ISSN No: 2348-4845
International Journal & Magazine of Engineering,
Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Authentication Payment Method for E - Commerce

Bosubabu Sambana
MCA, M.Tech (CSE),
Assistant Professor, Department of Computer Science & Engineering,
Simhadhri Engineering College, Visakhapatnam, AP-531001, India.

Abstract :

Now a day's every one widely using Web. Internet is one of the part of our habitual daily life. Rapidly changes in Science and Technlogies.escapically our Banking/Financial system is also changes in last decade. Previous days banking operations is everything in manual but today every operation is done in online mode like RTGS and NEFT etc... In this case money transaction in various payment gateways is openly and secures mode. Sender and receiver both of them acceptance their payment Transaction. Sometimes third party user is easy to access original payment transactions. Unfortunately payment gateways are trapped in other (third) person. Security provides in existing gateways in various methods. In meanwhile I proposed new methods for overcome problem of unauthorized access. To give more security methods is involving in efficient payment transfer from fraud /suspicious attacks.

1)Keywords:
E-Commerce,Cryptography, Security, Authentication protocol, Transaction methods.

1. INTRODUCTION:

E-commerce, the security of various commerce applications is critical, on especially when it involves applications that deal with user sensitive data such as credit cards details, online payment details etc. The technique of using PIN for authentication has been shown to have memorability problems and overcome hidden problem Users adopt non-secure behaviors to circumvent those problems. To improve the usability and the security of authentication, alternative techniques have been suggested. PIN authentication remains as the primary login technique across many (or possibly all) implementations of e - banking. the security issues that arise with the growth in this field cannot be neglected.

Then problem is solved in in exiting methods available in cloud computing.

2. BACKGROUND:

2.1. E – Commerce :

E-commerce has allowed firms to establish a market presence, or to enhance an existing market position, by providing a cheaper and more efficient chain for their products or services through online and major marketing segments are B2B ,B2C, C2C,C2B.

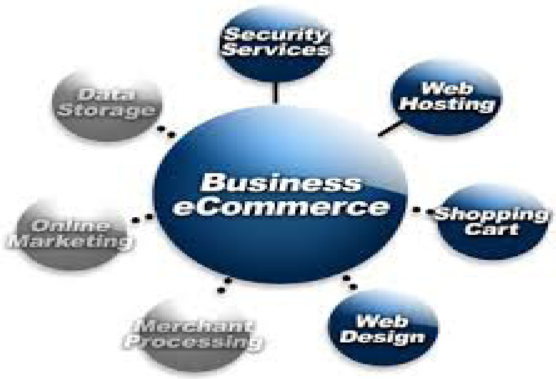


Figure 1: Basic View of .E-Commerce

2.2.Cryptography:

Secure stored information - regardless if access obtained. Secure transmitted information - regardless if transmission has been monitored

2.3.Security :

Information Security Threats are using the following
a)Internet Cryptography Techniques
b)Transport Layer Security
c)Application Layer Security
d)Server Proxies and Firewalls
e)Week resources in web sites/Hosts

2.4.Authentication Protocol :

A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

2.5.Payment :

A payment is the transfer of an item of value from one party (such as a person or Group) to another in exchange for the provision of goods, services or both, or to fulfill a legal obligation. The simplest and oldest form of payment is barter, the exchange of one good or service for another.

2.5.1 electronic Payment
2.5.2 M-Commerce
2.5.3 Secure gateway payment Transactions

Figure 2: Example of Payment Transaction

2.6.Payment Security:

Secure payment protocols are not necessarily tied to any of the aforementioned transport mechanisms, or even tied to a specific network architecture. These payment schemes exist in various degrees of implementation and secure transactions.

2.7.E-Commerce Applications:

Many more applications in e-commerce. like M-commerce, B2C,B2B,C2C etc. examples of e-commerce is M-commerce means mobile commerce, It is the buying and selling of goods and services through wireless handheld devices such as Cellular telephone and Personal Digital Assistants (PDAs). And Online money transactions etc.

3.RELATEDWORK:

3.1 Literature survey:

It involved many researching previous studies that were conducted in the area of authentication system , as well as reviewing what underlining existing system techniques using current existing authenticating systems to use.

4. EXISTING SYSTEM:

In e-commerce, Security threats of authentication systems can be classified into two categories: malicious and non-malicious. Malicious security threat is a view of state when a system or a user can login then user deficiency is being exploited and open by illegitimate users with an intention to do harms Phishing attacks and Hackers, for example, are a malicious activity made by attackers to trick legitimate users to give out their login passwords or personal information.

It is very case sensitive texts. The obtained information can be used to gain access into the user's accounts form original source. Other common forms of malicious attacks against password systems are dictionary attacks, keystroke logging, and shoulder-surfing and secrete messages. Dictionary attack is a type of password attack that uses words from dictionaries to crack a user‘s password. Users tend to choose weak passwords, then third party user(Un authorized) will easy to access this attack is most efficient against authentication systems that allow users to choose personalized passwords without policy restrictions. A more exhaustive version of dictionary attack is brute force attack.

Types of Security Threats:

•Unable to user server resources
•Type of DOS Attacks
•Web jacking –Web site vandalism
•TCP/IP SYN attack-Normal mode
•PING of Death
•Flood server with URL requests
•IP Cracking

Figure 3: Example of Simishing Attack

5. PROPOSED WORK:

The main objective of this work is to propose a secure platform- independent authentication and payment method for e-commerce applications free from Simishing attacks, Dictionary attacks and Malware and risk factors etc. Online payment/Debit/Credit card fraud is identity theft in its most simple and common form in view of Security socket layer. The objective is to enhance existing authentication and online/mobile payment method to prevent from credit card fraud attack.

Dictionary attack is a type of password attack that uses words from dictionaries to crack a user‘s password. Add pop-up Service blocking mechanism is implemented.Users tend to choose weak password, therefore this attack is most efficient against authentication systems that allow users to choose personalized passwords without policy restrictions. then this problem is easy rectifying using IP Security, and threat elimination searching algorithms ,frequent checking assenting and descending order of web server using Identity Based – Public key Infrastructure(IB-PKI).

DES algorithm and Internet Protocol(IP) address is using and maintain key management then diving partitions in Secure manner existing operations at easiest performance in safely without any consumption and error control.The authentication and Secure payment method tested through Android emulator. Coding done in Java through Eclipse Software and any other related software. And online Security providing through Hyper text transmission protocol security (https) using Secure Socket Layer (SSL).

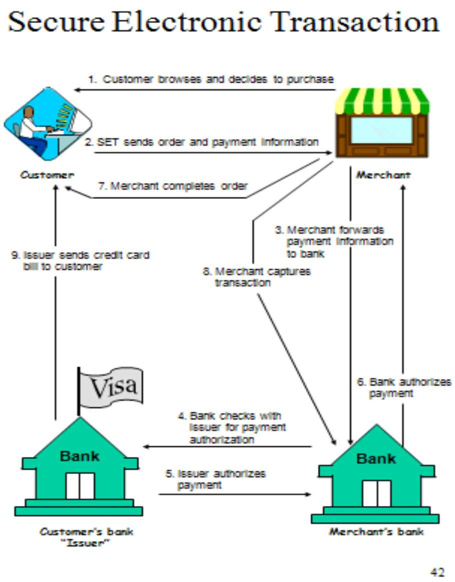

Secure Electronic Transaction
1. Customer browses and decides to purchase
2. SET sends order and payment information
Customer
Merchant
7. Merchant completes order
3. Merchant forwards payment information to bank
9. Issuer sends credit card bill to customer
8. Merchant captures transaction
6. Bank authorizes payment
Visa
4. Bank checks with Issuer for payment authorization
Bank
5. Issuer authorizes payment
Bank
Customer's bank "Issuer"
Merchant's bank
42

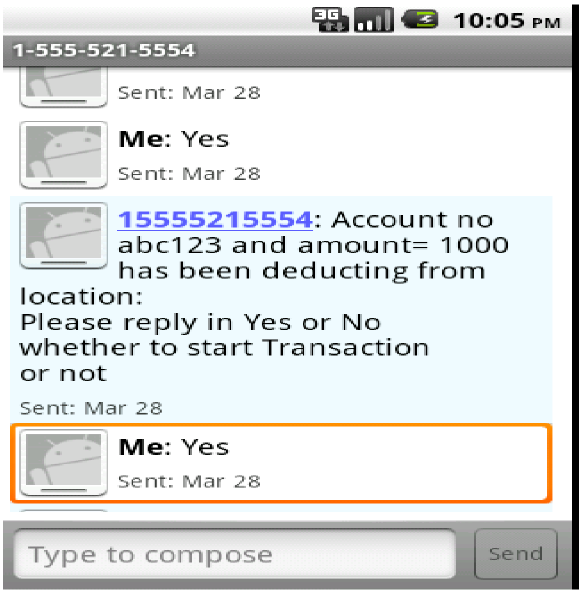
Figure 4: Secure Electronic Transaction

6.RESEARCH WORK AND SUPPORTING EXAMPLES:

The current online/mobile banking login method is PIN (Personal Identification Number) authentication. For a client to use online/mobile banking, the bank requires the client to register for the service. During Registration, the client receives (or provides) a four or five digit Personal Identification Number (PIN) as a password. To access the service, the client is required to enter the correct combination of his/her identification and the registered PIN to authenticate. Yet, this mechanism is unsatisfactory.

The use of a text-based password requires a trade-off between security and memorability; the trade-off arises from the limitation of human memory, and, as a result, passwords are easily forgotten. System security is often considered to be a technical issue. Before conducting a transaction, a client is required to login with a PIN and only a valid PIN code will grant the client access to the service.

In public key encryption and other authentication methods, proper authentication of user is missing. So security enhancement of mobile payment system is done in this work and as well as modification of current authentication system is done .



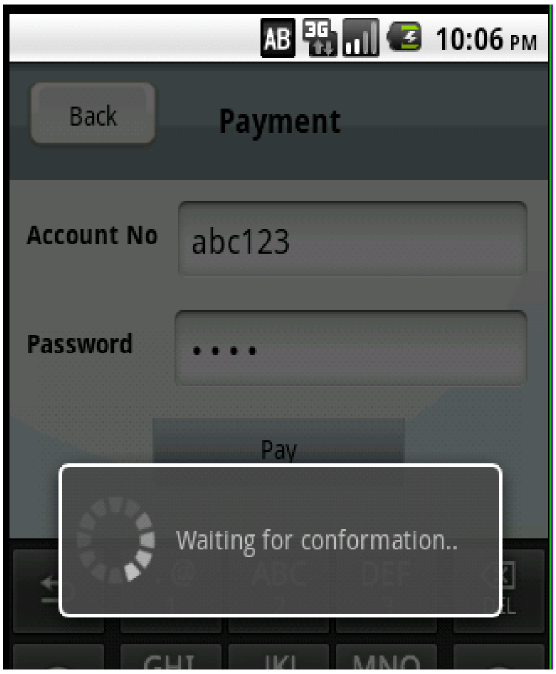
Sent: Mar 28

Me: Yes
Sent: Mar 28

15555215554: Account no abc123 and amount= 1000 has been deducting from location:
Please reply in Yes or No whether to start Transaction or not
Sent: Mar 28

Me: Yes
Sent: Mar 28

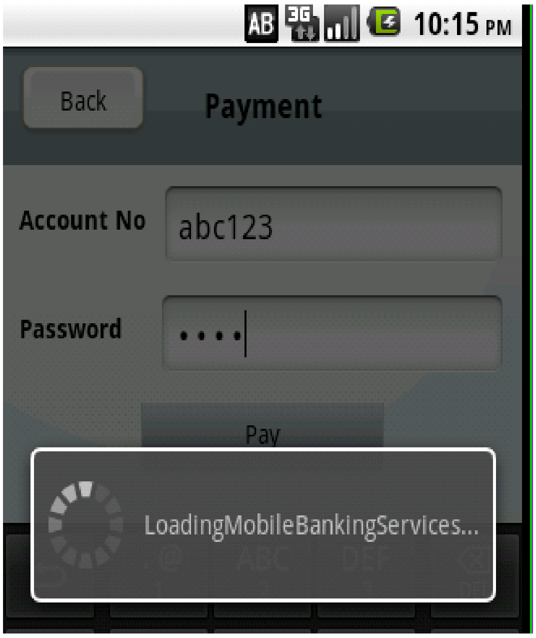
Figure 5. Based on user reply ‘Yes’via SMS



Account No: abc123
Password: ••••

Waiting for conformation..

Figure 6: Time given for confirmation (1minute)



Account No: abc123
Password: ••••

LoadingMobileBankingServices...

Figure 7: Successful Execution Start

7.EXPECTED RESULTS:

Steps:

1.Username and password will be provided for login.
2. User will enter the registered PIN to authenticate.
3. To prevent simishing, dictionary attacks from attacker , an SMS will be given whether to proceed with the transaction or not with suitable timing constraints(1 minute).(Reply in Y or N).
4. User has to reply with Y or N to enable transaction to execute.
5. SMS will be generated to genuine user to his/her registered mobile number .
6. If the attacker is going to do M-Commerce transaction then transaction will not execute.

8. CONCLUSION:

Now a days everyone widely used in e-Commerce through purchase anyone, In this mode every customer must knows minimum things. In this paper discuss about Secure payment transactions fully authenticated manner types and risk factors. Applications in e- commerce domain range from normal information consumption to high security financial electronic transactions. I hope this paper avoid minimum doubts in common man.

REFERENCES:

[1] http://www.android.com/
[2]http://www.androiddeveloper.com/
[3]http://developer.android.com/guide/topics/location/obtaini ng-user-location.html
[4]http://developer.android.com/guide/developing/tools/emul ator.html
[5]http://developer.android.com/resources/tutorials/hello World. html
[6]http://mobiforge.com/developing/story/sms-messagingandroid
[7]http://mobileprogramming.com/
[8] http://www.youtube.com/watch?v=EfTkDg9cC0c
[9]all images and Related Infoamation -https://www.google.com/

ACKNOWLEDGMENT:

This paper is Heartily Dedicated to my parents Sri.S.Dandasi & Smt.Janaki and My life Inspirer Eminent Scientist Sri.Dr.A.P.J.Adbulkalam.

Authors' Profiles:

Bosubabu Sambana working with as an Assistant Professor in Simhadhri College of Engineering ,Visakhapatnam. He completed Master Degree in Computer Applications and Master Degree in Computer Science & Engineering from JNT University-Kakinada.Andgra Pradesh, India. He has 3 years good teaching experience and having a good Knowledge on Computer Subjects. He is Published 3 Papers in Various International Journals. He is the member of MECS-PRESS, IAENG, IAAET and IJECSE.