless Application Security Model.

WAP security functional area includes Wireless Transport Layer Security (WTLS), Wireless Identity Module, WAP Public Key Infrastructure, WML Script sign Text, and End-to-End Transport Layer Security. The WTLS (Wireless Transport Layer Security) protocol is a PKI-enabled security protocol, designed for securing communications and transactions over wireless networks. It is used with the WAP transport protocols to provide security on the transport layer between the WAP client in the mobile device and the WAP server in the WAP gateway. The WTLS protocol services are authentication, confidentiality and integrity. It provides functionality similar to the Internet transport layer security systems TLS (Transport Layer Security) and SSL (Secure Sockets Layer), and has been largely based on TLS. WTLS is implemented in major micro-browsers and WAP servers. In case of WAP model, all the applications and contents are specified in a well-known format which is based on World Wide Web (www). Data transportation is done by using some standard of www communication protocols.

Despite of security support added at middle ware such as WAP, end – end security is still a problem. For financial application, wireless PKI a system to manage key and certificates, can be used to authenticate and obtain digital signature from mobile users. But failure of a wireless infrastructure will greatly affect the M- transaction failure of HLR/VLR that stores approximately location of mobile user ill affect the location based mobile transaction

Security Risk at WAP:

- Attacker can access unencrypted access
- During switching of protocol process at gateway the data is not in encypted form
- Eavesdropping Attack
- Man in Middle Attack
- Malicious Software

Security Risk at Server

- Server Failure
- System Crash
- Virus Attack

8. SECURE M-COMMERCE CHALLENGES

When people use mobile commerce, their information must be transmitted through mobile Internet, including the customers' private information, the order information, and the payment information and so on. All these information should be kept secret for other people. Therefore in M- Commerce, the security transmission of the data and information is the important guarantee of safe mobile commerce. Security requirements in M-Commerce generally should include the following several aspects, each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network Access Security (I):** The set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link.
- **Network Domain Security (II):** The set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wire line network.
- **User domain security (III):** The set of security features that secure access to mobile stations.
- **Application domain security (IV):** The set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** The set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use.

9. CONCLUSION

This paper mainly focused the security issues related to the customer distrust in Mobile Transactions based on Location Based Services, especially in mobile financial transactions like SMS banking transactions and WAP Based transactions including the authentication process and its security aspects in mobile transactions. Mobile customers are required security before access the mobile transactions. Though, normally customer is not knowledgeable about the Technology whatsoever is being provided to him but initially it explained the various mobile technologies and analysis of these technologies. Based on the analysis above, it is considered that mobile and related security technology can provide the needed security capability to protect mobile transactions and services, despite of that the end-end security threats and attacks are possible. Mobile Service Providers are to ensure the customer about the secure technology. Due to various technology standards interoperability among the application, devices also affect the conveniency to adopt the M – Commerce. Thus ease of use, should be taken into account when evaluating the applicability of M-Commerce and security technologies for mobile transaction.

10. REFERENCES

[1] http://en.wikipedia.org/wiki/Telecommunications_statistics_in_India

[2] D.Yang, H. Wang, Y. Ren, J. Wang, "Mobile Payment Pattern Based on Multiple Trusted Platforms - China Case" in Proc. Mobile Business and Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference, 2010, pp. 353-362.

[3] P. Soni, "Payment Between Banks Using SMS [Point of View]" in Proc. IEEE, vol. 98, 2010, pp. 903-905.

[4] S. Alam, H. Kabir, M. Sakib, A. Sazzad, C. Shahnaz, and S. Fattah, "A secured electronic transaction scheme for mobile banking in Proc. Bangladesh incorporating digital watermarking,Information Theory and Information Security (ICITIS), IEEE, 2010, pp. 98-102.

[5] J.Ondrus & Y. Pigneur, “An Assessment of NFC for Future Mobile Payment Systems.” in Proc. Management of Mobile Business, 2007 , pp. 43 - 53

[6] N.-J. Park , Y.-J. Song, "M-Commerce security platform based on WTLS and J2ME," ISIE 2001. IEEE International Symposium on, 2001.

[7] S. Basudeo, K.Jasmine, “ Comparative Study on Various Methods and types of mobile payment system” in Proc. International Conference on Advances in Mobile Network, Communication and Its Applications,India 2012, pp.10.

[8] Vahid, R., & Habibi, J. “MPaySmart: A Customer Centric Approach in Offering Efficient Mobile Payment Services” in Proc. Asia-Pacific Services Computing,Taiwan: IEEE, 2010.

[9] Manoj V, Bramhe (2011) International Journal of Engineering and Technology Vol.3 (6), pp. 472-479, ISSN : 0975-4024

[10] Jin Nie and Xianling Hu, “Mobile Banking Information Security and Protection Methods” in Proc. Computer Science and Software Engineering International Conference, pp. 587-590.

[11] C. Narendiran, S. Albert Rabara, and N. Rajendran, —Public key infrastructure for mobile banking security,‖ Global Mobile Congress 2009, 2009, pp. 1-6.