

INTEGRATION OF SECURITY MECHANISM IN CLOUD BASED EWALLET

Nancy Malik, nancymalik339@gmail.com

Abstract: Electronic wallets system we have introduced several security mechanisms such as one time password, Session based security, Cookies based security, Capcha, IP authentication, Cryptography. Here we have discussed the threats to security of digital wallet. In this paper we have implemented access control mechanism to develop an electronic wallet based system where security is the major concern. This system is widely used in banking and financial institutions. The funds of people are stored in digital wallet and its security is must. In order to enhance the security of digital

ISSN : 2348-5612 © URR



Keywords: ECOMMERCE, DIGITAL WALLET, IP Authentication, Capcha, OTP.

[1] INTRODUCTION

E-wallet is a type of electronic card which is used for transactions made online through a computer or a smart phone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments. E-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc. For setting up an E-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user's information on the payment form. To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.



Fig 1 E-wallet

[2] THEME OF RESEARCH

The theme of this research is to secure the digital wallet system in ecommerce application and provide following features to the system.



1. Encode user data at the time of storing in database.
2. Decode data when user login to allow him to access his own account.
3. Restrict user to make transaction using pattern lock.
4. Making digital wallet available to him if we are correctly logged in as well as he has inserted correct pattern lock.
5. More over at the time of transaction from digital wallet one time password would be generated so that it could be access by user.

[3] PROPOSED WORK

The objective of proposed work is to make security of user data during storage.

1. Providing Security to the user data at the time of storing in database.
2. When user submits data from sign up form then the information is encrypted using cryptographic algorithm so that hacker could not access general information of user.
3. Allow user to access data when user login to allow him to access his own account.
4. Information of user is stored in hidden form so user should be able to access information at the time of login. When user successfully logs in then he could make the transaction to buy the product.
5. **Securing the transaction:**
A pattern lock is applied to restrict the user to make transaction. Once user enters valid pattern he would be eligible to perform transactions.
6. **Securing digital wallet:** Digital wallet allows user to buy the product from his own

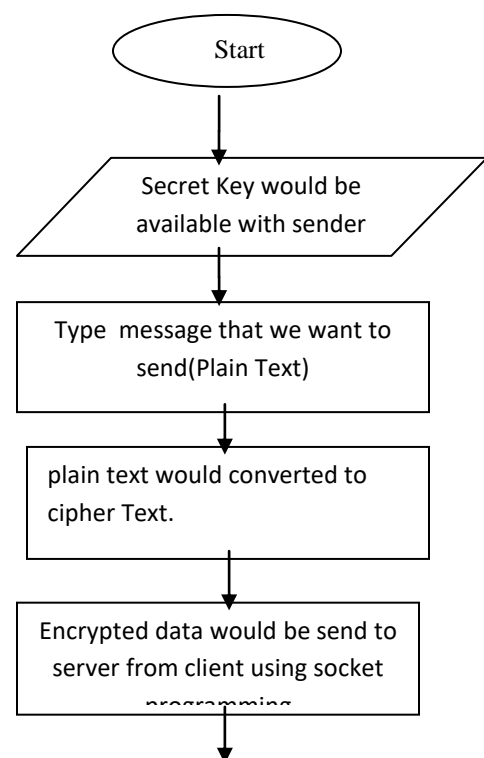
balance. In proposed work we are making digital wallet available to him if we is correctly logged in as well as he has inserted correct pattern lock.

7. One time password security during transaction
8. At the time of transaction from digital wallet one time password would be generated so that it could be access by user. This OTP could be send to him using email or sms.

[4] ENCRYPTION AND DECRYPTION

Encryption

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.



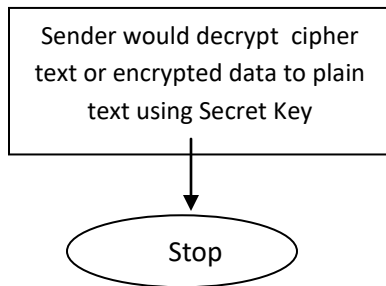


Fig 2 Encryption

Decryption

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

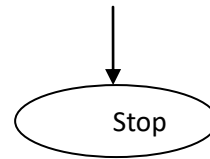
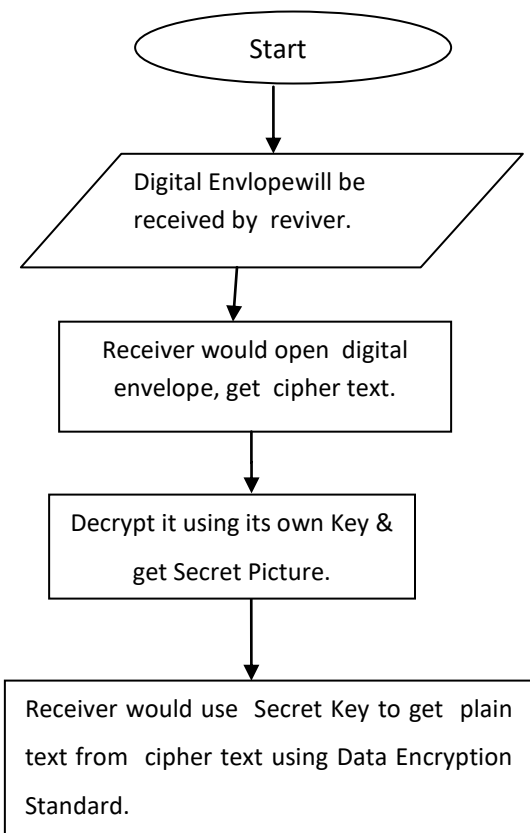


Fig 3 Decryption

[5] IMPLEMENTATION

In this section we are discussing the implementation of electronic wallet system. This system is beneficial for banking and financial sector. User once login using this username and password.

A session is created for him then he becomes able to access the resources as well as he could modify his personal details in this panel.

Customers are allowed to edit profile online along with management of login password as well as transaction password. If Customer need to view account details then he use manage login password. And if he want to make online transaction then he use transaction password.

This is the admin panel form from which the products are added but user list, list of transaction, list of orders can be obtained as output module as these modules represent the results.

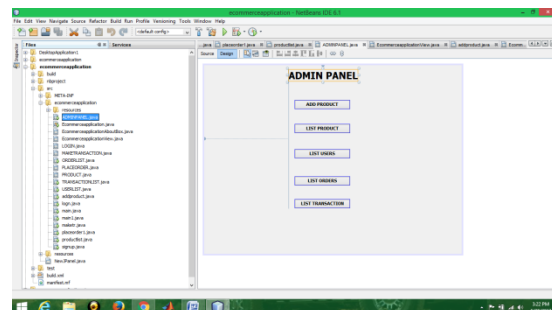


Fig 4 Admin Panel



When the admin clicks on Add Product, he is allowed to add products to his cart.

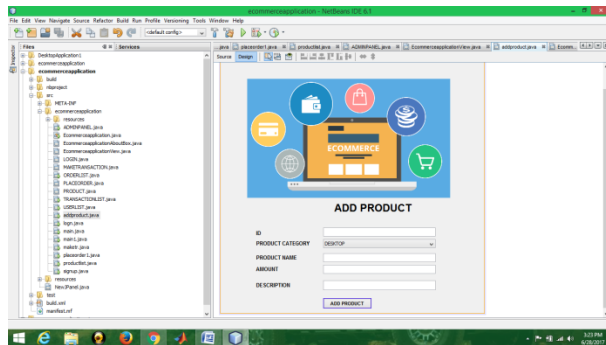


Fig 5 Add Product

The following form is used to take input from user in order to place order.

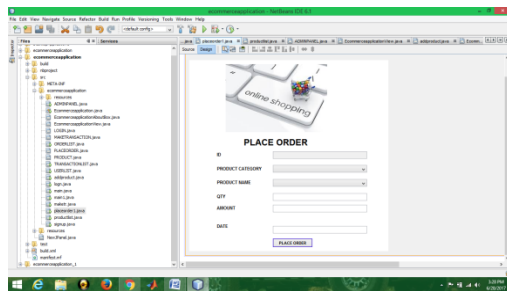


Fig 6 Place order form

The person who has logged in could login from login panel using the following panel.

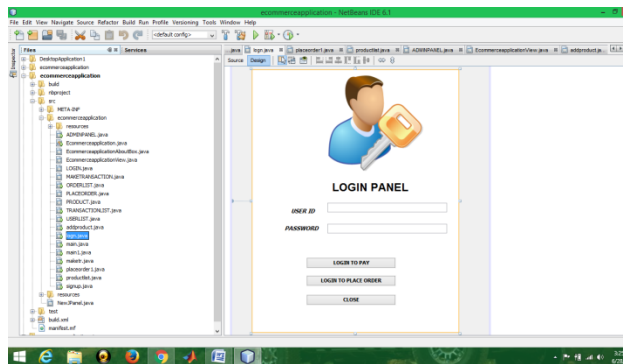


Fig 7 Login Panel

The following window represent the make transaction module.

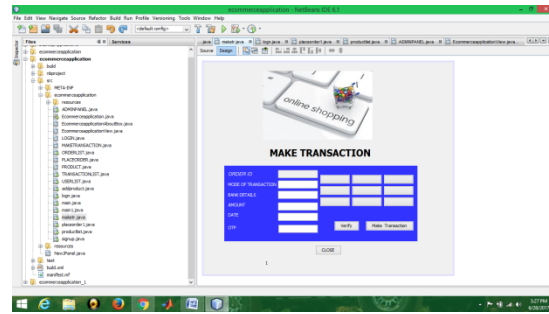


Fig 8 Make Transaction Module

Outputs

The following windows are accessing data from Remote Database Server. View product list, View Invoice, View list of orders as well as transaction are listed with the help of the buttons on Admin panel.

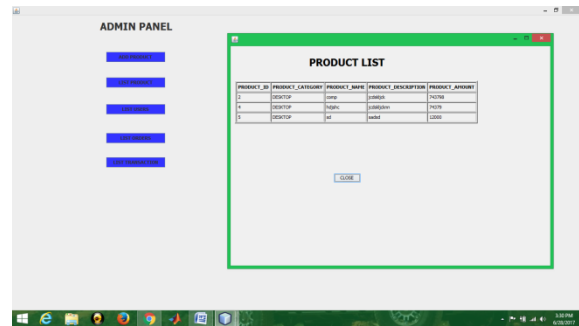


Fig 9 Product list

The Size of traditional ecommerce application is approximately 30 mega bytes but proposed application size is approximately 1 mega byte.

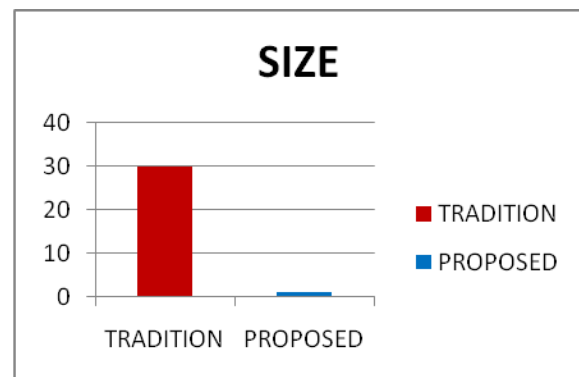


Fig 10 Comparative study of size of Traditional and Proposed work



The application is accessible to more users as compared to traditional system..

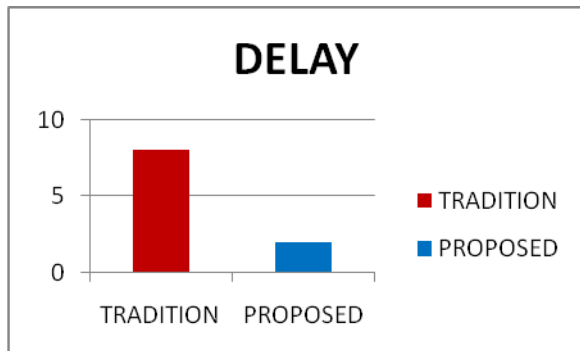


Fig 11 Comparative study of delay in tradition and proposed work

Proposed system is light weighted as it is using swings for graphical user interface but the tradition systems are heavy weighted. So the performance of proposed system is approximately 4 times better than traditional systems

[6] SCOPE OF RESEARCH

Internet technology is changing way people live, the way they compute, and the way they conduct business. Nothing has changed more than the way applications are designed, built, and distributed. Web technology has brought us to a new world of software engineering, with new techniques, new tools, and a new design and deployment environment. Technology brings challenges, including competing architectures, platforms, and tools, most of which are still evolving. Developers are being challenged to explore new methodologies and best practices to address World Wide Web-specific development issues, such as maintenance of content-rich Web applications, security, application scalability, and an ever-increasing demand for fast system deployment by customers. Web application is an essential

element in E-commerce. They offer system developers many challenges and opportunities. Design and implementation of successful Web application require a disciplined approach that takes organization's long-term development into consideration. Instead of viewing an application as having a start and finish, developers should treat Web applications as living entities, constantly adjusting to the changing business environment.

[7] CONCLUSION

The proposed system is far better than the existing e-Wallet application. Here we have introduced security at the registration level as well as at transaction time. There is always threat to digital wallet due to hackers. We know that during online transaction the security threat get increased. So this research is an attempt to make e-commerce system more secure and prevent the unauthentic operations. System would definitely help in securing e-commerce transaction. There may be two cases of online transaction. One is the situation when users pay for product from his bank account. Other situation is when user pays for product from his digital wallet. There is always risk to such situation as banking sites have their own security mechanisms but the security of users amount in digital wallet is responsible is provided by its makers. Here we have made such digital wallet and secure it using pattern lock and one time password facility.

References

1. Umair Mukhtar Ahmed Naushahi "Profile Based Access Control in case of Cloud Computing Environments with applications in Health Care Systems"



2. Prosunjit Biswas, Ravi Sandhu(B), And Ram Krishnan “Uni-Arbac: A Unified Administrative Model For Role-Based Access Control”
3. Roszelinda Khalid, Zuriati Ahmad Zukarnain, zurina Mohd Hanapi, Mohamad Afendee Mohamed, “Authentication Mechanism in case of Cloud Network And Its Fitness With Quantum Key Distribution Protocol: A Survey” , 2015.
4. Sneha Warang, “Role Based Access Control Model For Cloud Computing Using Rbe Scheme” ,2016
5. Christopher Alm, Michael Drouineaud, Ute Faltin, Karsten Sohr, And Ruben Wolf “A Classification Framework Designed For Advanced Role-Based Access Control Models And Mechanisms”
6. Haodong wang & qun, “Distributed user access control in sensor networks”
7. Multi-factor authentication protection framework in cloud computing by prachi soni, (asst. Prof.) Monali sahoo 2015
8. Peter mill & Tim grance, “The NIST Definition of Cloud Computing”, 2011, National Institute of Standards & Technology ,Gaithersburg,MD 20899-8930, NIST Special Publication 800-145.
9. Ellen Messmer, “New security demands arising for virtualization, cloud computing”, 2011, security-demands-arising-for-virtualization—cloud computing.html
10. .Sumedha Kaushik & Ankur Singhal, “Network Security Using Cryptographic Techniques” 2012, volume 2, Issue 12.
11. Charles Miers, Fernando Redigolo & Marcos Simplicio, “A quantitative analysis of current security concerns & solutions for cloud computing ”, 2012, Journal of Cloud Computing: Advances, Systems & Applications electronic version of this article is
12. Rabi Prasad Padhay, “An Enterprise Cloud Model for Optimizing IT Infrastructure”, 2012, International Journal of Cloud Computing & Services Science (IJ-CLOSER) Vol.1,
13. Nelson Gonzalez, et. al. , “A quantitative analysis of current security concerns & solutions for cloud computing ”, 2012, Journal of Cloud Computing: Advances, Systems & Applications doi:10.1186/2192-113X-1-11The electronic version of this article is complete one & could be found online
14. .CSA “Security Guidance for Critical Areas of Focus in Cloud Computing”, (2009), Tech. rep., Cloud Security Alliance.
15. Rowstron & P. Druschel. Pastry: Scalable, distributed object location & routing for large-scale peer-to-peer systems. Accepted for Middleware, 2001, 2001.
16. Ben Y. Zhao, John Kubiawicz, & Anthony Joseph. Tapestry: an infrastructure for fault tolerant wide-area location & routing. April 2001.
17. Andr´ea W. Richa C. Greg Plaxton, Rajmohan Rajaraman. Accessing nearby copies of replicated objects in a distributed environment. In Proceedings of ACM SPAA, pages 311– 320, June 1997.



-
18. Stefan Saroiu, P. Krishna Gummadi & Steven D. Gribble. A Measurement Study of Peer-to- Peer File Sharing Systems. July 2001.
 19. Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, & Hari Balakrishnan. Chord: A peer-to-peer lookup service for internet applications. August 2001.