Enhancing Security of One Time Passwords in Online Banking Systems

S. Sri Hari, C. Kavinkumar, Gurram Keshav Niketh, N. Harini

Abstract--- The advancement in the technology has led to introduction of many popular Internet applications. Internet Banking also called as e-banking is one such indispensable application which has a major impact on our modern life. Although banks strongly encourage their customers to do online transactions and advertise it as a very safe and secure mode of transacting, in reality there is a huge risk associated. The continuous growth of online banking application brings with it several security issues and increased cost of implementing higher security systems for customers and banks. Online banking system maybe compromised in a wide variety of ways like using trojan horse, botnets, Phishing etc. Although multifactor authentication schemes exist to verify the authenticity of the client, the drawbacks with these schemes is that they work at transaction level rather than at the authentication level. This paves way for so called for man in the middle attack between the user and security mechanisms of browsers, smartphones etc. With online banking security becoming a critical requirement one needs to find better usable and workable solution based on transaction cum authentication level. An attempt has been made in this work to propose an authentication that enhances the security of the online banking systems.

Keywords--- Authentication, e-Banking, One Time Password, Fingerprint, Biometrics, Short Message Service, Subscriber Identity Module.

I. INTRODUCTION

The advancement in the computing paradigms and Internet has drastically changed the way one performs banking transaction. With electronic banking becoming a more successful internet service customers can frequently carryout payments related transactions with a smartphone (a personal dependable tool). SMS banking services is quite popular service, that facilitates information enquiry notification and alerts, payment transfer etc.

Online banking authentication generally requires customers to authenticate using username and passwords. A lot of factors need to be considered relating to security issues like whether a correct banking site is being contacted, whether individual credentials are safeguarded during transmissions and whether these credentials are really from the individual whom the sender claims to be. Adoption of HTTPS facilitates secured connections to the banking sites.

Manuscript received February 01, 2019

S. Sri Hari, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Tamil Nadu, India. (e-mail: cb.en.u4cse17457@cb.students.amrita.edu)

C. Kavinkumar, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Tamil Nadu, India. (e-mail: cb.en.u4cse17428@cb.students.amrita.edu)

Gurram Keshav Niketh, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Tamil Nadu, India. (e-mail: cb.en.u4cse17422@cb.students.amrita.edu)

N. Harini, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Tamil Nadu, India. (e-mail: n_harini@cb.amrita.edu)

Literature has discussed wide variety of single and multi-factor authentication schemes to verify the identity of the claimant. Also, to double verify the identity of the sender, schemes like OTP has been integrated with banking services. However, this is not enough to prove the security as a lot of attacks like mobile phone malware attacks, physical theft, phishing attack, session hijacking is possible. This demands a framework capable of enhancing the security of the online banking system. The work presented in this paper uses a multi-factor authentication scheme based on OTP and biometrics. Experimentation clearly revealed the simplicity and the effectiveness of the proposed authentication scheme to combat the different online account threats and frauds.

II. LITERATURE REVIEW

Internet banking

Any online system has to satisfy four goals of security namely, Secrecy, Integrity, Availability and Accountability. Internet Banking systems generally uses fixed or dynamic passwords, digital signature-based hardware tokens for authenticating clients. The explosion in the Internet has also increased cyber related crimes. The hackers adopt mechanisms to fraudulently acquire sensitive information from a trust worthy victim to impersonate a trustworthy entity [6]. Banking systems incorporate defense mechanisms, trust models and access control models to protect the privacy of the users and enhance security in transactions. Examples for these include login procedure, authenticating a transaction using OTP through SMS[5] etc. Prevention is better than cure, so any malicious transaction has to be detected even before it happens. Banking organizations have to continually look into improving cyber-crime detection systems. The Internet banking process generally takes place in as follows: Firstly, the credentials of the customer is sent from customers PC/mobile to the web server. The received credentials are then verified by the web server[3] using customer information database. The privacy of the communications between the customers PC and bank server is preserved by establishing a secure session using a protocol like SSL.

Online authentication

Authentication process enables one to verify the claimant's identity. Onetime passwords are used as additional factors in multi factor in authentication application. These passwords are valid for short duration of time and exactly for one authentication process. A convenient way to provide a user with an OTP is to send it via SMS. The mobile phone of the user must be registered by the user during the registration phase.

It is possible that these OTPS may be intercepted, sent by a malicious user who successfully steals the registered user's credentials. [1] The present security systems use user ID and additional factor of authentication in the form of OTP's, Biometric, QR codes[11], answers to security questions etc. However, the existing Internet banking systems are still being exposed to various forms of attacks. Evidences for insecurity in online baking application is evident from the report the states, 'New Delhi has come aross new ways in which attackers are syphoning of money from legitimate user's accounts'. This was identified only after an account holder complained about Rs. 11.5 lakhs withdrawn from his account without his knowledge.

Smart Phone users

The fact that more functionalities are integrated within mobile phones like banking, browsing, shopping, chatting etc., brings with it an exponential growth in the number of people considering mobile phones as their indispensable part of their lives. The statistics in Fig. 1 clearly confirms the claim. The statistics also presents the number of users relying on mobile banking services.

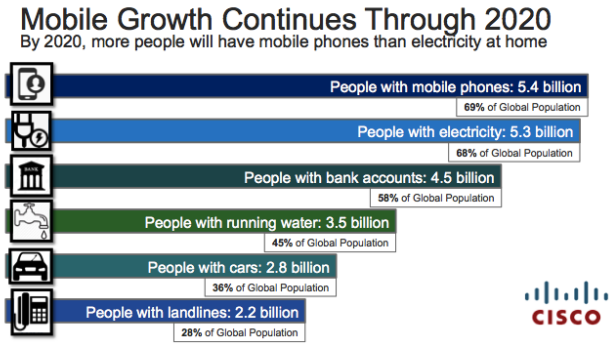

Fig. 1: Statistics of number of users relying on mobile banking services.

About One Time Passwords (OTP)

With a number of people relying on Internet banking solution[4] application must guarantee resistance against offline credential stealing attacks. A challenge response based One Time Password Authentication scheme[2] is generally used by banking applications. These credentials are short lived and generally delivered through an SMS. Literature has also discussed encrypted short-lived passwords being used for user authentications. The possession of mobile phone[6] is often used in multi-factor authentication. Mobile phones are generally protected with Graphical patterns, PIN, Facial Identification Recognition, Fingerprint Authentication[7] etc. These are generally used to gain access to the device but not applied when a textual message is communicated from the device.

SIM allows attackers to steal phone numbers, SMS can be intercepted in many ways. In other words, a sophisticated attacker with a bit of personal information could hijack the mobile and gain access to online accounts to use those accounts to drain the bank accounts. This brings a clear need for an enhanced security scheme that facilitates secure online banking based on transaction and authentication levels.

Attacks on Online Banking

Despite the benefits the banks offer to customers Internet baking has raised many security issues which is sure to put customers at risk leading to customer loss or business loss[9], if a strong security service is not provided. Frauds in Internet banking can take multiple forms like a phisher could attempt to acquire credentials by masquerading as a legitimate person, MITM attacks where the hackers' place themselves between banking servers and online customers. Fraudulent SMS's or emails could be circulated to collect the credentials of using malwares[8].

Summary of findings

With online baking becoming indispensable part of everyone's life, security has become a frequent concern to both banks and users. Unfortunately, electronic financial transactions are offering a new revenue model for hackers. While innovations in security measures like using SSL[10], authenticating using OTP, etc. lowers the risk of data getting hacked, the methods suffer from providing an absolute safe environment for online financial transaction as they work only at a transaction level or at the authentication level but not on the combined level. The security solution based on transaction level fails to perform a clear authentication or vice versa. This necessitates the need for further investigating and identifying a process that would operate at a hybrid level (Authentication level and Transaction level).

III. PROPOSED SYSTEM

The security models adopted in online banking systems are based on several security layers and consists of diverse solutions aiming to protect the users and banking data. Digital signatures are used to authenticate the users and banking system itself. OTP's are used as second authentication factor. Virtual keyboards thwart the use of key loggers. Device registrations are used to provide restricted access. CAPTCHA is used for identifying Bots from human users. SMS notifications are used to notify about transactions to user. The security model existing presently in online banking system based on SMS OTP is depicted in Fig. 2(a) and 2(b) (Transaction level).

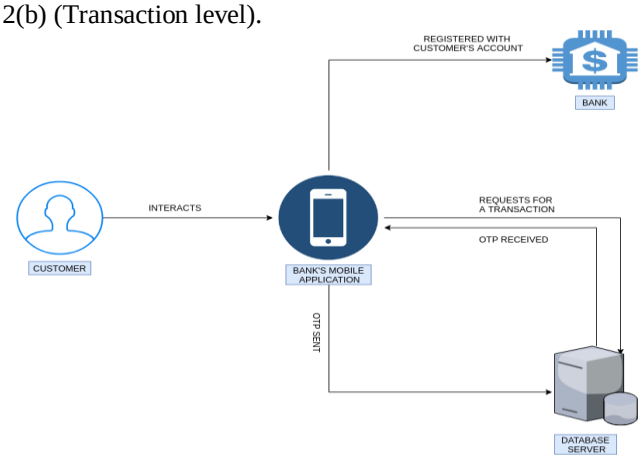

Fig. 2(a): Legitimate user carrying out transaction (transaction level)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It can be seen that attacker has successfully impersonated the legitimate user and carried out transaction successfully. This can be prevented with a slight modification in the scheme to include authentication using biometrics at the time of communicating OTP associated with the transaction and the same is depicted in Fig. 2(c) and 2(d) (Transaction and authentication level).

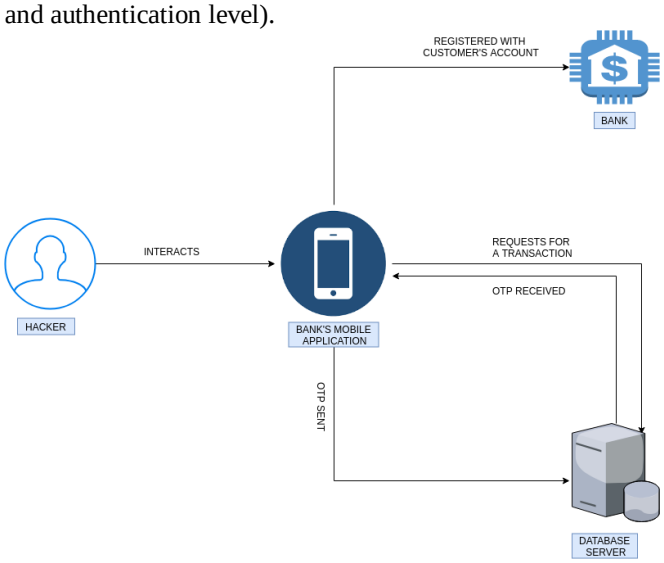

Fig. 2(b): Attacker carrying out transaction (transaction level)

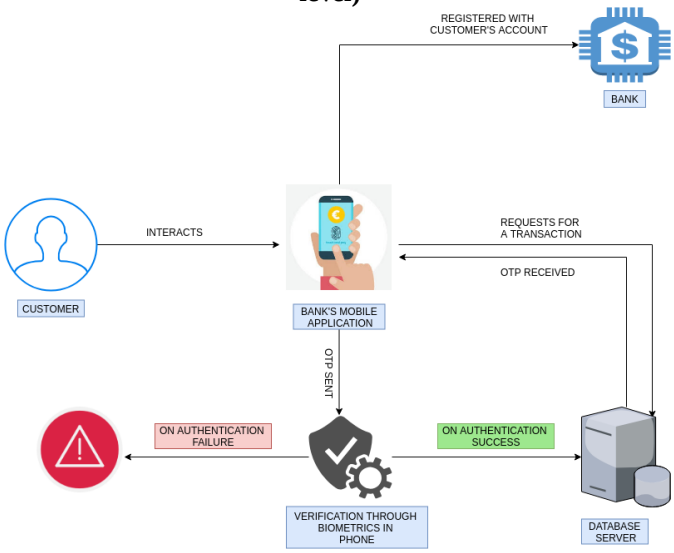

Fig. 2(c): Legitimate user carrying out transaction (transaction level + authentication level)

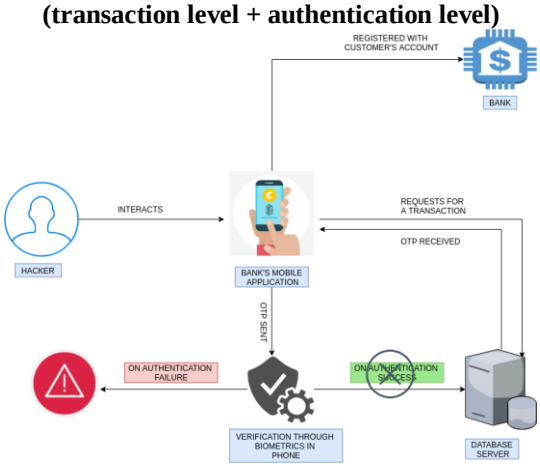

Fig. 2(d): Attacker carrying out transaction (transaction level + authentication level)

Fig. 2(a) depicts the working of existing system of online banking based on SMS OTP.

It is possible that attackers (Fig. 2(b)) can abuse the connection system to intercept SMS messages on network and route them elsewhere using fake cellphone towers. A person who knows a legitimate user's mobile phone can get access to the personal information and adopt a SIM swap process to authorize transactions.

IV. RESULTS AND DISCUSSIONS

The working of the scheme takes place in three phases:

1) In the registration phase the user has to register his/her fingerprint in the mobile device that would serve as authentication token in the online banking system. The screenshots associated with registration of fingerprint using the steps add fingerprint, store the valid fingerprint and confirmation received on successful registration of the fingerprint is shown in figures Fig. 3(a)-(d) . The registration phase also includes the installation of the APK file , created to securely deliver the OTP for carrying out an online banking transaction.

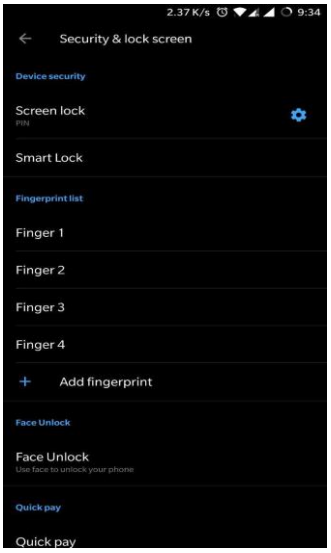

Fig. 3(a).

Fig. 3(b).

Fig. 3(c)

Fig. 3(d)

2) The registration phase is followed by the authentication phase. On the receipt of OTP, the application provides a screen to enter the received OTP and the mere press on the send button will prompt the user to swipe his/her finger for authentication. On Successful authentication the OTP is sent and the transaction is complete. On Authentication failure leads to OTP not being delivered within the short duration of time marking the failure of the transaction.

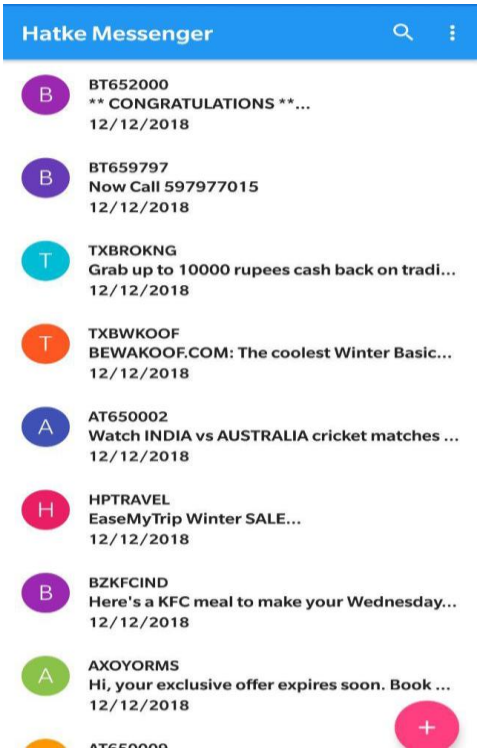

Fig. 4(a)

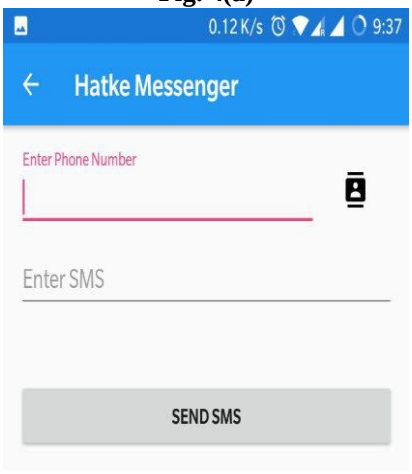

Fig. 4(b)

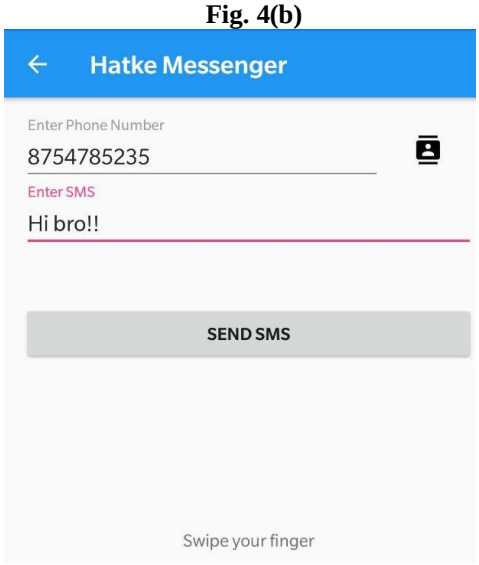

Fig. 4(c)

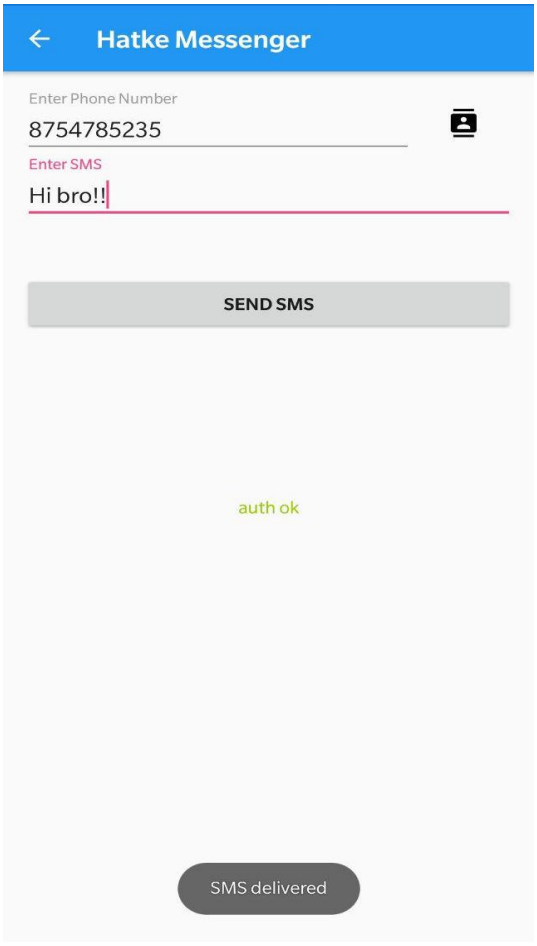

Fig. 4(d).

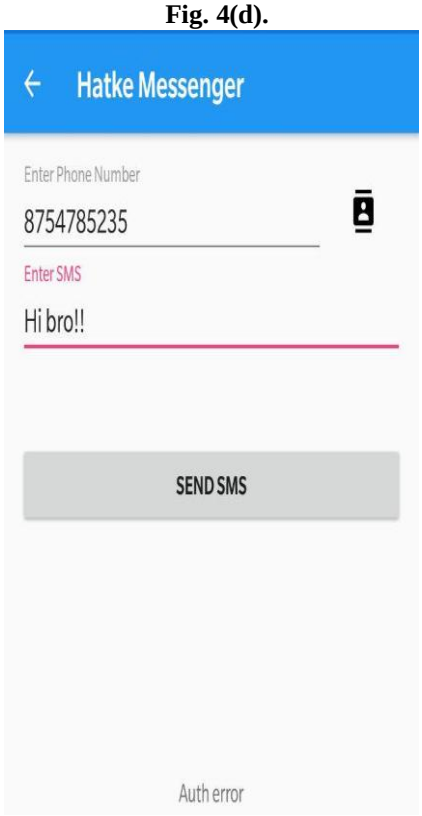

Fig. 4(e).

3) The screenshots of the code snippet for the mobile application that facilitates the delivery of OTP is given in Fig. 5(a) and 5(b) :

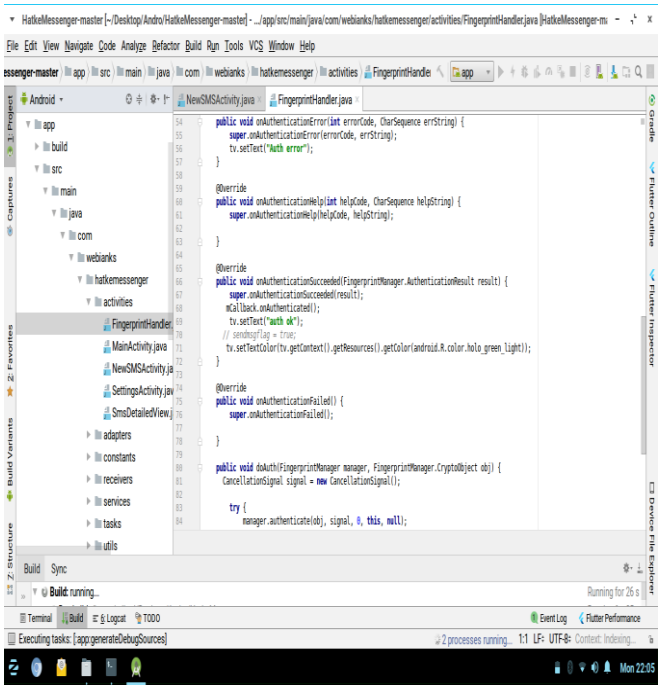

Fig. 5(a): Screenshot 1 of code snippet

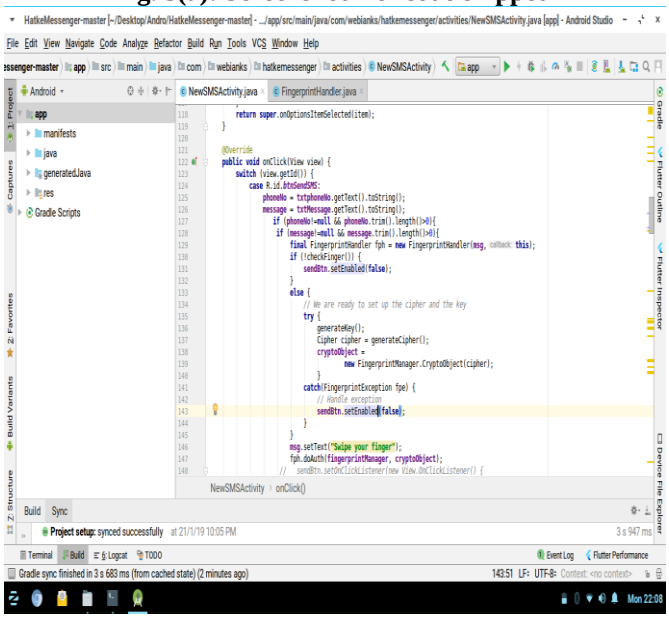

Fig.5 (b): Screenshot 2 of code snippet

V. CONCLUSION AND SCOPE FOR FUTURE

The prevailing security models for online banking systems are either based on transaction or authentication levels. Survey states that most of the attack in the online banking systems focus on obtaining authentication information from legitimate users and impersonating a trusted entity. Existing schemes are unable to provide highly secure banking services because of information leak. This fact necessitates a new scheme capable of performing security verification at transaction cum authentication level. This research work proposes a scheme capable of enhancing security in online banking systems that is usable and works at a hybrid level(transaction and authentication levels).

Further work is being made on identifying efficient data mining and pattern recognition methods to strengthen the working of the proposed scheme.

REFERENCES

1. https://www.moneycontrol.com/news/trends/current-affairs-trends/indian-banks-lost-rs-109-75-crore-to-theft-and-online-fraud-in-fy18-2881431.html
2. Jun Lu, Bingjun Zhang. Security product research in the Internet banking based on OTP, Financial electronic .J.China, 2009.11.pp80-81
3. C. Grier, S. Tang, S. King, "Secure Web Browsing with the OP Web Browser", in IEEE Symp. on Security and Privacy (SP 2008), pp. 402-416, 2008.
4. K.Chikomo, M. K. Chong, A. Arnab, A. Hutchison (2006), ―Security of mobile banking‖, University of Cape Town,South Africa, Tech. Rep. [Online]. Available: http://pubs. cs.uct.ac.za/archive/ 00000341/01/Security of Mobile Banking paper.pdf.
5. N. Croft, M. Olivier, ―Using an approximated One-Time Pad to Secure Short Messaging Service (SMS)‖, in Proceedings of the Southern African Telecommunication Networks and Applications Conference (SATNAC), 2005, pp. 71–76.
6. Xing Fang, Justin Zhan. Online Banking Authentication Using Mobile Phones,IEEE 2010. [18]. A. Hisamatsu, D. Pishva, and G.G.D. Nishantha.
7. Online Banking and Modem Approaches Toward its Enhanced Security, ICACT 2010.
8. Online Banking: Threats and Countermeasures Revised Version: 1.3 Release Date:June, 2010 AhnLab, Inc.
9. Singhal, D and V. Padhmanabhan (2008). A Study on Customer Perception Towards internet Banking: Identifying major contributing factors. The Journal of Nepalese Business Studies. V (1), 101 – 111.
10. Dr.N.Harini, Dr T.R Padmanabhan and Dr.C.K.Shyamala , ―Cryptography and security‖, Wiley India, First Edition, 2011
11. N. Harini and Dr. T.R. Padmanabhan, "2CAuth: A New Two Factor Authentication Scheme Using QR-Code", International Journal of Engineering and Technology (IJET),Vol. 5:2 Apr-May 2013, Pages: 1087 -1094