Security Issues in M-Commerce for Online Transaction

Deepak Kumar[1], Nivesh Goyal[2]

[1,2]*Amity Institute of Information Technology Amity University Uttar Pradesh, Noida, India*
[1]*deepakgupta_du@rediffmail.com*
[2]*nishugoyal35@yaho.com*

Abstract: **M-commerce is defined as carrying a business or a service on an internet-enabled mobile based application for making a transaction over the mobile devices for any monetary value. It can be used for buying product online, paying bills, sending money to someone, booking accommodation, getting your favorite dishes from nearby restaurants, etc. Today all our devices are connected through the internet and mobile phones. It has become necessity for all the humans in todays world. This paper undertakes a thorough examination of the security issues involved in the field of M-commerce. Due to the transaction over the internet, M-Commerce creates more security concerns than the traditional E-Commerce. In this paper, security measures in M-Commerce, wireless security, and the application of key generation, authentication and SSL Layer and its issue while making transactions will be discussed. Issues in online transaction are also being discusses in M-Commerce.**

Keywords: **Mobile, security, E-commerce, M-commerce, Authentication**

I. INTRODUCTION

E-commerce security involves wider ranges like data security, computer security, and other related forms of information security framework. E-commerce includes providing security to users for daily business transaction. In the present day, security and privacy is major concern in E-Commerce as well as M-Commerce and as well as in other technologies [1]. M-commerce is defined as conducting business or a service on an internet-enabled mobile based application by making a transaction over the mobile devices using any monetary value. The transactions can be carried out from fixed locations at anywhere at any given time. With growing technologies, M-Commerce today has widespread usages. In present, Mobile phones are going to be looked upon as a mode of payment mechanism with the help of communication device. Mobile phones have replaced paper money and even credit cards. M-commerce includes: purchases on mobile web and apps, mobile payments, mobile gaming, mobile money transfers, m-banking, and mobile financial services. But beyond the positivity of M-Commerce, it poses serious security issues. Customers have many concerns like privacy and security. We cannot neglect customer's primary issue.

That is the reason e-commerce security providers keep improving their security from time to time. Currently development in PDA, wireless communication technology and enveloping infrastructure promise to provide better alternatives.[2].M-Commerce makes people's lives comfortable and provides the security to the user. M-Commerce hada shift from 2G to 4G. 4G provides a wider array of abilities besides basic voice communication, such as multimedia transfer and streaming, video conference, and complete connection to the web.

In this paper we have discussed about the SSL Layer also discuss the online transaction security. This paper has been arranged in the following sections. Section II presents the headlights the issues in online transaction for E-Commerce. Section III depicts the concerns regarding M-Commerce Security Concerns. In Section IV, Secure Online Transaction has been reviewed. In Section V, Online transactions have been reviewed defining the problem faced with SSL Layer. Section VI, compares the Transaction with and without SSL Layer through a Case Study on PayTM. Finally the paper has been concluded.

II. ISSUES IN ONLINE TRANSACTION FOR E-COMMERCE

E-commerce provides security in online transaction so that unauthorized person cannot access and modify the data. E-commerce security provider does not provide complete security, we need to improve and implement a completely secure system. Some of security features are as follow:-

A. Authentication

In authentication, username and password of the user are matches with entries in the database and if the detail matches then he is authenticated as a genuine user and is given the rights to access the information. Authentication is a process of giving the authority to the individual to change the information according to the situation. It verifies that the person is an authentic user and wishes to access his account and only once the authentication is approved the system lets the user to login.

B. Authorization

After authentication, the person can make the necessary changes to the data. Authentication and authorization goes parallel. If you have the authentic username and password,

then you are an authorized person and are allowed to make the essential modifications with the data.

C. Encryption

Encryption provides the means of securing the information using an encryption key in order to protect the confidentiality of the individual. Using this technique the data is encoded into an encrypted form and only an authentic person having the decryption key is able to access the secured information.

III. M-COMMERCE SECURITY CONCERNS

Main concerns of M-Commerce is the security aspect in wireless communication. Visa was among the first in the field of m-commerce to implement payment verification. Visa allows cardholders to authorize the payment in real time and makes sure that payment information sent over the network system cannot be accessed, thus enabling users to secure their visa a/c by not all owing illegal use. It helps the users by securing inter-operability when accessing the world-wide web, which is the network of networks, without directly taking care of the equipment or technology to be used and without a robust and complete knowledge. It has simply three security requirements:-

A. Confidentiality

Today data is one of the major assets for any organization. To make it secure and confidential, we need to keep information safe from unauthorized access, for example, any personal information, bank account, government documents, credit card numbers etc. For privacy reasons, we need to keep data safe and secure.

B. Integrity

Data Integrity is used to save information from being modified by unauthorized users. Data has value only if it is correct. If data is altered, it might lead to heavy losses. For example, if our account information is tampered with while transferring money to another account, the money might be lost into unknown accounts.

C. Availability

A user authorized can access data only when data is available. Data holds value only if the right user can access at the correct time. Hence, to access data, the user needs to have permission to avail the data.

A. Features of M-Commerce

Following are some unique features of M-commerce.

- **Ubiquity:** Mobile devices provide customers the added ability to hold info and allow to perform the transaction from any remote location. M-commerce users are widely spread, with the similar level of access as is presented over the fixed-line technology. This exchange of info is independent of user's site.
- **Localization:** Internet makes M-commerce more beneficial instead of the wired e-commerce. Using the location available through the GPS technology, we can easily find the location of any user. Also, through m-commerce, data can be easily sent and received at any location.
- **Proactive functionality:** This feature ensures that the information can be shared immediately at the time of requirement. Just like 'opt-in' marketing, users may choose the given offers at any time they like.
- **Personalization:** Generally, only a single person uses a mobile device. Mobile devices take advantage of sending and receiving message, based upon the time and address, we can also manage sound and sight. Latest advances in data-mining and Info Tech make altering conversations to separate users pragmatic and cheap.

Fig. 1. M-Commerce Security Concern

IV. SECURE ONLINE TRANSACTION

A. Cyber Security

Cyber security is an important topic now a days. In currently, cyber security is one of the major issues for national security. Customer's trust and security is also a prime concern for any company in 21th century. Some of the other mechanisms are authentication, authorization, integrity, confidentiality, availability, non-repudiation and privacy [6].

B. Transaction Authentication Number (TAN)

Online banking services use transaction authentication number in the form of OTP to authenticate monetary transaction. TAN enhances the additional security because it provides the two way authentication. Any transaction cannot be done without having a valid TAN if the login information is obtained, no

transactions can be done and if we lose token or document; it is rendered incapacitated without the password.

C. Wireless Application Protocol

Wireless application protocol is an open, global specification that authorizes mobile users with wireless devices to simply access and interacts with the services and information directly. Only solution to wireless communication is WAP. WAP also allows M-commerce to share information via wireless devices and also provides functionality to the user. They can access any information from any place.

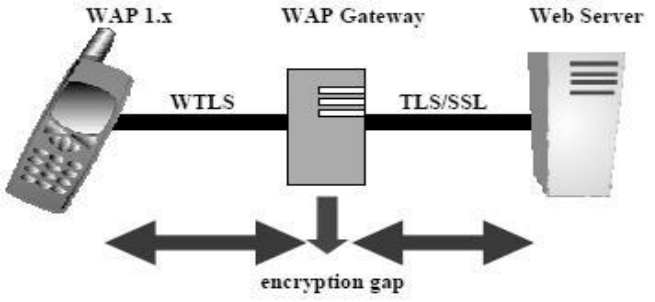

Fig. 2. Wireless Application Protocol Security

D. Mobile Transaction Authentication Number (MTAN)

Bank's of many countries uses MTAN, first time when a user do the transaction then banks generates TAN and send to user cellular phone via SMS. SMS may include transfer details and allow user to validate that transaction is not modifying by other person and bank. The main objective of this is to provide the security to mobile transaction.

V. SSL LAYER

SSL helps to establish a link of encrypted form between a web server and browser. SSL is also called as slandered security layer. SSL makes sure that the information transferred between the web server and the web browser will be always secure and integral. Netscape Inc officially applies SSL protocol. Due to its acceptance and popularity, it is now applied on all web browsers.SSL have two key objectives:

- It provides and ensure privacy, by encrypting the information that runs among the communicate party (the server and client).
- It also provides validation of the session partners, including RSA algorithm. Secure Socket Layer includes two protocols:

  *1)*The SSL Handshake protocol, that is include the communicating between the server and client verify them and bargain an encryption key. Now we have remembered one thing that in SSL there is a overhead in starting up a SSL session.

  2) Verifies protocol, in which communicate with the server and client and exchange their data within encrypted trend.

Old network protocol is benefited by SSL because it is easy to lucent and integrity services of TCP protocol.

It's also authenticating services and important users can submit, if they are talking server, and not few invited spoofing to the server.

Fig. 3. SSL Layer

In present, SSL is used generally to set up security protocol. For the security reason behind secure HTTP, it is responsible for small lock in web browser.SSL works on TCP and their main objective is to secure many protocols. A SSL starts with the handshake for transaction of costumer server. It send it's credentials for server's reply. Credentials could be like user_ID and password server authenticate when they get correct user_ID and password. Credentials is part of information that include a public key conjoined to the server and other important bits, such as the holder of the license, its expiry, and the domain name along with the server.

When a browser try to create a connection to the secured website by means of SSL, the browser and the web server make an SSL connection using a secretive method called an "SSL Handshake". Three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa.

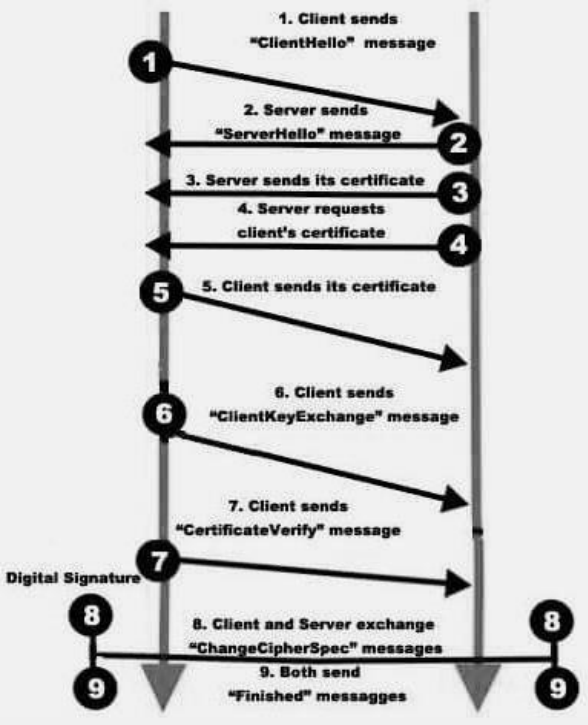

Fig. 4. SSL Handshaking

After the secure connection is made, the session key is used to encrypt all transmitted data[10].

Browser generates a certificate signing request (CSR) when connected with the SSL secured web server, then servers sends the copy of its SSL certificate with its public key.

Browser verifies the origin of the certification in the database of reliable CA (Certificate Authority) and that the certificate is valid, genuine, and that its common name is valid for the website that it is making the connection to. If the browser allows and verifies the same, it makes, encrypts, and sends a symmetric session key back to the system using the server's public key.

The server then proceeds to decrypt the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

Server and Browser now encrypt all transmitted data with the session key.

A. Online Transaction Problem with SSL Layer

SSL is an effective protocol. If someone knows it and uses it well then they can easily misuse it. Many difficulties arise while deploying SSL, but with a little bit of effort, many of them can be avoided.

- The genuine cardholder is not known to the seller. In case the customer makes a transaction using the robber card details the shipper is responsible to introduce exchange charge backs. These testaments are not necessary and are rarely adopted while the opportunity of customers check using customers exchange and provided by SSL/TLS[6].
- Only the communication connection between the vendors and the client is defended by the SSL. The vendors are approved to see the imbursement data. SSL/TLS will not ensure that the vendor won't mistreat this data, or it is possible to safeguard it against interference while it is stored at the merchant's site.
- SSL/TLS cannot guarantee assurance of the absence of acceptance against third-party sites. So SSL protocol cannot facilitate non-repudiation.
- SSL/TLS intensely encrypts all talk information by the comparable key strength, which is do not use as the complete system wants almost range of safety.

VI. CASE STUDY ON PAYTM

A survey is conduction on PayTM IT Company that provides the online recharge facility to the customer. It provides the security to the customer using SSL Layer. PayTM is uses the SSL certificate for online transaction security. SSL Layer provides the security for end to end user. In India, many business transactions are done by the PayTM payment gateway. Table -1 summarizes the different parameter between transaction with SSL Layer and transaction without SSL Layer.

A. Transaction with SSL Layer and without SSL Layer

Table 1. Transaction with SSL Layer and without SSL layer

Parameter	Transaction with SSL Layer	Transaction without SSL Layer
Security	It provides the security between client and server. Anyone can not access your information because it generates the secret key (unique session ID and generate the public key). SSL layer uses the handshake protocol to check the users is valid or not. Handshaking is a type of messaging where a user sends the data to server and server sends it back. It also verifies the client certificate.	Lack of security because it does not make any unique id. Anyone can access information easily while transaction is being processed on internet [9][8].
	In SSL, if the user is valid then encryption is done by the secure	It does not provide any type of message

Encryption	Encryption tunnel. changes your information form. in chipper During the data transfer both side (client and server) ke exchange the secret y [9][8].	encryption. Encryption changes your information in plain form.
Performance	SSL Layer provides better performance.	It does not provide better performance.
Authentication	When the user log in the account, then his MAC address gets stored which is later verified. Digital get signature also s verified.	It checks the user name and password and does not store the MAC address of any system.
Authorization	If the user is valid, then only he can change own information.	If someone hack your account then he will be able to modify your information because it does.
		not generate any private.
WWW Application	Browser use the **HTTPS://** protocol, **s** stands for secure.	Browser normally uses the **HTTP** protocol.

B. Survey by the PayTM Online Transaction

Based on above survey,Table-2 shows comparison between transaction with SSL Layer and without SSL Layer. It also gives the rating of the survey conduction on PayTM **1 is given for Very Poor, 2 for Poor, 3 for Average, 4 for Good and 5 for Excellent.**

Table 2 Performance Table with and without using SSL Layer Transaction

Performance	Transaction with SSL Layer	Transaction without SSL Layer
Security	5	2
Encryption	5	2
Performance	4	3
Authentication	5	3
Authorization	4	2
WWW Application	4	2

C. Online Transaction Security Chart

Based on the performance Table-2, security chart is drawn for online transaction with and without SSL Layer security. It shows that transaction with SSL Layer is more secure then the without SSL Layer.

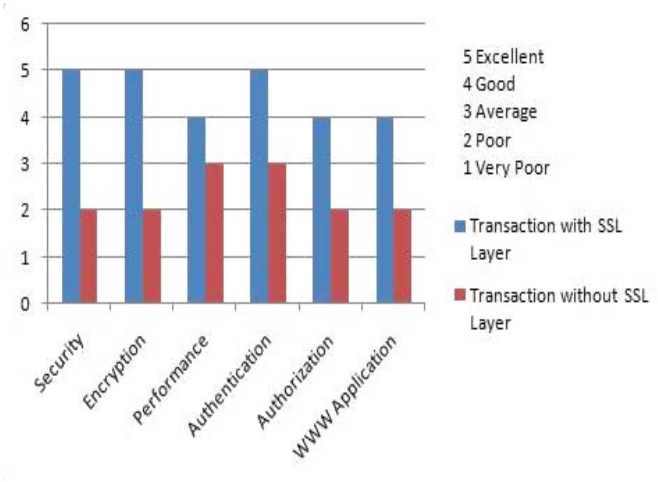

Fig. 5. Online Security Chart

VII. CONCLUSION

E-commerce is majorly used for the sale and purchase of goods using the web, but the financial exchange is carried out using electronic devices. M-commerce and E-commerce playing a crucial role in online business and customers increase day by day. M-Commerce security is extremely vital issue now in these days that wants more study to begin effective and efficient solution. In this paper, I have tried to cover safety concern for online transaction. The issue likes privacy, verification, encryption and authorization is discussed to make secure transactions over the wireless devices. Encryption only is not enough. Un-authenticated with SSL certificate gives integrity and confidentiality, but they require to third-party verification. It allows the recipient with a digital SMS to verify the authentication. Security of payment can be enhancing using the SSL Layer. This security technique is used to give safety to the client as well as the customer to in order to purchase the desired items.

REFERENCES

[1] Niranjanamurthy D. C. " The Study of E-commerce Security Issues and Solutions" International Journal of Advanced Research in Computer and Communication Engineering vol. 2, Issue 7, July 2013.

[2] Wushishi,U. J.,Ogundiya,A, O." Mobile Commerce and Security Issues" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 vol 3, Issue 4, July 2014

[3]]D. A. Montague, Essentials of Online payment Security and Fraud Prevention, John Wiley & Son, 2010, p.1-5

[4] Bajpai Anand" Impact of M-Commerce in Mobile Transaction's Security" *Research Journal of Management Sciences* ISSN 2319–1171 vol. 2(7), July (2013), 33-37

[5] Khan,M.H, Chandra,Manik "A Review: Secure Payment System for Electronic Transaction" International Journal of

Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 3, March 2012 ISSN: 2277 128X

[6] Giri Manoj, Singh Sonia" Issues in Mobile e-commerce: A survey",(IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5 (4), 2014, 5068-5070

[7] Wei-Jin Jiang, Yu-Sheng Xu, Hong Guo and Zhang Lian-Mei "Research on Transaction Security Mechanism of Mobile Commerce in Mobile Internet based on MAS", International Journal of Security and Its Applications Vol.9, No.12, 2015, pp.289-302

[8] W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International Journal of Computer Science & Information Technology vol. 1 No. 1 Jan. 2011

[9] Abdulghader.A.Ahmed.Moftah. "Challenges of Security, Protection and Trust on E-Commerce: A Case of Online Purchasing In Libya". ISSN: 2278-1021-IJARCCE vol. 1, Issue 3, May 2012

[10] A Sengupta, C Mazumdar "E-Commerce security – A life cycle approach" Sadhana Vol. 30, Parts 2 & 3, April/June 2005

[11] Tripathy Biswajit, Mishra Jibitesh. "Protective Measures in E-commerce to Deal with Security Threats Arising out of Social Issues – A Framework" IAEME -ISSN 0976 – 6375(Online) vol 4, Issue 1, January- February (2013)

[12] Rane P. B., Dr. B.B.Meshram. "Transaction Security for Ecommerce Application" IJECSE -ISSN- 2277-1956. 2012

[13] Niels Christian Juul and Niels Jorgensen, "Security Issues in Mobile Commerce Using WAP", 2002

[14] Linck, K., Pousttchi, Key and Wiedemann "Security Issues in Mobile Payment from the Customer Viewpoint", 2006

[15] Yadav S., "M-Commerce and its Security Issues", 2001.