SECURITY ISSUES IN M COMMERCE FOR ONLINE TRANSACTION

A PROJECT REPORT

Submitted to

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

In partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING IN COMPUTER SCIENCE AND ENGINEERING

By

J. GURU MONISH AMARTYA

191811365

Supervisor

DR. T. VIGNESH

SAVEETHA SCHOOL OF ENGINEERING

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL

SCIENCES, CHENNAI – 602 105

JANUARY 2021

BONAFIDE CERITIFICATE

Certified that this project report "SECURITY ISSUES IN M COMMERCE FOR ONLINE TRANSACTION" is the bonafied work of "J. GURU MONISH AMARTYA (191811131)" who carried out the project work under my supervision.

SIGNATURE	**SIGNATURE**
DR. BEAULAH JEYAVATHANA	**DR. T. VIGNESH**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Professor and Head, Department of CSE,	**Assosiate professor,Department of CSE ,**
Saveetha School of Engineering ,	**Saveetha School of Engineering ,**
Saveetha Institute of Medical and	**Saveetha Institute of Medical and**
Technical sciences.	**Technical science.**

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION BY THE CANDIDATE

I declare that the report entitled **"SECURITY ISSUES IN M COMMERCE FOR ONLINE TRANSACTION"** submitted by me for the degree of Bachelor of Engineering is the record of the project work carried out by me under the guidance of **"DR. T. VIGNESH"** and furthermore this work has not formed the basis for the award of any degree or diploma in this or any other University or other similar institution of higher learning.

SIGNATURE

J. GURU MONISH AMARTYA

(191811131)

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 today's 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.

ACKNOWLEDGEMENT

.

This project work would not have been possible without the contribution of many people. It gives me immense pleasure to express my profound gratitude to our honorable Chancellor **Dr.N.M. Veeraiyan**, Saveetha Institute of Medical and Technical Sciences, for his blessings and for being a source of inspiration. I sincerely thank our Vice Chancellor **Dr. Rakesh Kumar Sharma** for his visionary thoughts and support. I am indebted to extend my gratitude to our Director madam **Mrs. Ramya Deepak,** Saveetha School of Engineering, for facilitating us all the facilities and extended support to gain valuable education and learning experience.

I register my special thanks to **Dr. B.Ramesh,** Principal, Saveetha School of Engineering and **Dr .SP. Chokalingam ,** HOD, Department of Computer science engineering, for the support given to me in the successful conduct of this project. I wish to express my sincere gratitude to my supervisor **DR. T. VIGNESH**, for her inspiring guidance, personal involvement and constant encouragement during the entire course of this work.

I am grateful to Project Coordinators, Review Panel External and Internal Members and the entire faculty of the Department of Information Technology, for their constructive criticisms and valuable suggestions which have been a rich source to improve the quality of this work.

J. GURU MONISH AMARTYA

(191811131)

1. 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 . 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. M-Commerce makes people's lives comfortable and provides the security to the user. M Commerce had a 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.

The appearance of various technologies and applications has been in cognizance over the years, which are heading for at mobile computing and the web. Mobile commerce is known to be a significant functionality of the electronic commerce if not the most important type of electronic commerce. This form of commerce will be majorly included transaction activities being carried out over these new technologies as well as applications.

Today E-commerce has enhanced the focus on security both for systems and also for messaging and transactions. If we see the recent advancement in the handheld personal assistant (PDAs), wireless communication technologies and enveloping infrastructure promise to extend comfort in the environment for mobile users-commerce transactions can be performed over ad-hoc wireless networks or adhoc m-commerce which can be considered as wireless trading outside established computer networks.

While M-commerce has made life much easier for many people around the globe as the daily transactions are being carried out wirelessly which is more convenient but with that it poses some security threats. “M-commerce = e-commerce + wireless web”.

The term M-commerce (mobile-commerce) derives from E-commerce (e-commerce) which denotes business transactions over the internet. The transactions could be buying and selling goods/services by accessing the internet. Both M-commerce and E-commerce are part of two districts business markets: B2B (Business to Business) and B2C (Business to Consumer), the two distinct from dealing with business for the first and dealing end consumer for the last. From these business concepts, we can see that a B2B market, is more like E-commerce, where a business / user, accessing the internet for business transactions from an unstated devices. The technology used for this system could either be wireline (home PC, end user devices) or wireless (via mobile phones, PDAs, end user devices). In fact the term M-commerce, is all about a wireless E-commerce

that is where a mobile device is used to access the internet for business transactions either in B2B or B2C markets.

With the ubiquitous availability of mobile phones (other end user devices), M-commerce services have a promising future, especially in the B2C market. Future development applications include buying over the phone, purchase and redemption of tickets and reward schemes, travel and weather information, and writing contracts on the move. However, the success of M-commerce today, very much depends on the security of the underlying technologies. For example, credit card charges for transactions on the internet are 15%, versus 1% for POS (Point-of-Sales) credit card transactions. The chargeback rates grow to 30% digital product are sold. For M-commerce to take off, fraud rates have to be reduced to an acceptable level. As much security can be regarded as an enabling factor for the success of M-commerce applications. In this report, I discuss the security issues associated with M-commerce and their solutions based on two existing M-commerce applications, namely:

Mobile Payment Systems: business transactions on the internet require the payments of either goods or services. M-payment systems have different requirements and characteristics than E-payment systems (electronic-payment).

Mobile-Banking Systems: types of execution of financial services in the course of which – within an electronic procedure – the consumer uses mobile communication techniques in conjunction with mobile devices for banking transactions.

2. ISSUES IN ONLINE TRANSACTION FOR ECOMMERCE

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

2.1 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. Authentication is the process of recognizing a user's identity.

It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server. In the M-Commerce applications used is that user authentication. The user authentication involves the two steps in sequence,user identification, claimed identity verification and validation.

2.2. 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.

A transaction performed by using a payment card to determine if the card holder has sufficient funds on his/her card to pay for a given transaction. An authorization will take only seconds, and allows the merchant to ensure that payment will be taken from the card. When an authorization is declined, there are a few possible outcomes.

If the customer has insufficient funds in his account, the card will be declined and returned to the customer; if the card has been stolen or canceled then the merchant will cut the card in two. When an unauthorized card is used for an online transaction, the transaction will simply be declined.

2.3. 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.

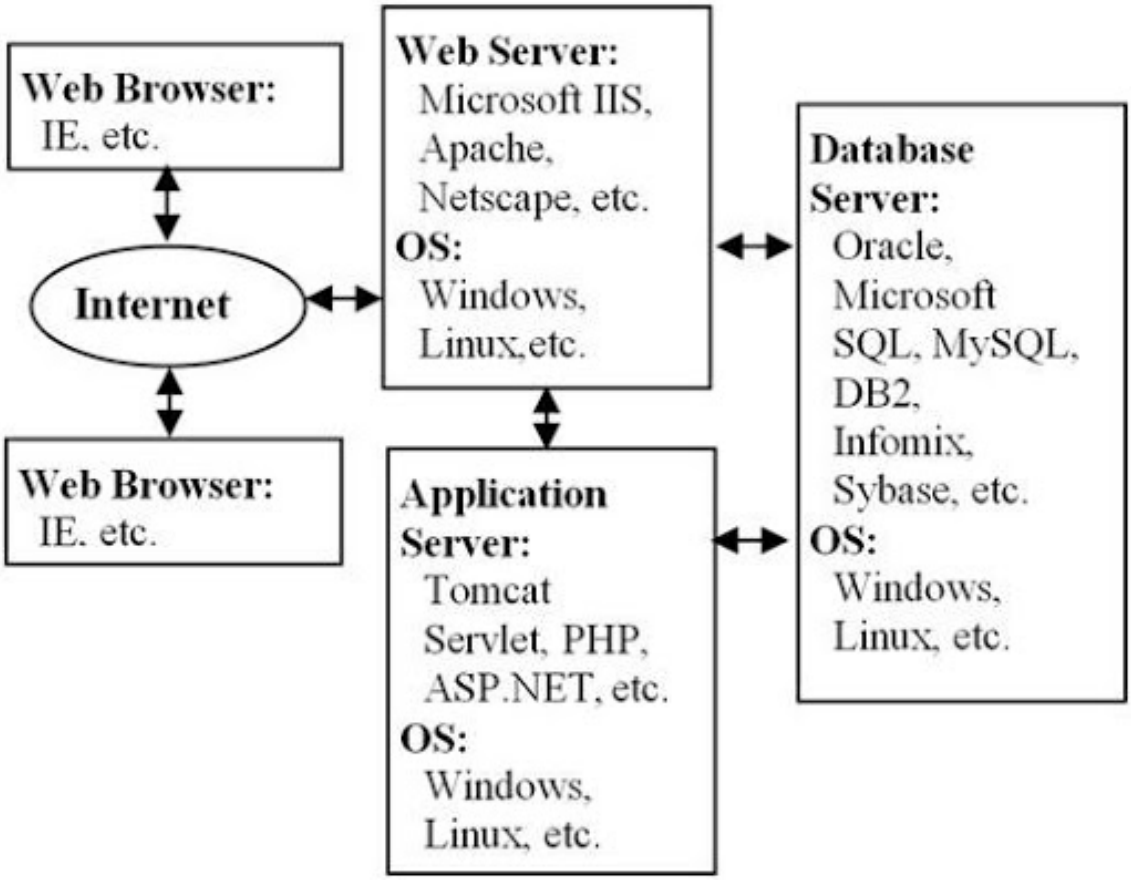
Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

In computing, unencrypted data is also known as plain text and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms, or ciphers.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a key, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Encryption is commonly used to protect data in transit and data at rest. Every time someone uses an ATM or buys something online with a smartphone, encryption is used to protect the information being relayed. Businesses are increasingly relying on encryption to protect applications and sensitive information from reputational damage when there is a data breach.



RISK MANGEMENT IN ONLINE TRANSACTION

3. 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:-

3.1. 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.

Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records. You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should. A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident.

Such a failure of confidentiality, commonly known as a *breach*, typically cannot be remedied. Once the secret has been revealed, there's no way to un-reveal it. If your bank records are posted on a public website, everyone can know your bank account number, balance, etc., and that information can't be erased from their minds, papers, computers, and other places. Nearly all the major security incidents reported in the media today involve major losses of confidentiality.

3.2. 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.

Integrity refers to ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine. Imagine that you have a website and you sell products on that site. Now imagine that an attacker can shop on your web site and maliciously alter the prices of your products, so that they can buy anything for whatever price they choose. That would be a failure of integrity, because your information in this case, the price of a product has been altered and you didn't authorize this alteration.

Another example of a failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.

3.3. 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.

Availability means that information is accessible by authorized users. If an attacker is not able to compromise the first two elements of information security (see above) they may try to execute attacks like denial of service that would bring down the server, making the website unavailable to legitimate users due to lack of availability.

3.4.FEATURES OF M-COMMERCE

Following are some unique features of M-commerce.

3.4.1.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.

Ubiquity refers to the ability of a company—and the products and services it sells—to establish a dominant presence among consumers. Although physical retail locations and traditional marketing initiatives support this end, the internet and e-commerce do much to champion ubiquity for a company. The Internet makes it possible for consumers and companies to be in constant contact with one another, albeit electronically. Thus, consumers who wish to buy goods and services online can do so at any time, and from virtually any location.

3.4.2.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.

Localization is the process of making something local. For e-commerce, this not only means making the site available for different countries, but the language adapts for those countries too. Localization is absolutely necessary if e-commerce businesses desire to be successful in different countries. Not only does it enable it to be accessible to more people, but it appeals to the target audience in a new way. Localization is modified in both software and content of an e-commerce site, and often requires specific tools and specialized help.

3.4.3. PROACTIVE FUNCTIONALITY: This feature ensures that th 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.

3.4.4.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.

M-Commerce Security Concern

4. SECURE ONLINE TRANSACTION

4.1 CYBER SECURITY

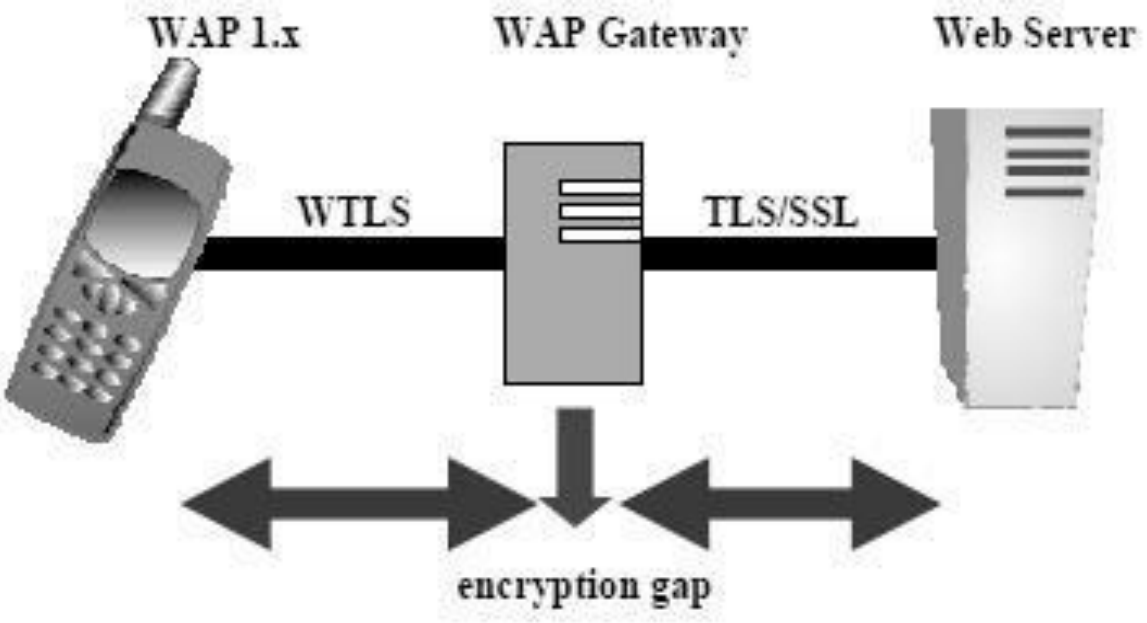
Cyber security is an important topic now a days. In currently, cyber security is one of the major issues for national security. Customer's trust and security is also a prime concern for any company in 21th century. Some of the other mechanisms are authentication, authorization, integrity, confidentiality,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

4.2. 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.

4.3. 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.



Wireless Application Protocol Security

4.4. 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.

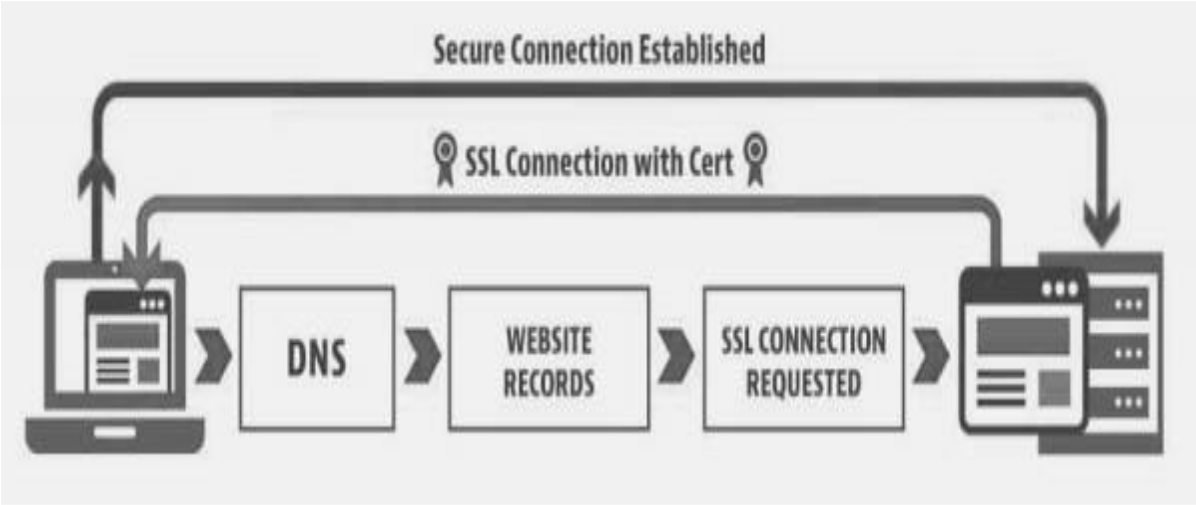
5. SSL LAYER

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.

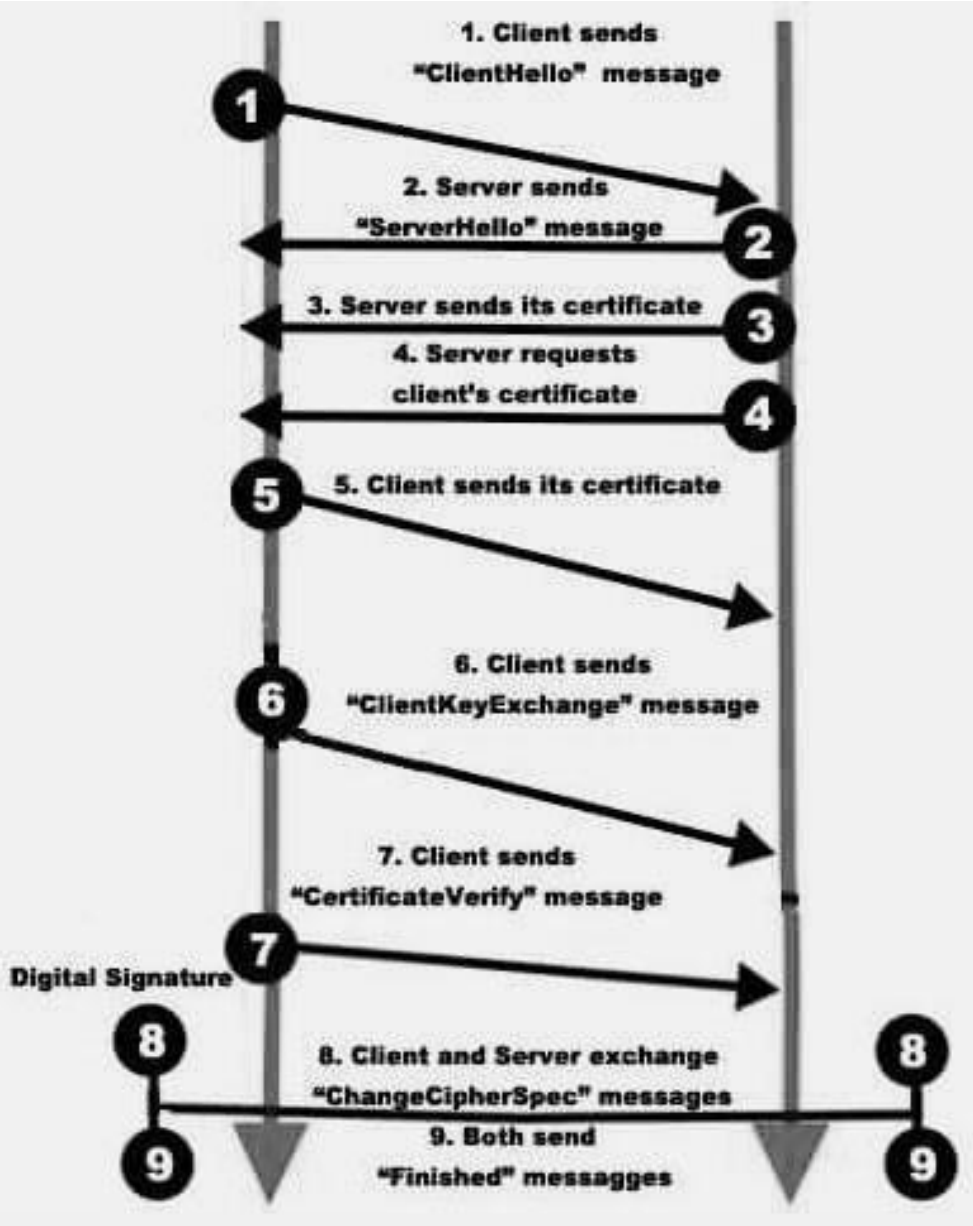


SSL Layer

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.

5.1.SSL HANDSHAKING ALGORITHM



SSL HANDSHAKING

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

5.2.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.
- 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.

6. 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.

M-Commerce security is a very crucial issue that needs further research to introduce efficient and effective solutions. In this article, various security concerns were expounded. ECC certainly appears to provide a viable alternative to RSA. There are potential advantages, especially when used in devices with limited processing capability and memory. Typical applications include M Commerce using handheld wireless devices. There are, however, some problems and issues that are inhibiting the widespread adoption of EEC. These include (i) the real security of such systems is still not well understood, (ii) difficulty of generating suitable curves, and (iii) relatively slow signature verification. Time will tell its future.

7. FUTURE SCOPE

E-commerce, which emerged in the early 90s, stands for purchasing, selling, and exchanging goods or services using internet-enabled electronic devices. E-Commerce enabled websites and the Internet have become part of today's business.

Addressing the issue of protecting consumers' privacy opens the door for many research opportunities. Different research efforts are currently being undertaken related to E-Commerce companies, the government, the interaction between the consumer and the E-Commerce company, the interaction between the consumer and the government, and the interaction between the E-Commerce company and the government .These research opportunities would provide a new set of insights and results, which would be beneficial to understanding the core issues and lead to the appropriate steps to safeguard the existing systems.

Amazon, Flipkart, Myntra, Snapdeal, Jabong stand testimony to the enormous success of E-Commerce in India, one of the fastest growing markets in the Asia Pacific region. 2016 recorded a growth of 70% and the consumer base almost touched 100 million in 2019, ensuring profits and growth. Nearly 35% of transactions happen through mobile phones – triple that of the percentage in the last fiscal.

8.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 Engineering Volume 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 Ecommerce 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.

[16] Woodbury, A.D., Bailey, D.V., and Paar, C. (2000), “Elliptic Curve Cryptography on Smart Card without Coprocessors”, Proc. of the 4th Smart Card Research and Advanced Applications Conf., September 20-22, pp.1-20.

[17] Xydis, T.G. (2002), “Security Comparison: Bluetooth Communications vs. 802.11”,

[18] Yeun, Chan Y. and Farnham, Tim, “Secure MCommerce with WPKI”, 2001.

[19] Ganley, M.J. (2000), “Elliptical Curve Cryptography”, Zaxus White Paper, 1-9

[20] Goldman, Jeff, “Wireless Security and M-Commerce”, The Feature, March 8, 2001,

[21] Harrison, A. (2000), “Motorola, Certicom Ink Elliptic Crypto Deal”, Computerworld, May 22.

[22] “How the French are Succeeding with M-commerce”, Wireless developer Network,

[23] Juul, Niels C. and Jorgensen, N. (2001), “WAP may stumble over the Gateway”,

[24] Maffeis, S. (2000), “M-Commerce Needs Middleware!”,

[25] Messham, James, “M-Commerce Security”,

[26] “Mobile Commerce (M-commerce)”

[27] Osborne, Mark, “WAP, m-commerce and security”, 2000,

[28] Pietro, Robert D. and Luigi V. Mancini, “Security and Privacy Issues of Handheld and Wearable Devices”, Communication of the ACM, September 2003, Vol. 46(9), 75-79.

[29] “PKI Moves Forward Across the Globe”, Wireless developer Network,..

[30] Vainio, J.T. (2000), “Bluetooth Security".