A Smart Mobile Banking Security Using Behavioral Context

S.Geetha, J.Mary Revathy, S.Ashvini, Dr. J. Madhusudanan, Dr. V. Prasanna Venkatesan

***Abstract*— The development in pervasive systems has converted the whole world into a smart environment. Everywhere we go people are interconnected with smart applications and are communicating in a smart space. This development in the pervasive systems has also impacted the banking sector. All banks are upgrading their systems to a smart environment and one among this is the mobile banking application. Through mobile banking without more invest in the technological background banks can reach more number of customers. This adds more advantage to the banking industry. The customers can do their transactions through their smart phones by which they can save their time and whenever they need to do transactions they can do it from their current location. In this paper we have concentrated on the location context. More issues arise when the customers use their mobile transactions from a different location, so to provide a better solution to this issue an location authentication mechanism is been implemented in the proposed work. Authentication is done with two-factor mechanism to produce a more secured transaction to the customers.**

***Index Terms*— Banking Security, Behavioral Context, Pervasive Security, Smart Banking, Smart Systems.**

I. INTRODUCTION

As the current world has been adopted by smart environment, the transactions done through online is also been made smart by providing mobile banking services to the customers. But security is considered as a major issue for many banks to introduce mobile banking applications. Customers make use their smart phones for purchases and fund transfers so there is more risk of data and information loss in the network. Since the smart phones are connected through a wireless network there are more chances of information to be tracked and spoofed by unauthorized person. Though better authentication and authorization mechanisms are followed by banks still there is a lack in the security of the mobile banking services. To help banks with the gap in the security concern and to provide a smart security application for mobile banking a model is been proposed. The model follows regular two factor authentication for identity theft and a behavioral authentication method for identifying the man-in-the middle attacks. In addition to this features location of the mobile transaction is also been verified to provide a more secured transaction for the customers. If the location of the user is different than he has to enter the OTP sent to his mobile along with the finger print authentication. As a result a more secured authenticated transaction can be provided.

II. LITEARTURE REVIEW

According to Cognizant’s Report [1], an increasing number of individuals are using mobile applications compared with traditional desktop/Web-based applications. A research report from ComScore shows that apps account for a majority of consumers’ mobile minutes, and 80% of their media time is spent on app usage compared with only 20% on Web browsers. The MQA survey revealed that security remains a major concern in adopting m-banking. Approximately 72% of respondents said they worry about the security of accessing financial data on a mobile device. Based on ISACA [2], Mobile banking provides an opportunity to reach a large proportion of the earth’s population without the need for a large investment in technology. Smartphone capabilities such as geolocation and Internet connection can be used to improve the security of the transaction and improve the capabilities of detecting fraud. The use of smart phones counters skimming methods that account for a significant portion of card fraud. Remote wipe functionality is widely available on smart phones and tablet devices either by default or as an application.

III. PROPOSED SYSTEM

The literature survey clearly shows the impact of the mobile devices in the day to day bank transactions. As the world has become smarter the online payments and purchases has also been converted into a smarter environment. Without using the banks browsers the customers use the mobile banking app for doing their payments online easily. With this increase in the mobile banking usage of the customers more security mechanisms is to be employed for the system to provide a secured service to the customers. The Proposed System consists of behavioral authentication to identify the context in which the user is working. Based on the location context of the mobile the security mechanism will vary. If a customer performs his transaction from a different location other than his home town then the authentication will be a two-factor authentication. To proceed with the transaction he has to enter the OTP along with his fingerprint, so that a more secured authentication can be ensured by the banks.

S.Geetha, Research Scholar, Department Of Banking Technology, Pondicherry University.

J.Mary Revathy, PG Student, Department Of Banking Technology, Pondicherry University.

S.Ashvini, PG Student, Department Of Banking Technology, Pondicherry University.

Dr. J. Madhusudanan, Associate Professor, Department of Computer Science and Engineering,Sri Manakula Vinayagar Engineering College,Madagadipet, Puducherry.

Dr. V. Prasanna Venkatesan, Associate Professor, Department Of Banking Technology, Pondicherry University.

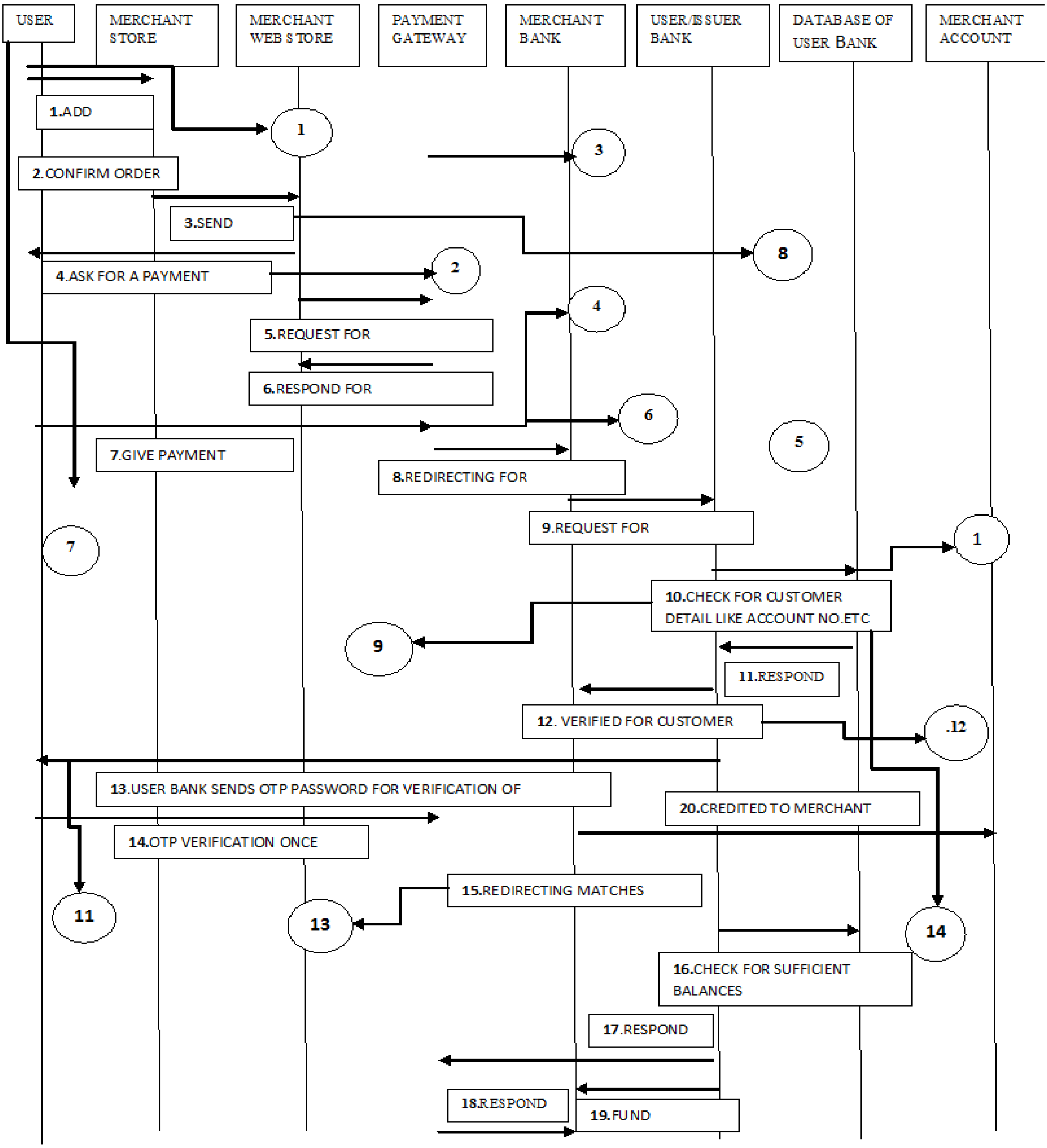


FIGURE 1: PROPOSED SYSTEM FOR MOBILE FUND TRANSFER

IV. IDENTIFIED THREATS

1. Malicious coded attack: virus, worms, Trojan horse, logic bombs

2. Cookie side jacking: sniffing data packets, session cookies, user session

3. Evil twin attack: rogue Wi-Fi access point, phishing attacks, tainted as a legitimate

4. Blue jacking: unsolicited message Trojan horse program

5. Syn flooding: intruder as a legitimate, Syn acknowledge, overloading memory

6. Session fixation attacks

7. **IP spoofing, Data packet sniffing, Port scanning, Trapdoors/Backdoors**

8. Man in the browser malware

9. Denial of service: Malware attacks hijacking

10. Pod slurping: Data theft from data storage device

11. Cross site scripting: Hijack an account, spread web worms, access browser history, browser control

12. Ping of death: TCP/IP data packet interception

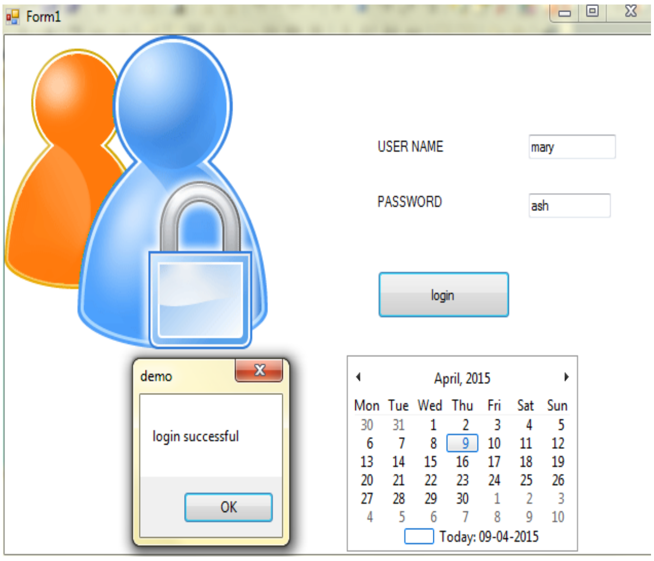
13. Sniffing data: Malicious actor-> intercept data

14. SQL injection attack

The proposed system is based on an electronic payment system and its threats and vulnerabilities. Electronic payment system is a system which helps the customer or user to make online payment for their shopping. An attacker who has gained access to data paths in your network to listen in or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem the administrators face in an enterprise. Only when the environment becomes smart, security will be stronger.

V. IMPLEMENTATION

STEP 1: Login with username and password



USER NAME mary

PASSWORD ash

demo

login successful

April, 2015

Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Today: 09-04-2015

FIGURE 2: Login Screen

STEP 2: Mobile banking main menu

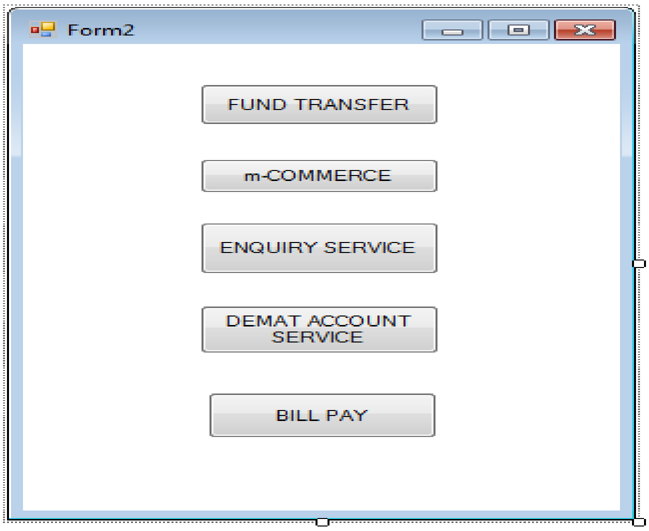
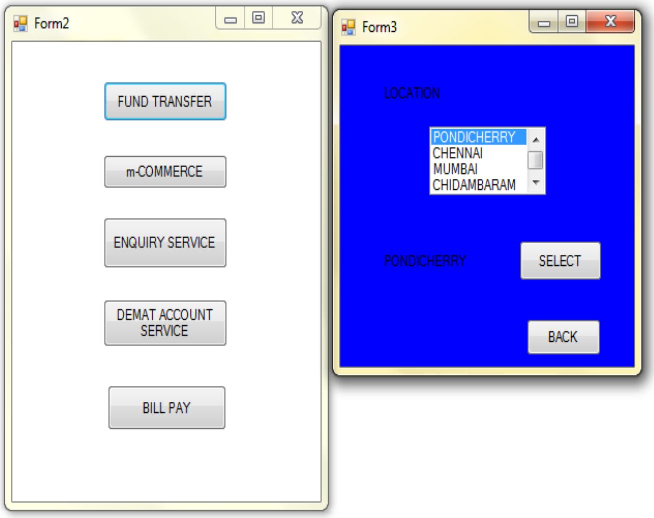


FIGURE 3: Main Menu of the Mobile Application

STEP3: If fund transfer is selected, following form will open. User should select his current location. If the selected location is preferred location form will change into blue colour. By default Chennai and Pondicherry is taken as preferred location



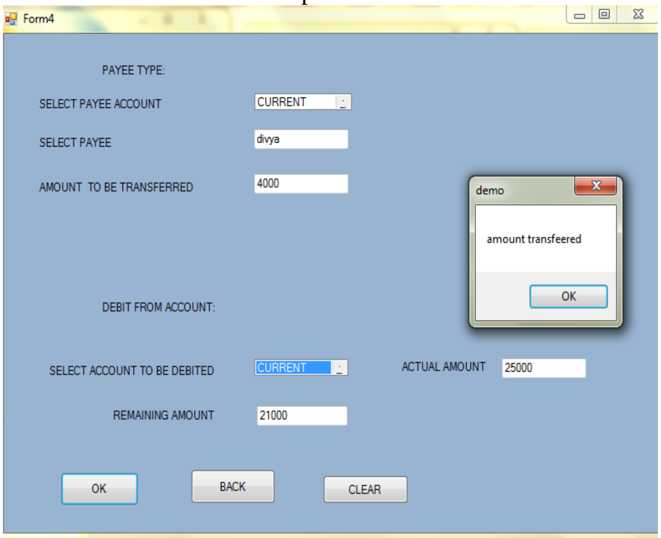
LOCATION

PONDICHERRY
CHENNAI
MUMBAI
CHIDAMBARAM

PONDICHERRY

FIGURE 4: Form to select Location of transaction

STEP 4: If the selected location is Chennai or Pondicherry then fund transfer form be opened



PAYEE TYPE:

SELECT PAYEE ACCOUNT CURRENT

SELECT PAYEE divya

AMOUNT TO BE TRANSFERRED 4000

DEBIT FROM ACCOUNT:

SELECT ACCOUNT TO BE DEBITED CURRENT

ACTUAL AMOUNT 25000

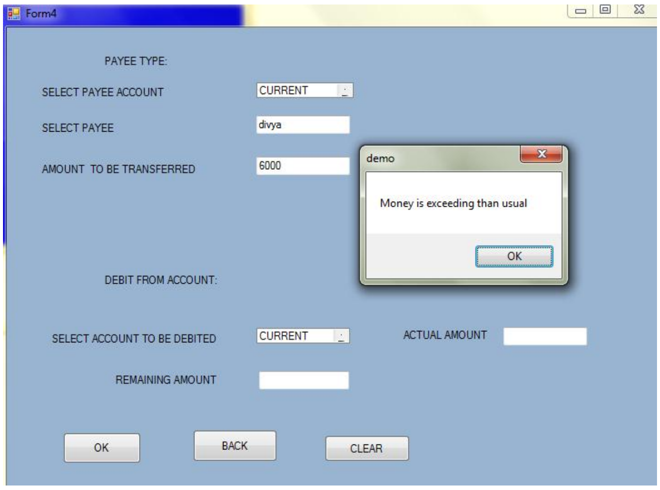
REMAINING AMOUNT 21000

demo

amount transfeered

FIGURE 5: Form to enter transaction details

STEP 5: When transaction seems to be abnormal then system goes for two factor authentication. In this form the user has typed transaction amount higher than usual so the system request the user to enter OTP to complete the transaction.



PAYEE TYPE:

SELECT PAYEE ACCOUNT CURRENT

SELECT PAYEE divya

AMOUNT TO BE TRANSFERRED 6000

DEBIT FROM ACCOUNT:

SELECT ACCOUNT TO BE DEBITED CURRENT

ACTUAL AMOUNT

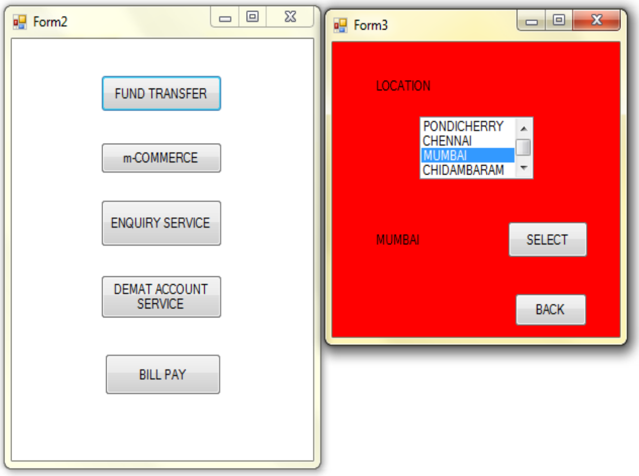
REMAINING AMOUNT

demo

Money is exceeding than usual

FIGURE 6: Form showing warning for excess amount in transaction

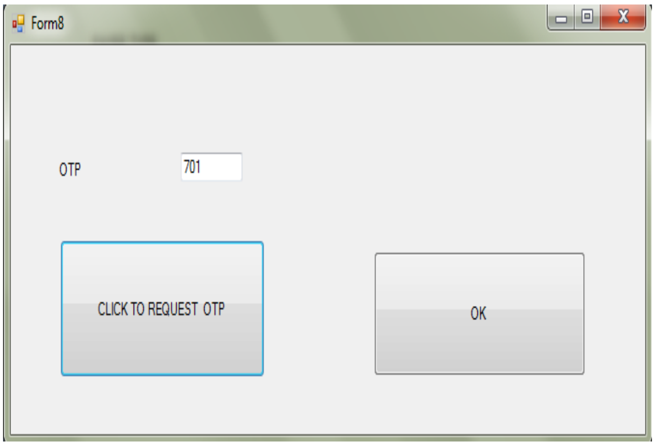
STEP 6: If the selected location is different from preferred location then OTP is send to the mobile



MUMBAI

FIGURE 7: Form to select location

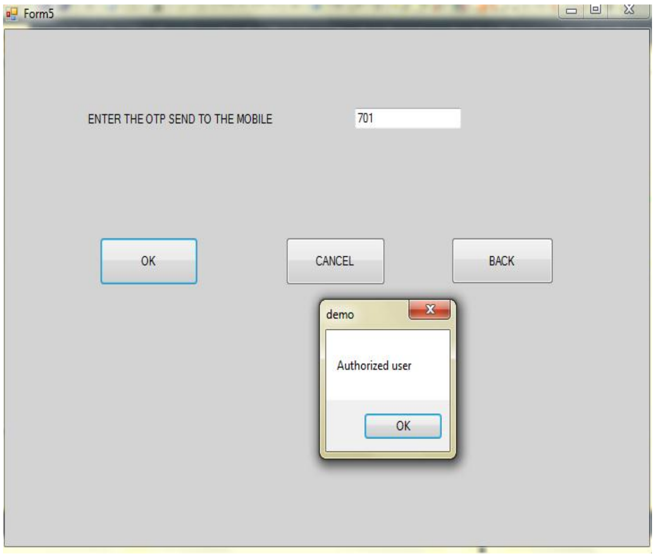
STEP 7: User requests OTP by clicking the button.



OTP 701

FIGURE 8: Form requesting OTP for different location transaction

STEP 8: User will be authorized only when he types the OTP which is send to mobile

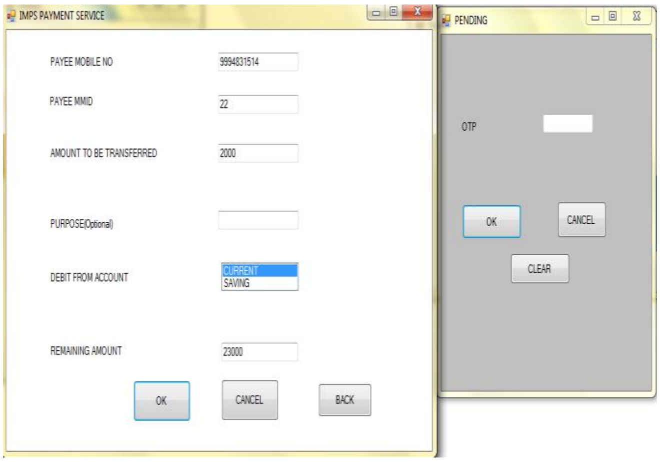


ENTER THE OTP SEND TO THE MOBILE 701

Authorized user

FIGURE 9: Form showing the authentication for user

STEP 9: Mobile banking payment. While doing payment the amount will be in pending state until the payee types the OTP which is send to his mobile.



PAYEE MOBILE NO 9994831514

PAYEE MMID 22

AMOUNT TO BE TRANSFERRED 2000

PURPOSE(Optional)

DEBIT FROM ACCOUNT CURRENT / SAVING

REMAINING AMOUNT 23000

FIGURE 10: Form showing the transaction details after correct OTP given

VI. DISCUSSION

The current mobile banking systems are with lack of security features which will act smartly during critical transactions. The proposed system will act according to the behavior of the users based on the location context for fund transferring. With this feature the mobile application can provide a smart security aspect to identify whether the correct user is transferring the funds or any intermediate snoopers are tracking the account of some others. Only when the two factor authentication of the mobile user is been completed the funds will be transferred thus better security can be ensured.

VII. CONCLUSION

The proposed system addresses the various threats identified in the mobile banking transaction. The behavioral context authentication provides a better security for the mobile banking users from their information disclosure and man-in-the-middle attacks. Though they track the account details only when the two process of authentication is been completed the actual process will be carried out. Hence a better security for the mobile transactions can be achieved.

REFERENCES

[1] Cognizant, "Mobile Banking Security: Challenges, Solutions", Cognizant 20-20 Insight, July 2014.

[2] **Nikolaos Zacharopoulos**, et al., "Mobile Payments: Risks, Security and Assurance Issues", An ISACA Emerging Technology White Paper, November 2011.

[3] **Niranjanamurthy M, DR. Dharmendra Chahar,** "The study of E-Commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.

[4] **Loucif Kharouni,** "Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit Feature", Trend Micro Incorporated Research Paper, 2012.

[5] **Ajeet Singh et al,** "Secure Payment System for Electronic Transaction",International Journal of Advanced Research in Computer Science and Software Engineering.

[6] **Yang Jing,** "On-line Payment and Security of E-commerce", Proceedings of the International Symposium on Web Information Systems and Applications, May 22-24, 2009, pp. 046-050.

[7] **Oz Shy**, "Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues", Public Policy Discussion Papers, March 2, 2010.