# OTP with Multi Factor Authentication

Kajol Gandhi[1], Divya Shah[2], Dhanshree Shelke[3] ,Chetana Dodke[4]

*Atharva College Of Engineering Department of Computer Engineering, Mumbai, Maharashtra, India*

**Abstract—** ***Network security deals with large number of devices to provide them secure access. It provides security for both public which can be access by all users and private networks which can only be access by legitimate users. OTP generates a new random password every time so even if the user did not recollect the old password its fine. Multifactor Authentication techniques can be used to provide secure web transactions using cell phones. Various methods have been proposed to provide multifactor authentication, such as biometrics etc.***

**Keywords—** ***Security, Authentication, Image hidden password.***

## I. INTRODUCTION

Network security is wide area of research today. Number of areas comes under this section are Mobile networks, Wireless Networks, Sensors Networks, cryptography, Information security, Mobile security, wireless communication etc. In future lot of research can be done on these areas, many algorithms are developed or modify, many security techniques are developed for providing the security in these areas.

Cryptography is main tool in network security. It works on three attributes i.e Confidentiality, Integrity and Availability.

**Confidentiality** means the authorized person is same as it claims to be,

**Integrity** deals with the concept that data is received same as it is send by the sender .

**Availability** deals with that the devices should available for providing network security. Cryptography uses many Encryption and Decryption algorithm to deal with confidentiality and Hash algorithms , MAC algorithms and Digital signature algorithms to deal with data integrity.

It is banking website that lets you perform operation online at your convenience 24X7, 365 Days of year. It is kind of web site that makes user e banking experience more pleasant and secure by providing two factor Authentication that minimizes the chances of Unauthorized access to users account by way of Phishing

It is banking web site that lets you perform following operations securely:

1. Secured Login by way of hiding second layer password in image
2. Create Account
3. Create Fixed Deposit of Various types and Tenures
4. Check FD Rates
5. Check Transactions for each Account
6. Check Balance in each Account

Traditional E-Banking website performs same operations as supported by Physical Bank. The main difference is just that the online process is fully automated and there is no “real person” who actually fulfills banking operations – it’s all done via computers that are directly linked up the Banking house.

Presently, Internet banking customers only need a computer with access to the Internet to use Internet banking services. Customers can access their accounts from anywhere in the world. Each customers is provided a login ID and a password to access the service. It is easy and convenient for customers.

However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is that when it has been compromised, the fraudsters and hence they can easily take full control of online transactions. In such cases, the password cannot be used as information and doesn’t works as an authentication token because we cannot be sure who is behind the keyboard typing that password in.

However, easy access and convenience should not be at the expense and mercy of the security of information. This is important to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters.

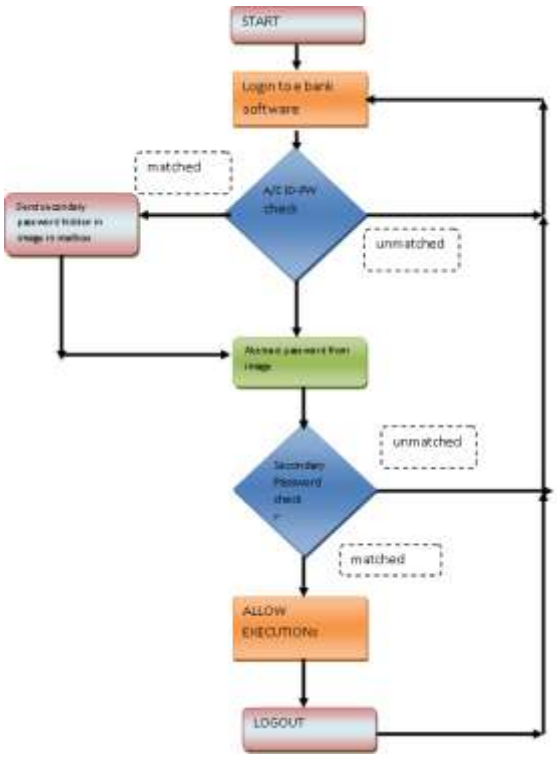
The paper is organized as follows: the first section provides a brief introduction. The second section describes about the design of the project, the third section describes about the implementation of the work. Conclusion and Future research directions are presented in the last section.

## II. PROJECT DESIGN

The most important goal of security enhancement using data hiding in image is to hide messages within the image so the intended receiver of the image get the data of his interest in the form of the image so even if this image fall in wrong hand chances are less that person receiving the image get to know that some data is hidden in the image.


Figure Transaction flow in Secure Electronic Transaction (SET)

Flow Chart:-




This kind of technology is very useful in case of increasing security of the secure system. Through hiding a secret message inside the Image, a simple image is taken as carrier to carry the data to be hidden in it. Once Image is obtained, data that needs to be hidden is taken from user and is placed between the data bytes of actual image such that receiver of the image may consider it as normal image but when supply this image to decoder, can extract the hidden message within it in its entirety.

## III. IMPLEMENTATION

The implementation have two important parts- building a website and a highly secured second layer authentication system.

*Algorithm for Login page:*

1. Ask user to enter username and password
2. Open database connection
3. Transfer to user info table
4. If match found then
    - Create session for user
    - Generate one time random password for the user
    - Encrypt this password
    - Embed this password in to image
    - Send image as an attachment in Email to Authenticated user on his registered email Id
    - Write one time password in to database.
    - Move to Security User Login page
5. Ask User to provide the image that has been sent to his email id on successful authentication
6. Fetch hidden password from image
7. If found
    - Open database connection
    - Get one time password from DB
    - Compare this password with one obtained from Image
    - If match

Set User Info in session and forward user to his home page

8. Move to Security User login page

9. Move to default home page

10. Else give error message.

## IV. CONCLUSIONS

We have presented a brief review of the multifactor authentication in E-banking using one time password. The first authentication factor can be the use of passwords and the second authentication factor can be the use of mailbox secondary image hidden password, is a good avenue to introduce the second factor.

## V. REFERENCES

[1] J. Gao, J. Cai, K. Patel, and S.Shim (2005), Wireless Payment, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), pp. 367-374
[2] .J. S. Kungpisdan, B. Srinivasan and P.D. Le, A Secure Account-Based Mobile Payments Protocol, Proceedings of the International Conference on Information Technology: Coding and Computing.
[3] Y.B. Lin, M.F. Chang, H. C.H. Rao, (2000), Mobile prepaid phone services.
[4] Horowitz, Sahni,Rajasekaran, Fundamental of Computer Algorithms.
[5] Young Sil Lee, HyoTaek Lirn, HoonJae Lee A Study on Efficient OTP Generation using Stream Cipher with Random Digit.
[6] Bayalagmaa Davaanaym, Young Sil Lee, HoonJaeLee, SangGon Lee and HyoTeak Lim,"A Ping Pong One-Time-Password system in Java application".
[7] Nadira Jasika, Naida Alispahic, Arslanagic Elma, Kurtovic Ilvana, Lagumdzija Elma, Novica Nosovic," Dijkstra's shortest path algorithm serial and parallel executionPerformance analysis".
[8] MeltemKURT , Tank YERLiKA Y A," A New Modified Cryptosystem Based on Menezes Vanstone Elliptic Curve Cryptography Algorithm thatUses Characters' Hexadecimal Values".
[9] Hamid Mehdi, "EABC: Data Encryption Method Based on Circle".