Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2468

Survey on M-Commerce

Bhanu Prakash Dubey
Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number:1758 - 1766
Publication Issue:
Vol 70 No. 2 (2021)

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

Abstract
The expansion that is worldwide of has led to the number of evolving technologies. The bone which is most popular is m- commerce it's also called as mobilee- commerce. Now-a-days mobile deals are adding most swiftly due to enabling of the internet banking services and online payment results etc. So, for all these services that are m- commerce has to connect to the internet. But whenever we are dealing with the internet security becomes main concern. And also all deals are performed over the internet enabled bias that are mobile. Because of this security in m-commerce now come more important than the traditionale- commerce system security. This paper deals with the mobile payment system, security issues and enterprises in m- commerce, some secure trade ways and results and ultimately case study one paytm operation that is m-commerce.

I. Introduction

Thee-commerce that's traditional are used to perform the online deals and payments. Thee-commerce system has a well- defined security frame work which provides the lesser range of information security, computer security and much further.

Now-a-days due to the technological advances in the movable bias increase the high speed internet access networking that's also mobile. By this internet enabled mobile bias we can perform the any where, any- timee-commerce deals via wireless network this is called mobilee-commerce i.e. m-commerce.

M- commerce is an marketable online sale service which is performed over the internet enabled mobile device by using m- commerce operation. This m- commerce is use to perform the buying of services and products online, for booking of hospices and tickets, for online bill payment, for m-banking and also for transferring the plutocrat to someone online. This adding use of m- commerce replaces the paper plutocrat and credit cards and wide operation in moment's world due to the evolving technologies in the m- commerce.

Apart of all the advantages and positivity of m- commerce it's also expose to the security pitfalls similar as data stealing. But security and sequestration of data is primary concern of any client hence we ca n't neglect it. So in this paper we're fastening on the major security issues and enterprises which are taken during designing of a mobile payment systems. In this paper we're also bandied about SSL subcaste for online sale security and one important mobile payment operation.

The paper has ensuing sections. Section II presents mobile payment systems, bracket and features of m- commerce. Section III explains about security pitfalls and enterprises. Section IV is security that's conforming. Section V correspond secure online sale technologies. and section VI contains a case study on PayTM. Eventually paper ended with conclusion.

Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2468

II. Mobile Payment Systems

A mobile payment system(MPS) can be defined as a payment system that enables fiscal deals to be performed securely from one association or an individual to other association or an existent over a network that's mobile. This M- payment offers openings that are seductive fiscal institutions, merchandisers, and also for druggies. These openings include the simplicity and ease of an sale that's m- payment.

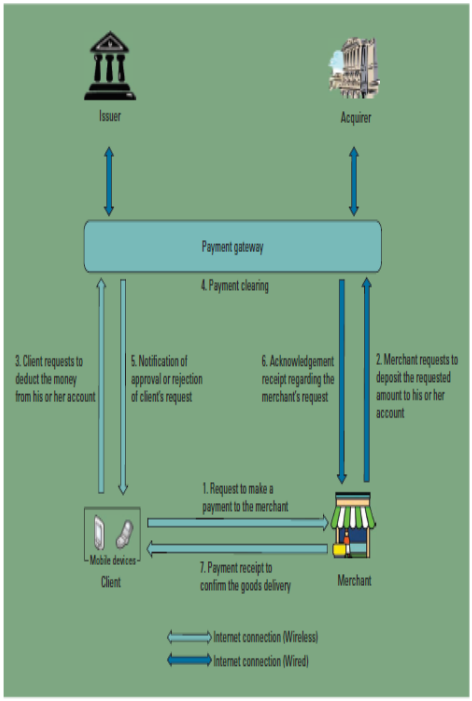


Fig1. Mobile Payment System

Figure 1 depicts the most significant aspects of the current state of an m-payment system. In general, an m-payment system is composed of four primary realities: the customer, the trafficker, the financial institution of the trafficker (also known as the acquirer), and the financial institution of the customer (also known as the issuer). The acquirer and the issuer on the side of the bank's private network and the customer and the trafficker on the side of the Internet can be connected through a short-range link made possible by the Internet and a payment gateway. A payment gateway is a relatively new technology that acts as an intermediary for the purpose of clearing payments between the the buyer and the issuer on the side of the bank's private network and the customer and the trafficker on the side of the Internet. Any Internet access service provided by an Internet service provider or the Internet itself can be used to establish a connection between a customer and a payment gateway, or between a trafficker and a payment gateway. This connection can be made using wired, wireless, or cellular technology for communication that are provided by a mobile-phone driver.

Classifying M-payments

There are two categories that are commonly accepted for classifying mobile payments: m-payment refers to either a remote payment or a payment made using a mobile device to pierce the m-payment

reverse-end system over mobile communication networks. A remote payment allows the stoner to make a payment without physically being there.

A mobile device with mobile short-range communication technologies is used to facilitate a propinquity payment, in which the stoner makes a payment using the gadget.

Features of m-commerce

Personalization Now-a-days each person has his own mobile device for transferring and entering dispatches and sale information of his private. So the m- commerce has handed the sequestration to stoner private information because stoner operates this on his own mobile device. It also manages the sound and sight in mobile device.

Ubiquity Mobile operations offer the stoner to hold the stoner information and allow stoner to perform sale from the remote position.

Quality and Easy Ordering m- commerce should allow the client to place order at moment of purchase intent and time that's real updates can help client with high effectiveness.

Localization The operation of internet makes m- commerce more salutary than the wirede-commerce using GPS technology. It also provides the discovery of stoner current position while moving also to shoot and admit data related to the stoner sale.

III. Security threats and concerns

Security threats and vulnerability and risks

Vulnerability	Threat	Risk
Over-the-air (OTA) transmission between a phone and point of sale (POS)	Interception of traffic	Identity theft, information disclosure, replay attacks
Inadvertent installation by users of malicious software on mobile phones	Downloaded application intercept of authentication data	Theft of authentication parameters, information disclosure, transaction repudiation
Absence of two-factor authentication	User masquerading	Fraudulent transactions, provider liabilities
Changing or replacing a mobile phone	Configuration and setup complexity	Reduced adoption of the technology, "security by obscurity"
Smartphone internet and geolocation capabilities	Malware on mobile devices, poor data protection controls by merchants or payment processors	Data disclosure and privacy infringement, profiling of user behavior
POS devices installed at merchant premises	Masquerade attacks, tampering with POS	Theft of service, replay, message modification
Lack of digital rights management (DRM) on the mobile device	Illegal distribution of content (such as, ringtones, video, or games)	Theft of content, digital piracy, risk to provider for digital rights infringement, loss of revenue to content provider or merchant
Weakness of GSM encryption for OTA transmission, SMS data in cleartext on a mobile network	Message modification, replay of transactions, evasion of fraud controls	Theft of service or content, loss of revenue, illegal transfer of funds
Weakness of GSM protocol for mutual authentication	Impersonation or man-in-the-middle attacks	Eavesdrop, modify, delete, reorder, replay, and spoof signaling and user data messages
Weakness of encryption technique on SIM cards	Tampering or cloning of SIM card	Malicious transactions carried out on user's behalf, theft of stored payment credentials
Weak cryptographic keys or predictable random-number cryptographic APIs provided by development platforms	Cryptanalysis and dictionary attacks	Unauthorized access to restricted functionalities

Fig2. Security Threats

Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2468

M-Commerce Security Concerns

The main security concerns which user wants in mobile commerce are Confidentiality, Integrity and Availability.

Fig3. Security concern

The confidentiality integrity and vacuity is integrated to known as CIA trio.

Confidentiality: Confidentiality is original to sequestration and the confidentiality is designed to help sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. moment information is one of the most important means in m- commerce so we've to give the confidentiality to the stoner information.

Integrity: Data must keep its thickness, delicacy, and responsibility throughout its whole life cycle for the integrity of the data to be maintained. The data must remain unchanged during the transportation process, and steps must be taken to prevent unauthorised individuals from being able to modify the data in any way. We have a responsibility to ensure the honesty of data generated by operations such as mobile commerce, which take place over the public internet.

Vacuity the data is only available to authorized druggies. Data is precious when it's in right hand nothing but use by the stoner that's applicable any- time and any where in the world.

III. Security Solutions

i. Cryptography

Cryptography is an important technique that provides security to the online transactions and payments because all these m-payments are performed over the public or open network so it needs high level security. One important cryptography technique that use for security purpose is symmetric cryptography that is key. In this both parties i.e. sender and receiver has same shared secret key and by this key parties performed secured communication.

The key operations in symmetric key cryptography is very complex, this complexity is reduced by using public key cryptography. The public key cryptography uses the set public and private keys. The public key is the one which is published in the network and private key is one which kept as secret. Usage of these public and private keys eliminates the need of sharing secret key.

However computational expensive traditional asymmetric key cryptography is not suitable for the mobile devices hence the introduction of the symmetric key cryptography improves the speed because there low computational speed. More than it also needs the verification from the certificate authority during each transaction so this symmetric key cryptography is more suitable for m-commerce requirements that it nullifies the impersonation attack, for every public key the certificate is required and.

ii. Secure socket layer

In order to create a safe and secure exchange of information between the client and the server, the protocol known as secure socket layer is utilised. This security layer is also known as the Slandered security layer (SSL). It ensures that the data that is transferred between a web server and a web browser will always be protected from unauthorised access. There are three different types of keys that are used to establish a connection: public, private, and session keys. The browser and the server establish an SSL connection through a process known as SSL handshaking, which is an encrypted mechanism.

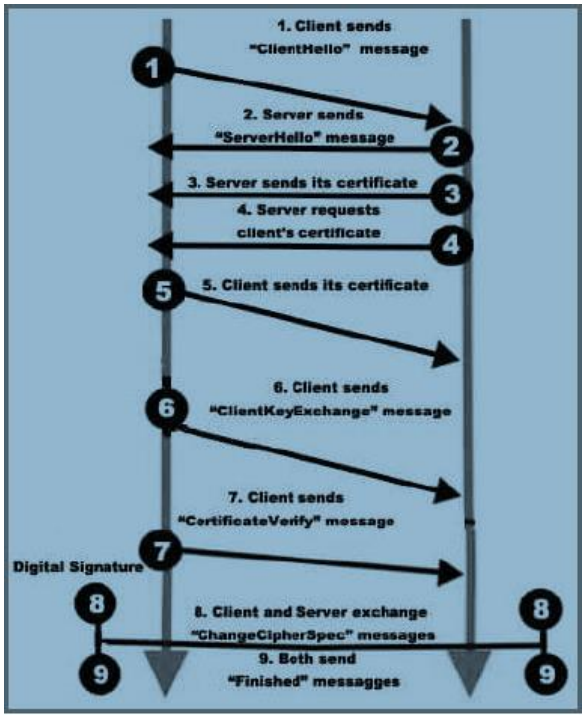


Fig3. SSL Handshaking

Following the construction of a secure connection, the session key is used to encrypt all of the data that is being transmitted. When a browser is connected to an SSL-secured web server, the browser will create a certificate signing request, also known as a CSR. The server will then transmit a copy of its public key to the SSL certificate. The browser checks the origin of the certificate in the database of a reputable CA (Certificate Authority), as well as the validity and authenticity of the certificate, and ensures that the common name associated with the certificate is appropriate for the website to which it is connecting. A symmetric session key is generated, encrypted, and then sent back to the system using the public key that is stored on the server. This happens only if the

browser permits and verifies the same. The server will then proceed to decode the symmetrical session key using its private key, after which it will send back an acknowledgement that has been encrypted using the session key in order to initiate the encrypted session. Both the server and the browser are now connected via a secure connection, and they are sending their data encrypted with the help of a session key.

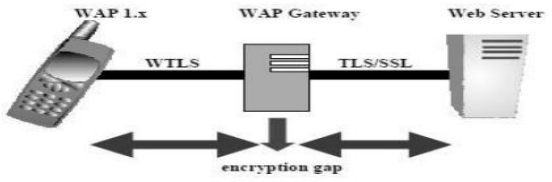
iii. Secure online transaction technologies

Transaction Authentication Number (TAN)

A transaction authentication number (TAN) is a sort of password that can only be used once and is used for online banking in addition to a regular ID and password. It is a type of OTP that is utilised for the purpose of authenticating financial transactions. TAN's involvement in two-factor authentication provides an additional layer of protection for the network. When it comes to applications for mobile commerce, transactions cannot be completed unless a valid TAN is present. In the event that we lose the token (TAN), we will not be able to complete any transactions.

Wireless Application Protocol (WAP)

WAP is a global definition of a collection for interacting protocols that are used to authenticate mobile users with wireless devices in order to simply access and interact with the data and services in a direct manner. WAP was developed by the Wireless Application Protocol Working Group. The Wireless Application Protocol (WAP) enables mobile commerce by enabling the sharing of transaction information between the customer and the merchant via wireless devices. In addition, the WAP provides the user with a wide variety of other features, such as the ability to access data and services at any time and from any location in the globe.



Mobile Transaction Authentication Number (MTAN)

The number of countries that have just started implementing MTAN, which is now the most. When a user completes a transaction by using his credit card, the bank creates the Transaction Authorization Number (TAN) and sends it to the customer's mobile device by way of SMS. Because of this, the TAN is now referred to as an MTAN. This is used to validate the client or user, as well as the transaction itself, to ensure that it has not been altered by another person or bank. The provision of safety for financial transactions conducted via mobile devices is the primary objective of the MTAN project.

III. Survey on PayTM

A check is conducted on the PayTM IT Company which is furnishing the sale that's online to the guests.

The PayTM uses the SSL instrument to give the online sale security to the guests and SSL subcaste provides the end to end security to druggies.

In India, All the deals are performed in the through PayTM gateway.

The Table 1 gives the description about the different parameters in sale with SSL subcaste and without SSL subcaste.

i. Transaction with SSL and without SSL Layer

Parameter	**With SSL**	**Without SSL**
Security	IT provides security between the server and the client. No one can't access the information because it uses secret key for communication and also uses the SSL certificates for verification and it uses the handshake protocol to check user is valid or not.	Lack of security because it does not make use of any unique ID and anyone can access the information.
Encryption	In this the encryption is done only when user is valid by a secure tunnel. Encryption is used during the data exchange.	It does not provide any type of message encryption.
performance	SSL provides the better performance	It does not.
Authentication	The authentication uses the MAC which is generated during the user login to the account then it get stored then verified. The digital signatures also verified in this stage.	It only checks user name and password during the login but does not store any MAC for verification.
Authorization	Only valid user can modify his own information.	When SSL Security not there, then anyone can hack account and access the information. There is no privacy.
WWW Application	Browser uses the HTTPS:// protocol for connection establishment.	Here browser only uses HTTP for connection establishment.

ii. Survey on PayTM Online Transaction

Table 2 presents a comparison between a transaction with an SSL Layer and one without an SSL Layer, based on the survey presented above. In addition to this, it provides a rating based on the survey that was carried out on PayTM. A grade of 1 is provided for Very Poor, 2 for Poor, 3 for Average, 4 for Good, and 5 for Excellent.

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

Table 2 Performance Table with and without using SSL Layer Transaction

iii. Online Transaction Security Chart

Grounded on the performance Table- 2, security map is drawn for online sale with and without SSL Subcaste security. It shows that sale with SSL Subcaste is more secure also the without SSL Subcaste.

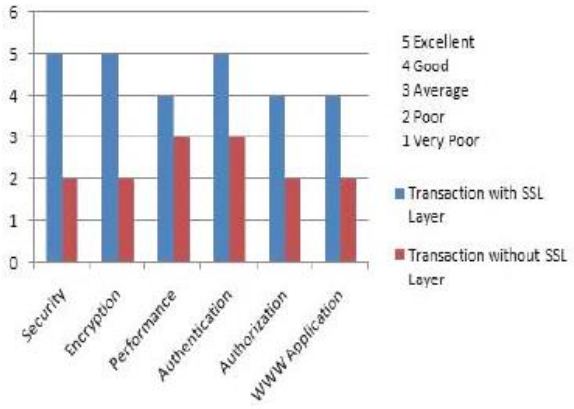


Fig4. Online Security Chart

IV. Conclusion

The m- commerce is an arising field which has a lot of attention by diligence and citizens. It also plays a part that's pivotal the life of business and guests, so the security in m- commerce is a vital issue now-a-days. This paper concentrates on m- commerce systems and safety in m- commerce systems. Then we bandied number of issues related to the m- commerce and also provides results similar as cryptography. This bone

is most important result but encryption fashion isn't enough to give security. So, along with this we're also talking about SSL instruments which give high position of security. Following with this we're also bandied some being technologies. Eventually we conclude that the advantages of security fashion in m- commerce that helps to give safety to the guests to place purchase and order particulars or services from online.

References

[1] Security Issues in M-Commerce for Online Transaction by Deepak Kumar, Nivesh Goyal in 5th International conference on Reliability, Infocom Technologies and Optimization in year 7.9.2016.
[2] Secure Mobile Payment Systems by Jesus Tellez Isaac and Shereali Zeadally in 2014.
[3] Evaluation of Mobile Network Security in case of mobile Transactions in Zambia in American International Conference on Information Science, Computing and Telecommunication in year 2013.
[4] 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.
[5] 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
[6] D. A. Montague, Essentials of Online payment Security and Fraud Prevention, John Wiley & Son, 2010, p.1-5

[7] 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
[8] 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