



## INTEGRATION OF ACCESS CONTROL MECHANISM IN CLOUD BASED EWALLET

*N.Ch. Ravi<sup>1</sup> Associate Professor, Dept of CSE, SIET, Hyderabad (ravi@saimail.com)*

**Abstract:** 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 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.

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

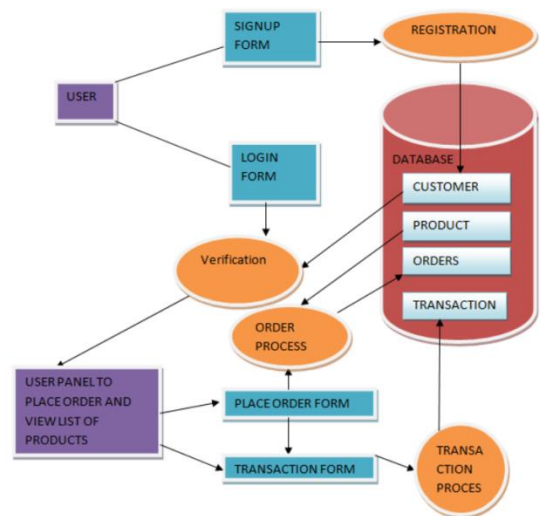
### [1] INTRODUCTION

There are lots of electronic wallet bases systems in market where people keep their digital cash. Here they make purchase of online recharge using this amount. Some time in case of banks the same wallets are used to make online fixed deposits or recurring deposits.

There are lots of issues with existing ecommerce system that are used to buy online products. Usually buyer registers themselves and place order. Their orders are getting paid using net banking or credit card /debit card or their digital wallet.

There are always threats to the existing digital wallet system from hacker. Someone may hack others digital wallet in order to buy product. The objective of our research is to enhance the security of digital wallet from external attacks. There is always threat to the personal details of user that are stored in remote database. Their information must be

in such form that other person could not access it.



**Fig 1.** Existing Electronic wallet Model

### [2] OBJECTIVE OF RESEACH

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

1. Encode the 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 the user to make transaction using pattern lock.
4. Making digital wallet available to him if we is 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] PROPOSED MODEL

In proposed model the security mechanisms to secure the digital wallet of customer are introduced such as one time password, storing encoded data in database and applying pattern lock on transaction to make them secure.

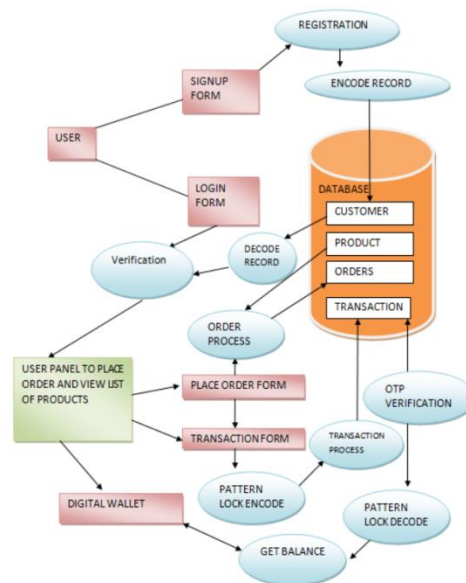


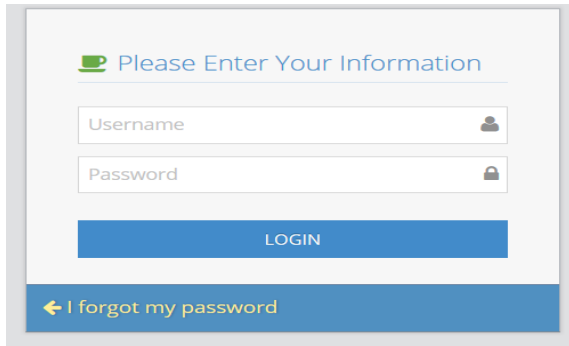
Fig 2 Proposed Models

### [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.

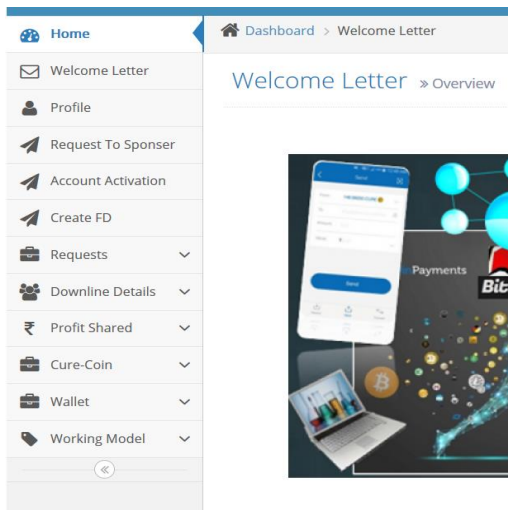


**Fig 3** Login for customer

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.

The user is allowed to invest online in fixed deposit and we could also view his account statement.

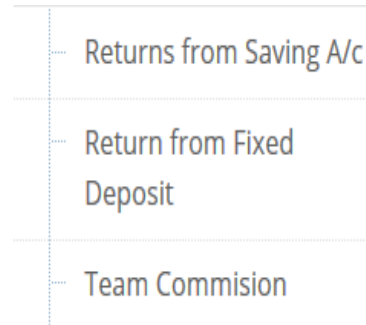
Summary of return from saving and summary of return from fixed deposit are shown in such system.



**Fig 4** Customer Panel

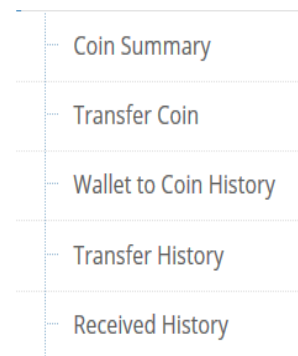
In customer panel user could select profit shared to get details of return from saving and return from fixed deposit and team commission.

Here the list of return from saving, return from fixed deposit and team commission id displayed.



**Fig 5** Profit shared details

Following menu represent the summary of coin as well as wallet coin history, transfer history, received history.



**Fig 6** Transaction of coin

Users are allowed to make fixed deposit from the existing wallet balance in order to get additional returns.



- Home
- Welcome Letter
- Profile
- Request To Sponser
- Account Activation
- Create FD
- Requests
- Downline Details
- Profit Shared
- Cure-Coin
- Wallet
- Working Model

### Create Fixed Deposit

Available Balance:432648

ID

AMOUNT

DESCRIPTION

**Fig 7** Create Fixed Deposit

Customer could make activation of his own account using balance fund in different packages.

### ACCOUNT ACTIVATION

Balance 432648

FROM\_ID

TO\_ID

AMOUNT

INVESTMENT

TYPE

DESCRIPTION

### ★ Special Offer

10,000 COIN  20,000 COIN

Return on Saving 0.5%

Return on Fd 1%

**Fig 8** Account Activation

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.

- 
- 
- 
-



Fig 9 Account Setting

## [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 sahuo 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.