Prevention of Online Transaction Using MAC Address of the Machine, OTP Two Layer Model to Identify Legitimate User

Aliza Basharat* Misbah Naz Khusbakht Afzal
Government College Women University, Silakot Pakistan

Abstract

E-shopping changed the world of selling and buying the products. With the Increase in technology and availability of resources on just one click modify the style of shopping, business, buying and selling. Use of online transaction to buy the products and conducting e- payments increasing day by day. Users now prefer to buy things and conduct shopping activities by just clicking from their machine. Trend of online shopping involved the online payments, involvement of online transactions enhance the use of credit cards, debit cards etc. The involvement of online payment is providing the facility to user and also providing the opportunity to fraudster took benefit of this to commit frauds like hacking of payment and transfer of money to some other accounts etc. The proposed model provided in this paper identify the user with the help of two layer model. The proposed model focus on the identification of user through MAC address of the machine used by the user to carry out the transaction process. With the concept that user's mostly use the same machine to carry out the transactions.

Keywords: Online shopping, cookies, MAC Address, OTP, Online fraud, identify theft, E-shopping, Online transactions

1. Introduction

Technology is evolving and emerging in human life day by day. In past people use to go markets to buy things, but in present life is too much busy people don't have time to go to market to buy things. They prefer to buy things online. Online things are one click away from the user. Because of this facility people are feel easy to shop online rather than buying from the market. The online trend of shopping includes online payment. Online payment increase threats. Fraudulent took services of internet and software's to gain knowledge of the security credentials like PIN and account number of the user. PIN of mostly users are based on their some personal information. Fraudulent perform different illegal activities like eavesdropping, man in the middle attack etc to listen the communication of devices and get the required data like user account number and password etc to perform the illegal activities. With the increase in security issues user's hesitation in using the services. This paper mainly focus minimize the security threat involving in online transaction. To maximize the security factor first step is to identify the legitimate user to carry out the legal transaction

Good security improves the trust of user's and increase the use of electronic commerce. Paper [1] describes a conceptual model that delineates the determinants of consumers' perceived security and perceived trust, as well as the effects of perceived security and perceived trust on the use of e-payment system.

This paper deals with authentication of user by tracing the Physical / MAC address of the machine. Mostly persons perform transaction from the same device like laptop and computers etc. OTP will be generated and send to user's mobile number to confirm the user if user provide the correct OTP system will authenticate the user. If user carry out the transaction from the same device system will authenticate the user by machine physical / MAC address and OTP will not generate.

2. Related Work

"Now a day's trend of online shopping is increasing day by day that gives opportunity to fraudulent to carry out the illegal activities easily. Paper [2] describes about the use of location of machine by placing the cookies on host computer. If transaction is not carry out from same device then it generate the OTP to identify the user. Paper [3] 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 [4] 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. Paper [5] purpose transmission of sensitive information like passwords etc by dividing the data into two sub sets and transfer through two different medium to secure the data over non-secure network and assemble the data at receiver side. Paper [6] identify the different type of threats / frauds like bankruptcy fraud, behavioral frauds and theft frauds etc. paper also purpose a different technologies to overcome the threats like neural networks and genetic algorithm etc.

3. Proposed Model

In this paper we implemented the security of web application for conducting online transaction by using two layer security mechanism.

1- **MAC Address based prevention**: when user first time initiates the transaction with server. Server will send the cookies to client computer for accessing the MAC address of the machine. The accessed MAC address will be saved and send to server computer through cookies. The saved MAC address on the server will be used for the comparison. When user initiates the transaction for the first time when MAC address is not available on the server site to authenticate the machine server will generate the OTP and send to user mobile number. If user provide the correct OTP. System recognize the user as legitimate user and proceed to normal transaction.

2- When user second time initiate the transaction from the same device it compare the MAC address of the machine stored on server. One time password will not generate if the MAC address of the machine is matched by the previously stored MAC address. But if the MAC address of the machine is not matched it will generate the OTP for authentication.

1. System Architecture

Proposed system architecture is explained here with the help of figure 1.

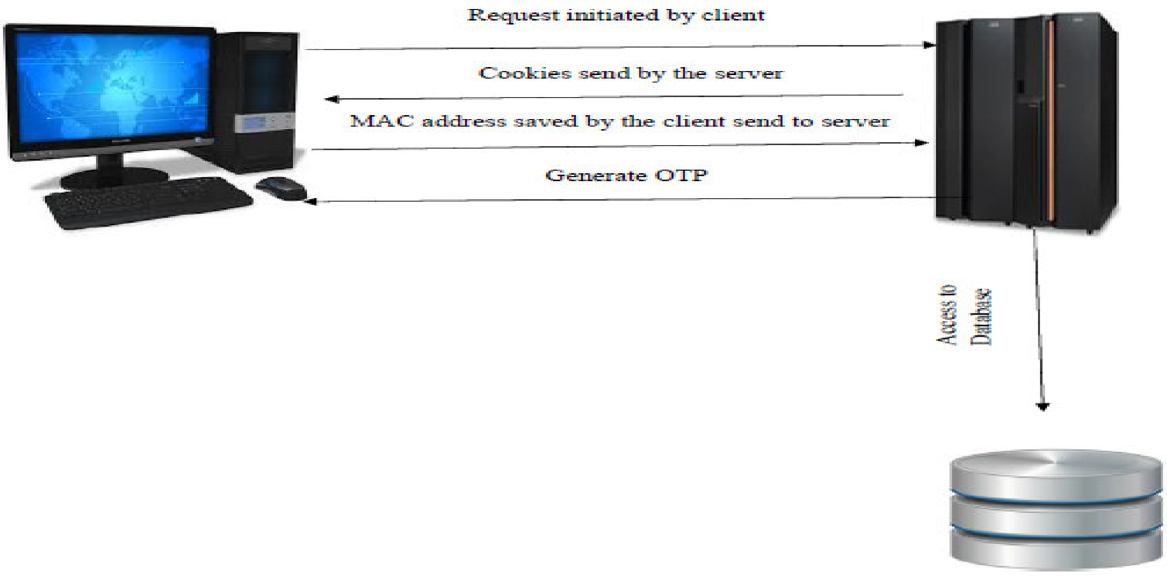
Request initiated by client
Cookies send by the server
MAC address saved by the client send to server
Generate OTP
Access to Database

Figure 1- Architecture of identifying legitimate user

Working of the paper with respect to the architecture draw above.

The proposed web application focused on prevention of online frauds occur by the fraudulent.

1- In first step when user initiate the request to webserver. Server sends cookies to user computer. Cookies save the MAC address of the client machine, and send the saved MAC address on server site

2- In second step if MAC address of the machine not match with the already present cookies then OTP will generate and send to user mobile number.

The proposed architecture provides the authentication of the user by keeping the saved MAC address of the machine with the view that user mostly use the same machine when conducting the transaction activity. If user used different machine it will save the address of the new machine and will generate OTP for the authentication, after completing the verification procedure further process will process to complete the transaction process. The proposed solution recognize the legitimate user by the authentication of the legitimate machine.

5- Conclusion

We have proposed the architecture that will provide a facility to recognize the legitimate user and keeps the fraudulent machines away from the system by saving the MAC address of the legitimate machine in the cookies and send over to server computer for keeping the record of legitimate machine. Saved MAC address of the machine on the server will help the system to recognize the user when user second time initiates the request of transaction. In case if MAC address is not saved or matched with the server MAC address system will generate the OTP and send to the mobile number provided by the client. OTP provided by the user verify the user and system will allow the client to complete the further procedure.

References

Kim, C., Tao, W., Shin, N., & Kim, K. (2009). Electronic Commerce Research and Applications An empirical study of customers ' perceptions of security and trust in e-payment systems. *ELECTRONIC COMMERCE RESEARCH AND APPLICATIONS*. http://doi.org/10.1016/j.elerap.2009.04.014

Amit Kulat1, Raghav Kulkarni2, Nagesh Bhagwat3, Kartik Desai4,"Prevention of Online Transaction Frauds Using OTP Generation Based on Dual Layer Security Mechanism" , International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 04| Apr -2016

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

Khan, A. A. (2013). Preventing Phishing Attacks using One Time Password and User Machine Identification, 68(3), 7–11.

Method, T. S. (2000). United States Patent [19] USER ' 5 PC.

Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. Banks and Bank Systems, 4(2), 57–68.