iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VII **Month of publication:** July 2018

DOI: http://doi.org/10.22214/ijraset.2018.7129

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

OTP on GPS: An Enhancement to OTP Security Model for Securing On-Line Transactions

Satti Sateeswara Reddy[1], M.A Prasad[2], V.Satish[3]
[1,3]*Assistant Professor,* [2]*Associate Professor Department of MCA, Dr.L.Bullayya P.G College*

Abstract: ***In this digital era, Online payment has become more prominent through various e-payment methods for faster and efficient way of doing business. Debit and Credit cards are used mostly for e-commerce. The major drawback here is when the transaction is under process, card owner have no control to roll back the ongoing transaction or in aborting the transaction. Online fraud is also increasing and spreading rapidly across many domains, the cyber criminals exploit various ways to find the vulnerabilities and performs the crime . This paper illustrates the on-line payment model which include the usage of credit and debit cards and discusses various threats and introduces a model to withstand the e-payment frauds. The main objective of this paper is to propose a model based on the concept of Global Positioning System (GPS) and One Time Pin (OTP) which tracks the location of the devices that participate in the transaction process.***

Keywords: ***Payment gateway, e-commerce, cybercriminal, one time pin(OTP), global positioning system(GPS)***

I. INTRODUCTION

Now a days, E-commerce is growing exponentially with the global market on internet platform and most of the online transactions are performed using a credit card or debit issued by bank, as people started adopting electronic money. Online business also started to grow in many diversified areas making a considerable surpass of general business. E-commerce made business available 24x7 with everything at our door steps from the entire globe making price comparison easier, advantage of selecting from wide range of available products, getting the reviews to know about the product pros and cons of the product, probable time of delivery and so on while saving the time to purchase something only at business hours. This will eradicate the time zone differences between the geographical areas.

Internet is widely accessible on ubiquities devices such as mobile phones which act as a participating entity in doing an online purchase. Banks started registering mobile numbers for their account holders to notify about the bank transactions made to their accounts to minimize the manual entries to bank for each and every financial operation they make. This way, banks also became a part of the internet and required to stay online round the clock.

Payment gateway act as a trusted third party between the user and the bank to secure the transaction process.

The payment gateway checks the credentials by contacting to the bank and provides the services with faster and efficient way. It is very difficult to compromise the system and because of this the merchant servers employee these systems for collecting the e-cash as they always have a strong secure mechanism.

The application on the merchant web site re-directs the user to this payment gateway once user shows the interest to pay the amount. The payment gateway once completes the transaction process in a secured way it then the user to have the merchant website to know the details. The e-commerce transaction scenario is depicted in the figure1.

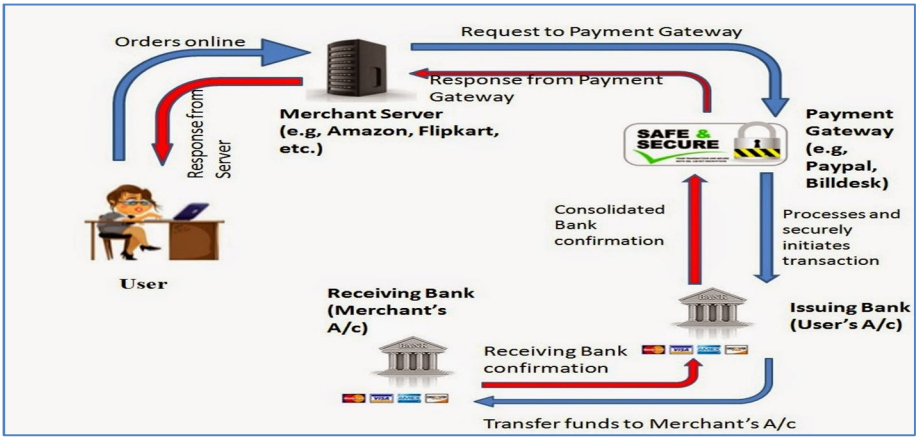


Fig.1 e-commerce transaction model[1]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Advancements in internet technology also bought new improvements in various types of cyber attacks which caused considerable financial damages, Online fraud is one among them. This paper focuses on the credit/debit card
associated risks and frames a model to shield itself to such type of threats to a larger extent .

II. TYPES OF CYBER ATTACKS

A. There are Numerous Types of Attacks Out of Them The Main Types Are Listed Below[2] [3]

1) *Hacking:*hacking is an act committed by an intruder by accessing your computer system without your permission
2) *SQL Injection:* used to attack any type of unprotected or improperly protected SQL database.
3) Cross-site scripting: also known as XSS attack, here the hacker infects a web page with a malicious client-side script or program
4) *Phishing:* a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise
5) *Cyber stalking:* Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her
6) *Data diddling:* Data Diddling is unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track
7) *Identity Theft and Credit Card Fraud:* Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name
8) *Salami attack:* is a technique by which cyber-criminals steal money or resources a bit at a time so that there's no noticeable difference in overall siz
9) Denial of Service attacks: They're carried out by opening many connections to your computer and leaving them open; this consumes plenty of resources on your computer and can crash it
10) *Malware:* "Malware" refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base
11) *Credential Reuse:* Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in and do all the damage
12) *Session Hijacking and Man-in-the-Middle Attacks:* The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server
13) *Telecommunication Attack:* is an emerging attack where a user gets a call from the attacker imposing himself as a bank employee and asks all the sensitive data which will be necessary to steal some money from your account
14) *Application Attack:* makes you to fill the data as if you are registering to any of the website and gains your personal data such as passwords for e-mails, credit card or debit card information and etc

III.ONE TIME PIN (OTP) SYSTEM

To overcome the financial frauds associated with the credit/debit cards this OTP system is being adopted, where your registered mobile is going to receive the OTP from the payment gateway whenever you want to do any online transaction. The OTP that you receive is time bounded i.e, you need to send the OTP back to the payment gate way to authenticate yourself as an authorized account holder to complete the ongoing transaction. The steps are given below

A. Step 1: User order's online through the merchant's website to the merchant server.
B. Step 2: Merchant server send the request to payment gateway

C. *Step 2:* Payment gateway prompts for your debit/credit card details through merchant server.
D. *Step 3:* User enters the details asked for and send to the payment gateway
E. *Step 4:* Payment gateway send the details to the associated bank to verify the account validity.
F. *Step 5:* If details are verified bank will send the positive response else will deny the existence of account.
G. *Step 6:* Then the payment gateway will send the four digits as OTP to the user's mobile which is registered with the bank for re-verification.
H. *Step 7:* The user receives the OTP and enters it on the payment gateway web page.
I. *Step 8:*The gateway verifies the OTP if it is correct, it will notify the bank to credit the amount to the merchant's account or if the credentials are wrong it will abort the transaction.
J. Step 9: Bank will check the account balance if sufficient funds are available it will grant the request and credit the amount in merchants account which was verified by the payment gateway or if the funds are less the same is informed to payment gateway
K. Step 10: If the payment is successful it is informed to the user or the insufficient funds message is sent.

The major drawback in the OTP system is that the user will receive a message about the amount deduction and asks to complain about it if it wasn't made by him.

There are various complaints filed in the OTP system as telecommunication fraud is closely associated with this system, where once OTP is generated some one pretends to be a bank employee asks for the OTP and performs the false financial transaction .

The man in the middle attack is also closely related to it, if the users mobile is compromised then the copy of the OTP is received by the cyber criminal along with the legitimate user and the stealing of money will be done.

The attacks not only exploit the wealth but also makes a huge loss to the credibility of merchants web site as well as the trusted payment gateway leading to decrease in the transaction through it.

To overcome, this type of attack a model OTP On GPS is proposed to maintain a good relationship between the authenticated users and the merchants.

IV. OTP ON GPS MODEL

Global Positioning System(GPS) is a navigation system that uses satellites to determine the approximate location of someone or some device anywhere on the planet where a cell phone signal is available.

This GPS is used in this model which is a refinement to the existing OTP model where in addition to the OTP details, the payment gateway also checks the location of the device which has placed the order as well as the registered mobile location which received the OTP to cross verify the identity of the user.

The Proposed model makes use of three variables, fixes it to some value. x ,used to store the ordering device location.
y, used to store the registered mobile location

When, the difference between x and y is less than the threshold value then the probability of fraud is less. If the difference between x and y is than the threshold then there is a probability of threat and is verified by communicating directly with the user whether he has initiated the transaction or not.

The difference between OTP and OTP on GPS change as illustrated below:

Step 1: user order's online through the website to the payment gate way.
step 2: payment gateway prompts for your debit/credit card details and stores the users device location in 'x'
Step 3: user enters the details asked for and send to the payment gateway
Step 4: payment gateway send the details to the associated bank to verify the account validity.
Step 5 : if details are verified bank will send the positive response else will deny the existence of account.
Step 6: then the payment gateway will send the four digits as otp to the user's mobile which is registered with the bank for re-verification and also store's the mobile location in 'y'.
Step 7: the user receives the otp and enters it on the payment gateway web page.
Step 8: the gateway verifies otp and if diff(x,y) < threshold it will notify the bank to credit the amount the merchant's account or if otp and if diff(x,y) > threshold then communicate to user and allow or abort the process or if the otp is wrong it will abort the transaction.
Step 9: bank will check the account balance if sufficient funds are available it will grant the request and credit the amount in merchants account which was verified by the payment gateway

The entire model is given in the following figure2.

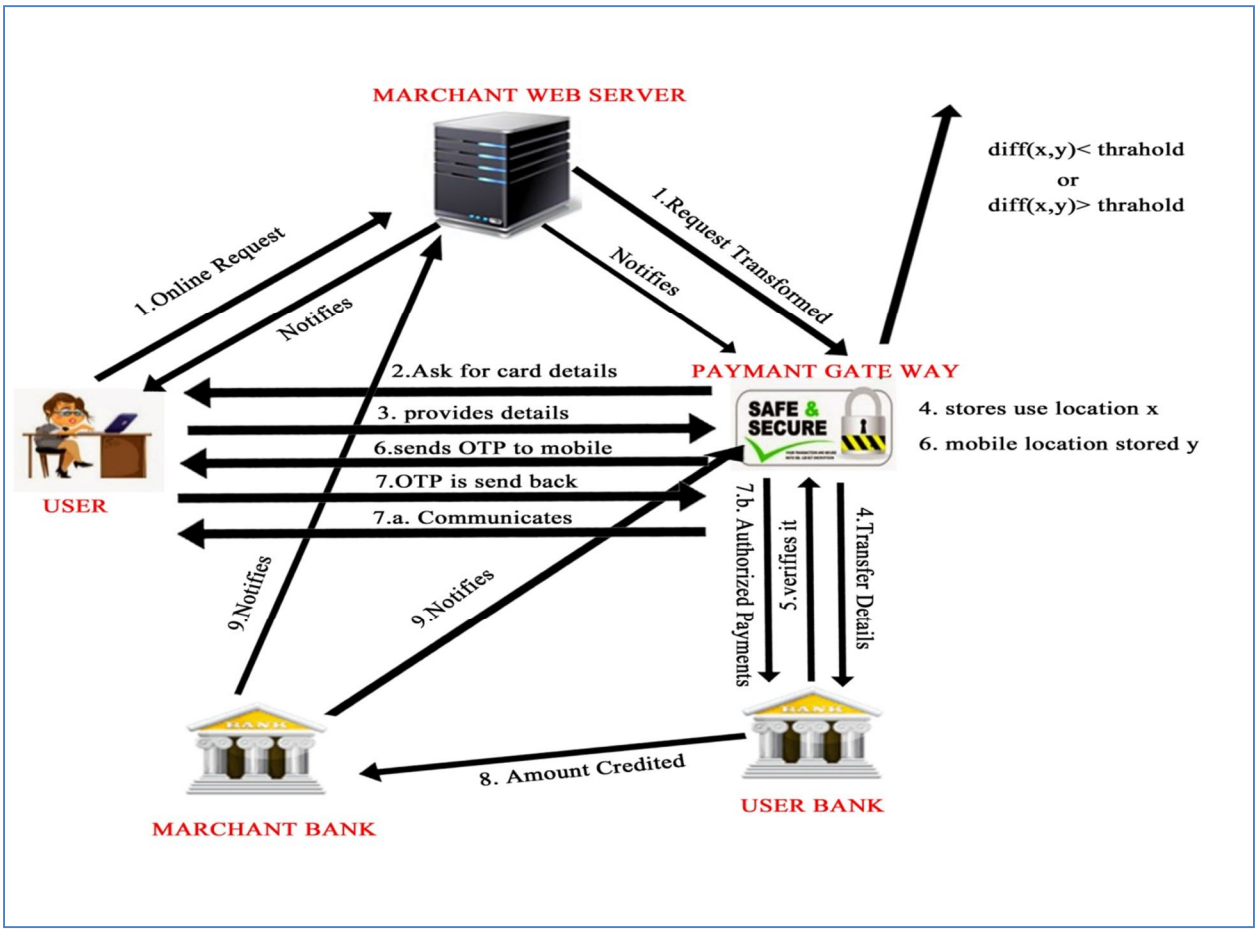


Fig.2 OTP on GPS Model

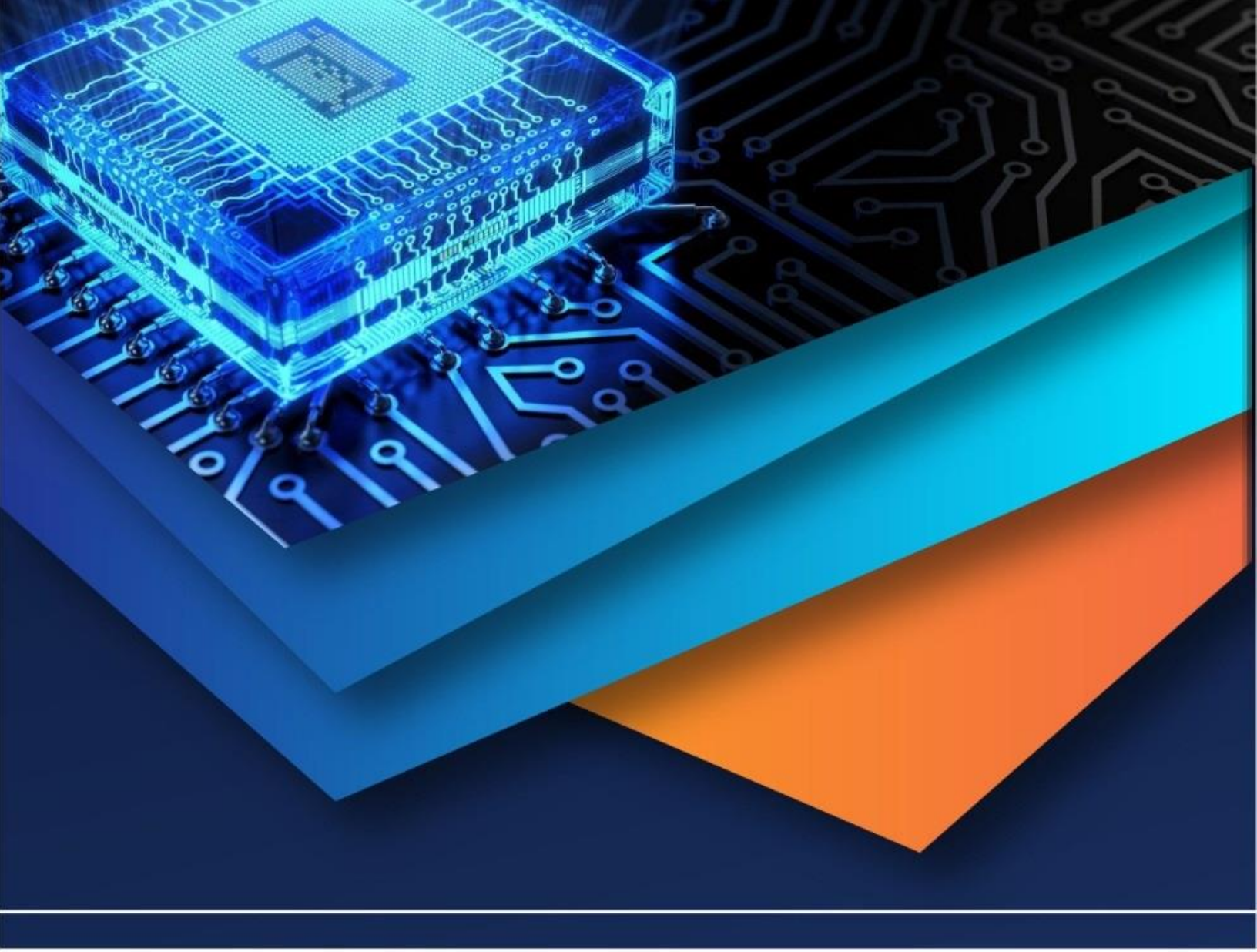
Note: The threshold value should be taken in such a way that it should give accurate results.

V. CONCLUSION

The Cyber attacks are evolving day by day and there are no means to stop them the only way to deal with them is to anticipate the affect and deal with them such that the loss is minimal. The proposed OTP on GPS model works well in reducing the online frauds compared to the existing model. This works as a fraud anticipation model, the disadvantage here is the devices which are used in the transaction should have the GPS option, if there is no such option there is a least possibility to find the accurate location of the device. Moreover, this model can be enhanced to more secured way if the mobile device has a bio-metric option to check the finger print of the user. The on line frauds can only be reduced if the users have some basic knowledge of the transactions which could be done by the merchants and the banks periodically if some change occurs in technology or a new feature is added in verification process.

REFERENCES

[1] http://www.netvuze.com/2014/05/how-to-cope-up-with-online-transactions.html.
[2] https://www.rapid7.com/fundamentals/types-of-attacks/
[3] https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
[4] Ishu Trivedi , Monika , Mrigya Mridushi," Credit Card Fraud Detection", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016
[5] Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli," Survey on Credit Card Fraud Detection Techniques", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 4 Issue 11 Nov 2015, Page No. 15010-15015
[6] Tej Paul Bhatla, Vikram Prabhu &Amit Dua,"Understanding Credit Card Frauds", Cards Business Review#2003–01



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY