International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

UPI Seamless Payment Transaction Using Neuro Fuzzy Technique

A.AKILAN[1], A.N.ABIRAMA VALLI[2], R.SURYA KALA[3]

Assistant Professor, Dept. of Computer Science and Engineering, MRK Institute of Technology, Kattumannarkoil, Cuddalore, Tamil Nadu, India[1]

Bachelor of Computer Science and Engineering, MRK Institute of Technology, Kattumannarkoil, Cuddalore, Tamil Nadu, India[2,3]

ABSTRACT: In today's world, banking plays an indispensable role among all people. If the banking is user friendly then it would benefit all users. So this situation has forced us to move towards mobile banking system. Emerging technologies have supported people with mobile devices and data connections. Mobile banking applications provide an easy door-step solution for customers. UPI is one of the mobile based applications which facilitate online transaction. UPI uses PIN to complete the transaction. The PIN entry can be noticed by nearby adversaries. Hence, a direct observation attack based on shoulder surfing becomes a great concern. In our proposed method, we strongly focus on security by proposing a novel approach called Covert Attentional Shoulder Surfing(CASS). In our proposal, we also implement the RNN Classifiers to analyze the behavior characteristics of the user to detect or to resist access by unauthorized people. Our solution or model is designed to be used in all platforms (platform Independent) like Android, IOS and other mobile platforms.

KEYWORD: Mobile Payment Application, UPI PIN, Shoulder Surfing, CASS, RNN Classifier.

I.INTRODUCTION

Micropayment systems offer the end user the chance to purchase through a mobile device a great variety of very low-value online services (news, apps, games, photos, movies etc.) for a small amount of money.

The very big idea of our proposal which we tend to focus in this paper is to prevent Shoulder Surfing (shoulder surfing is a technique used to obtain information such as personal identification numbers, passwords and other confidential data by looking over the user's shoulder) and Unusual Transactions. Our solution is to build a more secure mobile transaction application using the two approaches-Covert Attentional Security Surfing and detection of Unusual payments using RNN classifiers. In case, if any fraudulency is detected using the two approaches, then our solution also ensures that the user is aware of the insecure attacks by receiving an alert message. Google Pay, Phonepe and other mobile transaction applications are the best competitors for us. Our solution is to provide an alternative mobile application with enhanced security, which is a challenging factor and we aim to make it better than other applications in terms of security.

MICROPAYMENT SYSTEM:

Micropayment System is one of the research areas in electronic commerce. It's a system that allows for the payment of very low cost items online. For any commercial system to thrive, trust and security of the system must be guaranteed and the security is the basis of the trust. Trust in a payment system is a pre-condition for using the system.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

II.SYSTEM ARCHITECTURE

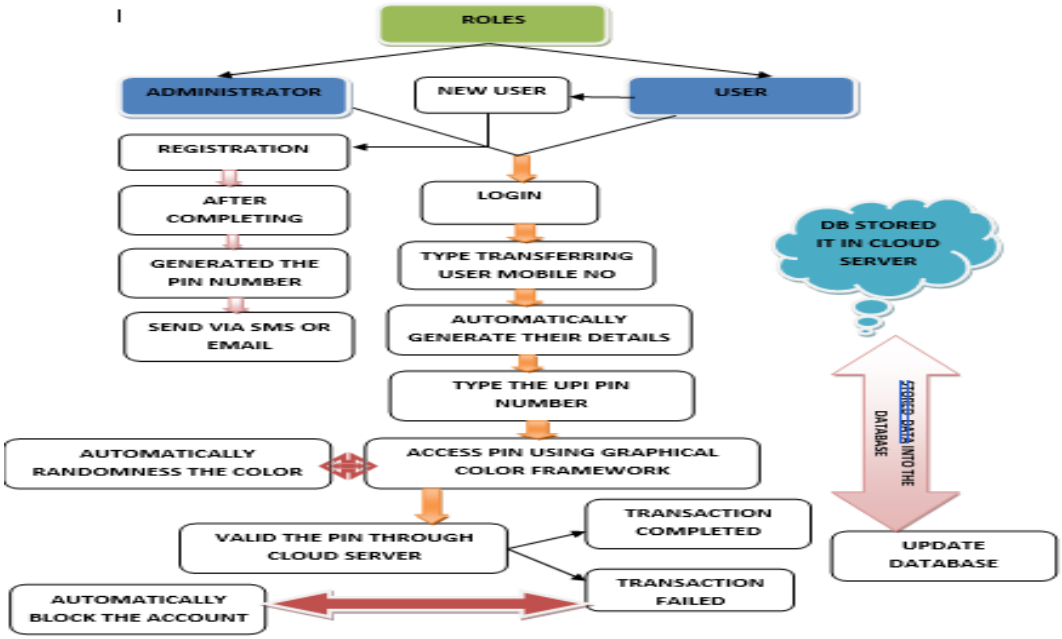


Figure 1.System Architecture

III.PROPOSED METHODOLOGY

In the proposed system, the product can be used in commercial transaction such as an interaction between two or more parties in which goods, services or something of value is exchanged for some type of remuneration and personal transactions (Person-to-person payments (P2P) is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone). Since our solution supports platform independency, it would really benefit a large number of users.

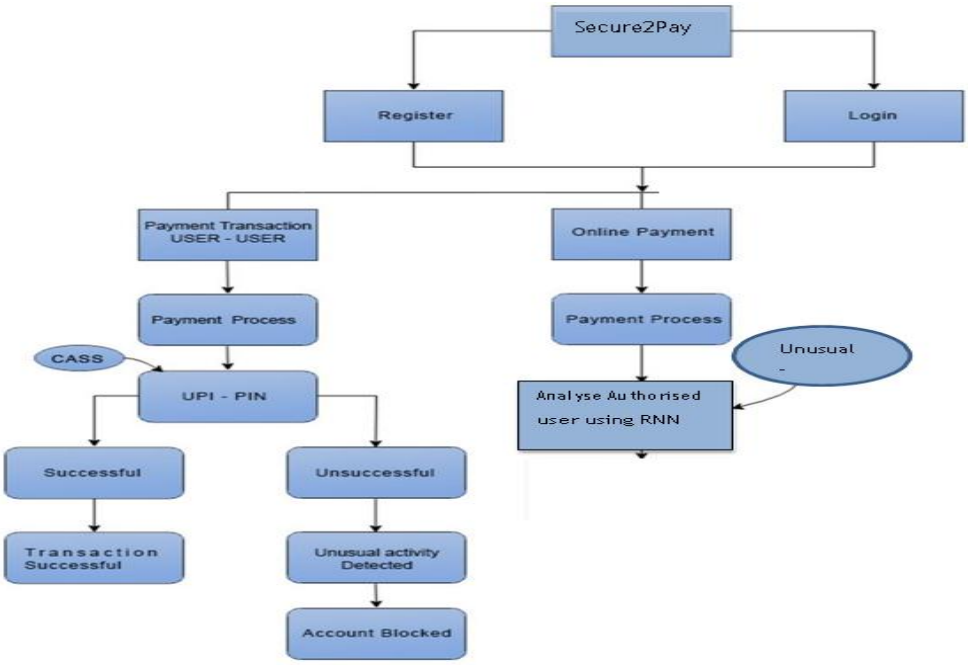


Figure 2. Process Flow Diagram

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

SYSTEM MODULES:

- Registration Phase
- Login
- Money Transaction
- PIN Entry
- View Transaction Details
- View Account Summary

1. Registration Phase

This is the initial phase in the payment system .To use the system, the user first have to register to it. For registering into the system the user have to give the mobile number which is linked to the a/c no and have to give the corresponding a/c no and a password for the account, additional details as email id for receiving OTP.

2. Login

In this phase once the user got registered into the payment system, he/she can login into their account by proceeding the login procedure. user has to provide their registered account phone number and password to login. which they have created in the registration phase .

3. Money Transaction

In this user can perform money transaction by selecting the corresponding account they would like to perform transaction. After providing the receiver account and the description the sender has to press the "pay" button. Once the user completed it UPI pin entry window will appear .

4. PIN Entry

The improved method runs as follows: The system displays a set of ten digits, $A = \{0, \cdots, 9\}$, on the regular numeric keypad with two split colors, chosen from P, in each numeric key; and the four colour keys below.

5. View Account Summary

In this phase user can view the current account details.

III.IMPLEMENTATION

In this paper we have proposed a system in which,the product can be used in commercial transaction such as an interaction between two or more parties in which goods, services or something of value is exchanged for some type of remuneration and personal transactions (Person-to-person payments (P2P) is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone). Since our solution supports platform independency, it would really benefit a large number of users.

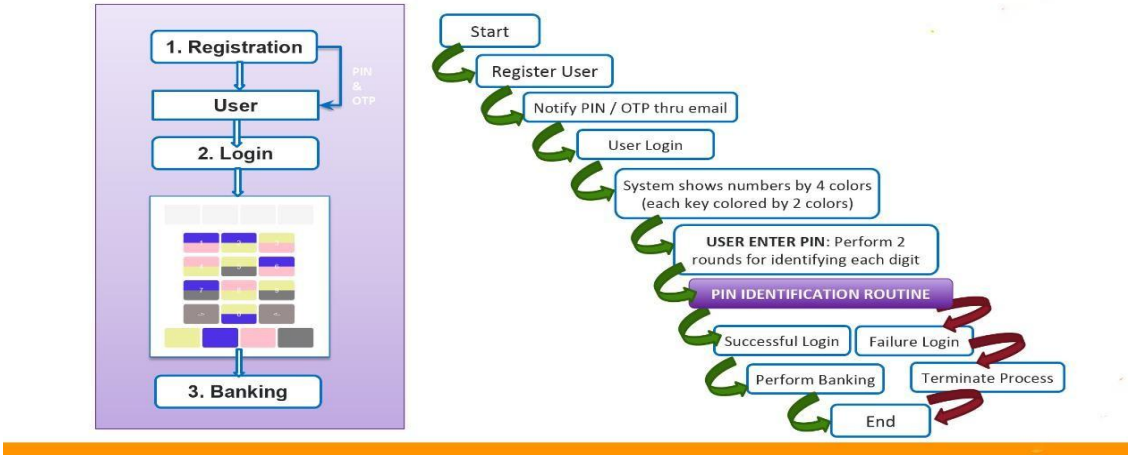


Figure 3. Pictorial view of implementation

In this solution, we have provided various features for the UPI users so as to benefit them with the seamless transaction. So to assist this, we provide with the following features,

- **Behavior Analyses using RNN classifiers:**

The gesture data capturing information reflects the way users interact with their mobile devices. This data is stored

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

and analyzed and if any mismatch is found with the behavioral characteristics, fraudulency is detected and alert message is automatically sent.

- **Covert Attentional Shoulder Surfing(CASS) :**

When a user enters a PIN, there is a chance of direct observation attack by the intruder. So this becomes a great concern and CASS plays a vital role in preventing the shoulder surfing attack.

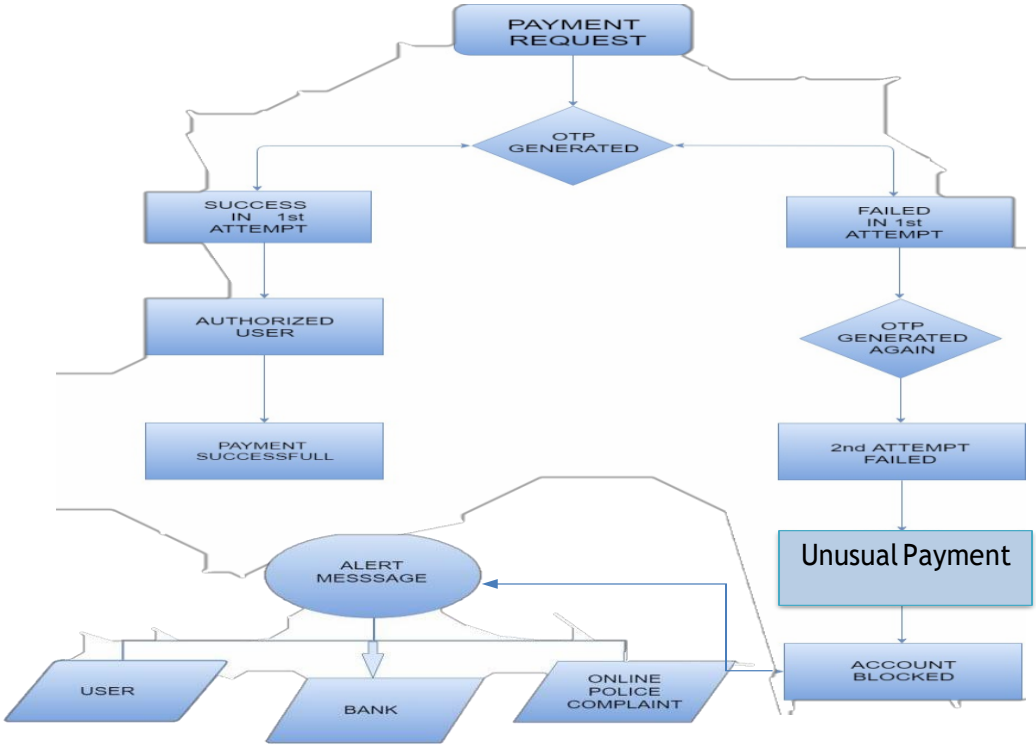
- **Platform Independent:**

When a product is supported by all the mobile platforms, then it would facilitate most of the users to easily connect with the mobile transaction applications from any platform.

UNUSUAL ONLINE PAYMENT DETECTION

When there is a large amount to be transacted, it is important to ensure authorization. So,

Figure 4. Flow Diagram for Unusual online payment detection



To confirm this huge transaction is performed by an authorized user, RNN classifiers has been implemented. This analyses the previous transaction history. If the amount to be transacted exceeds the range, then to verify the exact authorization, an OTP is sent to the user's mobile number. Entering a wrong OTP will identify unusual transaction and the process will be terminated. Hence Unusual Transactions can be prevented.

IV.CONCLUSION

The security password techniques are susceptible to neck browsing, many neck browsing proof color palette authentication password techniques have been suggested. However, as most users are more familiar with textual security passwords than pure visual security passwords, text-based visual security password techniques have been suggested. Unfortunately, none of existing text-based neck browsing proof visual security password techniques is both secure and efficient enough. In this paper, we propose an improved text-based neck browsing proof visual security password plan by using colors. In the suggested plan, the user can easily and efficiently sign in system. Next, we evaluate the security and functionality of the suggested plan, and show the resistance of the suggested plan to neck browsing and random sign in.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

REFERENCES

[1] A. Akavia, S. Goldwasser, And V. Vaikuntanathan, "Simultaneous Hardcore Bits And Cryptography Against Memory Attacks," In Proc. 6th Theory Cryptography Conf., 2009, Pp. 474–495.

[2] S. S. Al-Riyami And K. G. Paterson, "Certificateless Public Key Cryptography," In Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, Pp. 452–473.

[3] M. H. Au, J. K. Liu, W. Susilo, And T. H. Yuen, "Certificate Based (Linkable) Ring Signature," In Proc. Inf. Security Practice Experience Conf., 2007, Pp. 79–92.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, And G. Yang, "Malicious Kgc Attacks In Certificateless Cryptography," In Proc. 2nd Acm Symp. Inf., Comput. Commun. Security, 2007, Pp. 302–311.

[5] S. Habib, S. Hauke, S. Ries, And M. Mhlhuser, "Trust As A Facilitator In Cloud Computing: A Survey," Journal Of Cloud Computing, Vol. 1, No. 1, 2012.