International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 2 (Mar-Apr 2015), PP. 174-176

SECURED BANKING TRANSACTION USING VIRTUAL PASSWORD

Krishnammal A[1], Sindhiya S[2], Dhivya P[3], Janaki K[4]
Assistant Professor/IT, Student Final IT,
Sri Krishna College of Technology, Coimbatore.
a.krishnammal@skct.edu.in, p.dhivya92@gmail.com

ABSTRACT- One time password(OTP) is the authentication method used in online banking system today. Hackers are getting better each day at cracking sensitive information. Once this happened, they can gain access to our private network and steal our sensitive business information. A common technology used for the delivery of OTPs is text messaging.OTP over SMS might not be encrypted by any service-provider. In addition, the cell phones which is used to receive the SMS also play an important role, in which more than one phone comes into account. The vulnerable parts of the cell phone network can be mount to man-in-the-middle attack[13]. To overcome the difficulties the virtual password concept is introduced. The virtual password concept involves a small amount of human computing to secure user's passwords in on-line environments. To provide high security, we enhance the existing system with virtualization concept [1]. Hacker may guess our password but he cannot access our account because he cannot access virtual password. The major hacking threats like phishing, key-logger, shoulder-surfing attacks, and multiple attacks cannot affect our schema. In user-specified functions, we adopted secret little functions in which security is enhanced. Virtual password is a password that is valid for only one login session or transaction and after that it becomes obsolete [12]. The calculation of the virtual password is done at the client side which reduces the delay of time in receiving OTP via SMS. To make the client more convenient in calculating the virtual password an application is used which reduces the work of the client. This method is more instant than the traditional OTP system used today.

Keywords- OTP(One Time Password), PIN number (Personal Identity Number), KYC (Know Your Customer)

I. INTRODUCTION

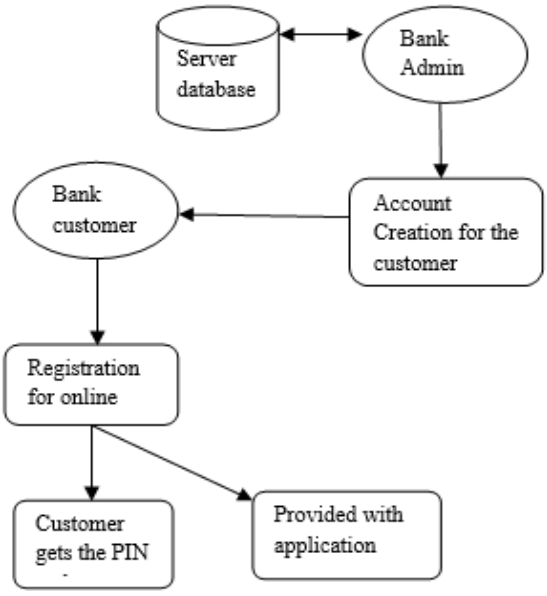
Today, The Internet has indulged into day -to-day activities of common man which expects the security system and authentication system to be of greater strength. Besides normal browsing we are more involved in sensitive transaction such as online payment, online booking, online banking, etc., more and more services have been moved online. One of the main sectors that are gaining more and more attention and importance is banking system, where once the sensitive information of an individual is stolen, the consequences are very dangerous. Hence the Research and Development (R&D) department is working hard to make the banking process more secured. The OTP received via mobile network is unsecured because of end-to-end security provided by the mobile network. There may be fluctuation or delay in time due to network facility available; using multiple mobiles for receiving OTP makes the password unsecured [9]. In Virtual Password schema, the calculation of the OTP is done by client side using an application in the mobile; it becomes independent of mobile network which increases the performance of the system [2]. The user is provided with permanent PIN number and a random number on the login page, which makes the hacking difficult. Even if the hacker hacks the account information of an individual, the intruder cannot access our mobile application, since it uses random number generation concept. The developer cannot guess the random number that is generated for the particular transaction at a time.

II. THE PROPOSED SCHEME

A. Overview

The account creation is done by the banker which allows the user to register for the online banking. To use the virtual password schema, during the registration a mobile application will be downloaded and a permanent PIN number will be generated for the user [11]. User has to install the mobile application in the mobile. In the mobile application, virtual password will be generated and, sent to the server database. This serves as the virtual tool for connecting the client and server. This reduces the burden of the server for calculating the OTP. In the login form the user will provide the user name and password. If the username and password matches with the database, a random key will be sent to the access page. The user has to enter the random value from the access page and the permanent PIN number suffixed/prefixed (as per the convince of the user) in the mobile application. The application will provide the virtual password which is re-entered in the login page .Thus the user can proceed with the normal banking transaction. By this client side calculation of the virtual password is achieved with greater heights of security.

B. Overall process



C. Scheme Description

This section describes the details of Banking, Registration module, Login module, online account transaction, financial intelligence.

1) Banking

The banker starts the process by creating new bank account for user who wants to keep money on bank. Users may have personal accounts or corporate accounts for doing transactions through online from anywhere in the world. Each user has been provided with user name and password for secured online transactions.

2) Registration Module

In the Registration Module, as per the registration a mobile application will be downloaded and a permanent PIN number will be generated for the user. User has to access the application through the cell phone. In the application the expression calculation of the virtual password is done, which is simultaneously updated in the server database. Thus the application serves as the virtual tool for connecting the client and server.

3) Login Module

In the login module, each and every user will be provided with the user name and password for secured authentication. After authentication, a random number is generated only with that further process proceeds.

4) Online Account Transaction

In this module, account holders are provided with facilities such as Fund Transfer, With Draw and Deposits. An account holder has to register their personal information and sends the report to Financial Intelligence.

Login: It is for Login Authentication for Account holders to enter inside and make their online transactions.

Account Transaction: Here, the account holder can make the account transactions through online. Each transactions has maintained by transaction number. It is unique number.

View Account Information: In this module, account holder can view the account information, balance information and transaction information.

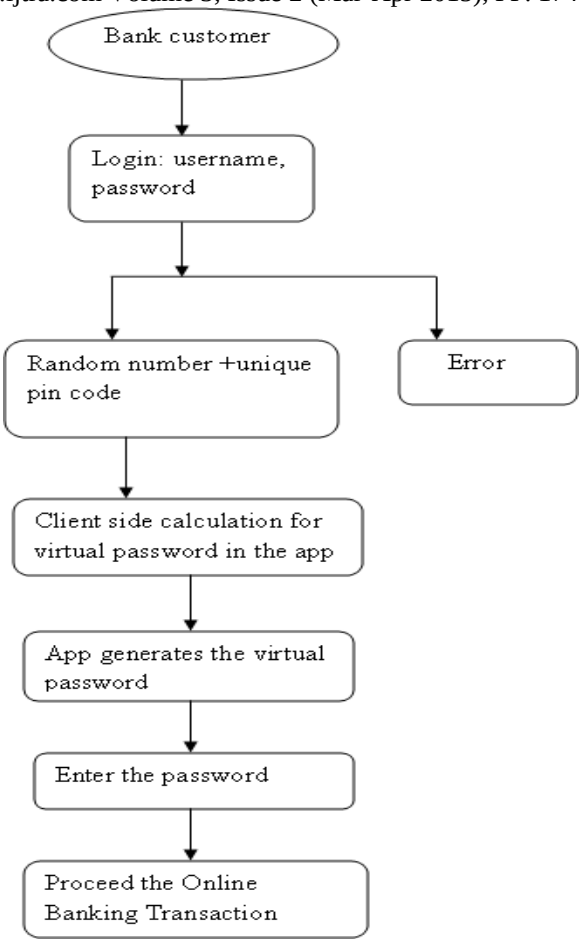
5) Financial Intelligence

The Financial intelligence people can view the account holder's information from Know Your Customer (KYC). Each Account holder will have unique number, it will be generated automatically. The main process is to view and filter money transactions and monitor their transactions information through online. If transactions are suspicious, that record has to be maintained separately. It is been stored at the Suspicious Activity (SA) report and update status after finishing enquiry.

With the use of money transaction report, financial intelligence people can view the transaction that has been made by the account holders.

D. Access Flow

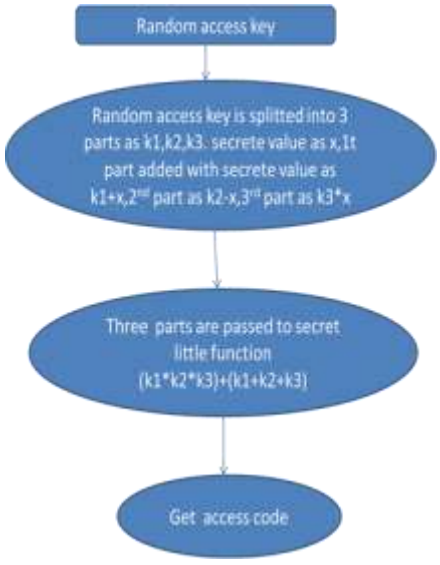
The flow of control takes place accordingly,



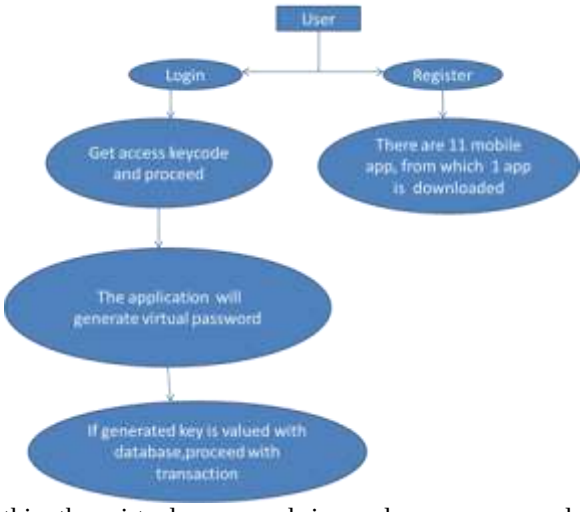
E. Algorithm Explanation:

TB-VP algorithm:

In the Time Based Virtual Password algorithm, A user have the choice of choosing their own algorithm or function for calculating the virtual password. The performance of the algorithm differs according to their security complexity [5].



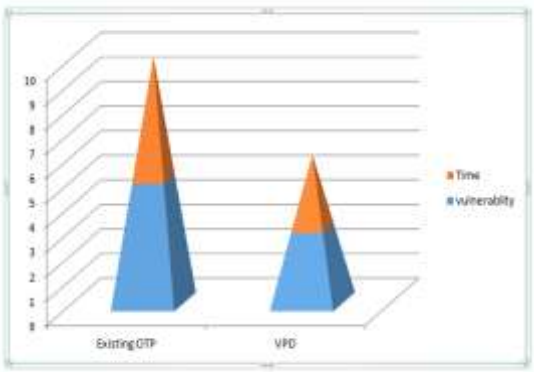
Secret little function and codebook are the two function that are used to generate the user defined function. The access code (PIN number) is generated using and importing the random number package which helps in automatic random generation of four digits PIN number. The user specified function approach is the one in which users themselves can choose any function they like. However, such freedom is based on the assumption that the user has some basic knowledge about choosing the security level. The access code generation takes place by the secret little function, the complexity of the virtual password is defined in the code book function.



By this the virtual password is made more secured and difficult to hack. The client side calculation of the virtual password is made more easy by using the secrete little function and code book enhancement.

1) Time & security:

The main goal of the proposed system is time complexity and security enhancement. The secured banking transaction generates virtual password more instantly whereas the traditional OTP followed today takes minimum of 2-3 minutes and it varies or it gets more delayed according to the performance of the network availability. Each application is nondependent on external factors.



III. CONCLUSION

In this paper, we have implemented the application only for the instant generation of virtual password. This application can further be enhanced by providing Location identification. This will help more in security criteria such as once the phone gets stolen by the intruder and when he tries to make the unauthorized transaction. An automatic alert to the bank authorities and track the location through GPRS longitude and latitude system.

REFERENCES

[1] Yang xiao, senior member, IEEE, Chung-Chih li, ming lei, and Susan V. Vrbsky differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft IEEE systems journal, vol. 8, no. 2, june 2014

[2] M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li, "Virtual password using random linear functions for on-lineservices, ATMs, and pervasive computing," *Comput. Commun. J. Elsevier*, vol. 31, no. 18, pp. 4367–4375, Dec. 2008.

[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder-surfing," in *Proc. 11th ACM Conf. Comput. Commun. Security*, 2004, pp. 236245.

[4] A. Herzberg and A. Gbara. (2004). *Trustbar: Protecting (Even Naive) Web Users From Spoofing and Phishing Attacks*, Cryptology ePrint Archive, Rep. 2004/155 [Online]. Available: http://eprint.iacr.org/2004/155

[5] Y. Xiao, C.-C. Li, M. Lei, and S. V. Vrbsky, "Secret little functions and codebook for protecting users from password theft," in *Proc. IEEE ICC*, May 2008, pp. 1525–1529..

[6] *One-Time Password* [Online]. Available: http://en.wikipedia.org/wiki/One-time−password

[7] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell, "Stronger password authentication using browser extensions," in *Proc. 14th USENIX Security Symp.*

[8] S. Lee and K. M. Sivalingam, "An efficient one-time password authentication scheme using a smart card," *Int. J. Security Netw.*, vol. 4, no.3, pp. 145–152, 2009.

[9] M. Abdalla, E. Bresson, O. Chevassut, B. Moller, and D. Pointcheval,"Strong password-based authentication in TLS using the three-party group DiffieHellman protocol," *Int. J. Security Netw.*, vol. 2, nos. 3– 4, pp. 284–296, 2007

[10] S. Laur and S. Pasini, "User-aided dataauthentication," *Int. J. Security Netw.*, vol. 4, nos. 1–2, pp. 69–86, 2009.

[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp.521–534, 2002.

[12] IETF. (2004, Jun.). *MTA Authorization Records in DNS(MARID)*[Online].Available:http://www.ietf.org/html.charters/OLD/maridcharter.html

[13] Alzomai M.; Josang A., "The mobile phone as a multi OTP device using trusted computing," Network and system security(NSS) 2010 4th international conference on, vol.,no.,pp.75,82,1-3 sept 2010.