International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04| Apr -2016 www.irjet.net p-ISSN: 2395-0072

Prevention of Online Transaction Frauds Using OTP Generation Based on Dual Layer Security Mechanism

Amit Kulat[1], Raghav Kulkarni[2], Nagesh Bhagwat[3], Kartik Desai[4]

[1234] BE IT, Department of Information Technology, RMD Sinhgad School of Engineering, Pune, Maharashtra, India.

Mrs. Prajakta Kulkarni[5]

[5]Assistant Professor, Department of Information Technology, RMD Sinhgad School of Engineering, Pune, Maharashtra, India.

Abstract – *With the developing technology online shopping of goods and various other products has increased to a great extent. With this service people tend to use their debit cards and credit cards for the online payment and this has been a common practice. Fraudsters take good advantage of this situation to commit frauds by making an identity theft. To avoid this many technologies emerged lately but they had some disadvantages which was not very comfortable for the end user. This project aims at implementing the web application for preventing online transaction frauds considering user comfort while making transactions from regular or different machine and from same or various other locations. Security is provided by the generation of OTP (One Time Password) providing a dual layer security mechanism which includes cookie based OTP generation and location based OTP generation. The key points of OTP generation, cookies, location parameters, dual layer security mechanism have been discussed in this paper considering user satisfaction and comfort with implementing the best possible security measures.*

Key Words: **online shopping, OTP, one time password, cookies, online fraud, transaction frauds, identity theft, security**

1. INTRODUCTION

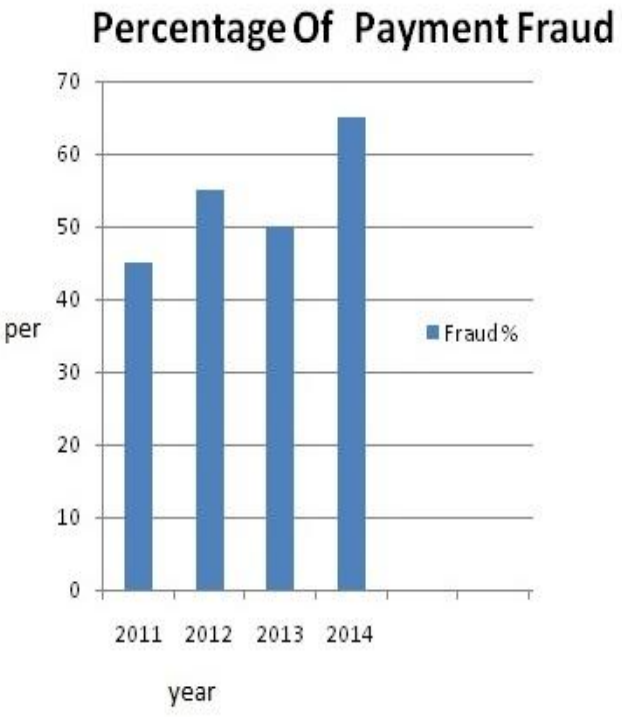
Science and technology is evolving day by day and new inventions are being made all over the world. With the growing technology lifestyle of humans has also changed to a great extent. Earlier everything that people used to buy was sold in the market. People used to go out of the house to buy a number of things. But today, with changed lifestyle, everything is sold online on various websites. People just need to sit at home and everything they want arrives at their doorstep with just a click. Because of this people are attracted to online shopping. Due to this online transaction fraud has been increased. Online transaction fraud comes into the category of internet fraud where there is a use of internet services or software with internet access to defraud victims or to otherwise take advantage of them, for example, by stealing personal information which includes various credentials such as login, password and other information which ultimately leads to Identity Theft. The most common fraud is stealing credit card details, this is when the account number and PIN (Personal Identification Number) is hacked by malicious person or by group of hackers. This project implements the application which will detect the machine from which the transaction is done. In this different machines are detected from which the transaction is done using same credentials. The location of the machine is also considered. Usually and most of the time a person does the transaction regularly from the same device, which may include home PC, laptop or smartphone. So there should be no need to confirm the person or user who is performing the transaction is a legitimate person because, he is doing the transaction from the regular device. If it is found that the transaction is initiating from different device, OTP will be generated and will be send to the registered mobile number of the legitimate user. If the user is doing transaction from the regular device but from another location different from the previous transaction location, OTP will be generated.

2. RELATED WORK DONE

Nowadays users have been indulged in online shopping for most of the time. Many of the users do regular shopping online and everyone comes across the security mechanism of OTP generation. The OTP is generated every time when the customer initiate the transaction which hinders user comfort. Paper [1] describes about the inverse cookie-based virtual password authentication protocol. Whenever any client tries to login to the web server using ID and password and with each incorrect submission the server stores the cookie on the client's computer. It increases the computational efforts of the fraudster with each login failure to the web server. Paper [2] describes the mechanism to combat the Phishing attacks. The user will retrieve the OTP by SMS or alternate email address. The web server creates an encrypted token for the user's machine for authentication

purpose after receiving the one time password. Now if any time user want to access the particular website the encrypted token will be used for the identification of the user. It prevents the phishing attacks using user machine identification. [3] Generating OTPs and safe variable password for one time use using voice recognition mechanism. Using voice features, information of biometrics which is used for powerful personal identification. Simulation of voice samples is obtained from random five clients and there is a generation of keys for OTP with the help of noise-free recorded voices. Mobile device first capture the voice and then sampling process takes place from which the noise is removed and these noise-free sample is used to generate OTP keys. The protocol is used for secure communication and to exchange OTP keys between the devices. The paper [4] includes brief discussion of the generation of OTP based on image authentication. Nowadays due to increase in the execution of phishing attacks the image authentication is very beneficial. Image based authentication followed by HMAC based one time password is implemented to achieve high level of security. The website displays the grid of images to the user when he logins for the first time it consist of password set combined and mixed with other images. The user has to identify the correct images for the authentication process. The paper [5] shows studies about the impact of fraud prevention on bank customer relationships. The paper focuses on the German retail banking market. Fraud prevention techniques and methods are beneficial to increase the quality of customer relationship and the customer loyalty. Socio demographics shows the fraud prevention with customer familiarity with and knowledge of bank's fraud prevention considering relationship qualities which includes satisfaction with bank and services, trust in bank and services, commitment to bank and customer loyalty which includes customer intention to continue relationship and customer intention for cross-buying. Paper [6] gives details about credit card fraud detection techniques and methods. The implementation of the techniques in the paper not totally prevent credit card frauds but minimizes the possibility. One of the technique used in the paper is the decision tree in which the nodes and edges are labelled with attributes name and attribute values respectively. This method is easy to implement but the disadvantage is to check each transaction one by one.

2.1 Percentage of Payment Fraud

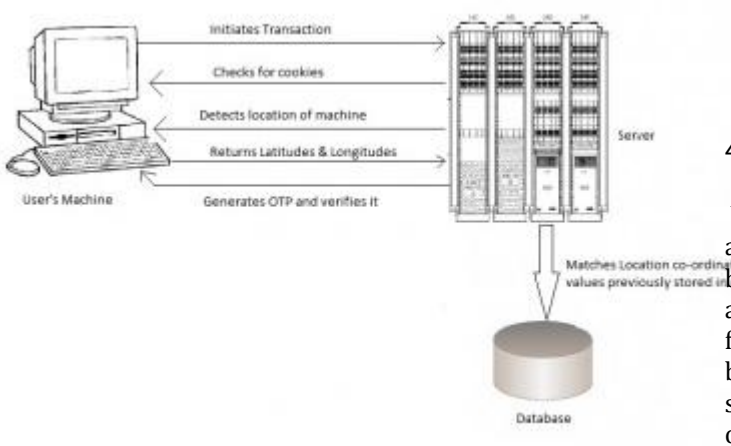


3. PROPOSED METHOD

In this paper we have implemented the web application for the prevention of online transaction fraud using dual layer security mechanism. Dual layer security in the sense, one layer which denotes cookie based prevention and the other denotes location based prevention.

1) Cookie-based prevention: When user initiates transaction for the first time, cookies get generated on the user machine and OTP gets generated. This cookie is specific to that user. If the same user again tries to initiate transaction from the same machine and same location OTP will not be generated.
2) Location based prevention: The system detects latitude and longitude wise locations of user's machine, from which the transaction is being initiated. The values obtained are then compared or matched with the location coordinates previously stored is the database. If these values matched, then the system will know that the transaction being initiated is legitimate and thus OTP will not be generated. Considering the same machine is being used to initiate a transaction from another location then the coordinates will not match and the system will infer that there is a change in location upon which the system will automatically generate the OTP.

3.1 System Architecture



Working of the system with respect to architectural components is explained below:

The web application focuses on preventing the frauds in online credit card and debit card transactions.

1) At first the system asks the user to get registered and then allows user to perform any transactions he wishes. After the user is registered he can then initiate the transaction process. When user initiate the transaction for the first time, OTP is generated by the server and sent to the user's machine. The server generates user specific cookies into the user's machine, so that when user initiates transaction next time OTP will not be generated, considering that the user machine is located in the same location of the previous transaction. Here the server first checks for cookies on the user's machine, and if the cookie for the particular transaction is obtained, then the server moves further and checks the location of that particular machine.

2) The server then obtains the exact location of the user's machine in the form of latitudes and longitudes. Then server then goes to the database to check whether there is a change in the user's location. This is done by comparing the location co-ordinates obtained by server with the location co-ordinates already present in the database. If a match is found then it is inferred that there is no change in the location and it gives free access to the user to perform the transaction that was initiated. But if incase the co-ordinates don't match, then system infers that there has been a change in location and immediately generates an OTP to the mobile number of the user specified by user during registration.

3) Thus the system provides a dual layer security mechanism with less or minimum effort for the user than the traditional system

4. CONCLUSIONS

We have designed the application using which we have added an extra layer of security in credit card transactions based on location ultimately providing double security and thus a secure online transaction system for the user for not just online credit card and debit card transaction but also transferring funds from one account to another securely. Similarly the application proves effective not only to the customers but also to banks and can easily implement it on a real time basis.

ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Mrs. Prajakta Kularni and our project coordinator Mrs. Snehal Nargundi and Head of the Department Mrs. Sweta Kale, RMD Sinhgad School of Engineering, for their valuable guidance and support.

We are also thankful to all the staff members and the institute for providing all the necessary required facilities.

REFERENCES

[1] Sandeep Kumar Sood, Anil K Sarje and Kuldip Singh , "Inverse Cookie-based Virtual Password Authentication Protocol", International Journal of Network Security, Vol.12, No.3, PP.292-302, May 2011

[2] Ahmad Alamgir Khan," Preventing Phishing Attacks using One Time Password and User Machine Identification", International Journal of Computer Applications (0975 – 8887), Volume 68– No.3, April 2013

[3] ByungRae Cha, NamHo Kim, JongWon Kim," Prototype Analysis of OTP Key-generation based on Mobile Device using Voice Characterstics",Information Science and Application(ICISA),2011

[4] Himika Parmar, Nancy Nainan,Sumaiya thaseen, "Generation of Secure One Time Password based on Image Authentication", CS & IT-CSCP 2012

[5] Arvid O.I. Hoffmann, Cornelia Birnbrich,"The Impact of Fraud Prevention on Bank-Customer Relationship" International Journal of Bank Marketing, Vol. 30 No. 5, 2012

[6] Linda Delamaire, Hussein Abdou, John Pointon,"Credit Card Fraud and Detection Techniques", Volume 4, Issue 2, 2009