

SECURE ELECTRONIC TRANSACTION USING STRENGTHENED GRAPHICAL OTP AUTHENTICATION

K. Sruthi Shivani¹, K. S. Epsibha², Mrs. C. Sangeetha M.E.,³

¹UG Scholar, Department of Computer Science and Engineering, Chettinad College of Engineering & Technology, Karur, India-639-114

²UG Scholar, Department of Computer Science and Engineering, Chettinad College of Engineering & Technology, Karur, India-639-114

³Assistant Professor Department of Computer Science and Engineering, Chettinad College of Engineering & Technology, Karur, India-639-114

Abstract Online banking is the effective means of money transfer. The online banking service helps the customers to carry out the bank activities easily. The more the security is improved, the more customers are retained. With the expansion of internet banking, a lot of security threats like hacking, viruses, grooming, phishing, spam, etc. are increasing. We tackle them by making improvements in security measures. The Secure Electronic Transaction using Strengthened Graphical OTP Authentication service requires user's security image, security pattern and security questions to be registered in the bank. The user authentication is done by verifying the security images in addition to username and password where only two wrong attempts are allowed for a day. We propose multi-level security in transactions by using Face recognition technique for the devices with webcam, Graphical OTP authentication for the devices without webcam and security questions verification along with OTP. We make use of fortified GrIDSure technique that uses secret Grid Transmission for user authentication which helps to make fully Secure Electronic Transaction

Key Words: Face recognition technique for transaction, Graphical OTP authentication, GrIDSure technique, Multi-level security, Secure electronic transaction.

1. INTRODUCTION

With the introduction of computer technology, electronic communication technology and information technology in the bank system, the online banking involves in development of the bank's electronization, leads to electronic bank, the Internet bank and the Virtual bank. Online banking is used to perform amount transactions instead of finding a bank or interacting with a teller. It is used to transfer amounts from one to another through the internet rather than by cheque or cash. It helps to make instant transactions everywhere. A customer can view their accounts and transaction details. But security is too low and also it does not give guarantee to the users. Besides security, other issues that need to be considered are convenience, flexibility, cost and maintenance. Most of the banks are using electronic transactions. Few only don't have online banking service at all. The customers wish to have high security for their online

transaction. And they expect more security for keeping their money safe from the hackers. They heard a lot about hackers and crackers ways to steal any logical password or pin, code number, character and scared of ID cards or credit cards fraud and security breaches.

In existing work, authentication is done by using a username and password and provides authorized access to a system. As usernames and passwords are weak they can be lost or stolen, in the authentication process the user is to be checked whether the access is really by humans. Nowadays, Hacking (stealing the money) has a leading role than securing the money. Because hackers are growing through lots of featured technologies. Those technologies are affecting the online users. People are getting cheated by the cheaters in this vast world. So they should understand what is going on?

Therefore the Internet banking makes great convenience to the banks and customer business, but it brings the risks to the banks in confirming the legality of customers, and it becomes an important subject to prevent the illegal intrusion and damage. We think it is necessary to strengthen the security measures of the Internet banking, many commercial banks have launched many security measures. In this paper, we have explained various techniques in different disciplines and laid out the advantages and disadvantages to strengthen the security of online banking

2. RELATED WORKS

V.Manju et al [2] proposed an Internet banking security and it can be improved with Face recognition using Biometric verification. Online banking services are vulnerable to security issues. In their assumption, cybercrime has become easier for hacking purposes. This may be issued with some technical problems for each and every customer. So they provide access by allowing the multiple persons to access the same accounts by providing access privileges to original account holders. The Experiments show that this system provides high level security in online transactions than the existing traditional approach.

Ravi Jhavar et al [1] proposed GrIDSure technique, a one-time PIN scheme using random grids and personal patterns. Graphical OTP Authentication strengthens the security in

transaction. They proposed a way to fortify GrIDsure against Man-in-Middle attacks on the basis of (i) multiple patterns and (ii) an additional secret transmitted out of band.

They evaluated this method with 26 participants making 15 authentication attempts each over a 3 week period. In comparing it with other research in using the multiple patterns, they found no significant difference in using the grIDsure with one and more than one patterns.

3. EXISTING METHODOLOGIES

Online Banking Services authenticates users by their username and password. In addition, some systems use reCAPTCHA to verify that the user is human and other techniques like selection of images, voice recognition based authentication, SMS alert to the users and Email alert regarding their successful login. If the mobile phone's SIM cards are not activated, there is no chance to get OTP. Hence we are not able to perform the amount transaction anymore. Most of the online banking portals are not giving the proper details and information about their own bank. So people didn't like that kind of websites. People wish to have attracting online banking websites and also it should provide proper details about their bank. In the portal, the payment section users are allowed to transfer the amount to their beneficiary. The transactions are made by verification of One Time Password (OTP)[10]. These transactions may be issued with poor network connection and this process becomes risk when the login credentials are known to others and the theft of the user's mobile phone.

4. SECURE ELECTRONIC TRANSACTION

In the proposed system the Online Banking service adds security in users' entry phase and transaction phase.

4.1 Registration

The registration process takes place in the bank. The users' who require online banking service need to register their security credentials. They are allowed to register in separate portal. It is a step wise process where security images, security patterns, security questions' answers are registered and face of the users are recorded.

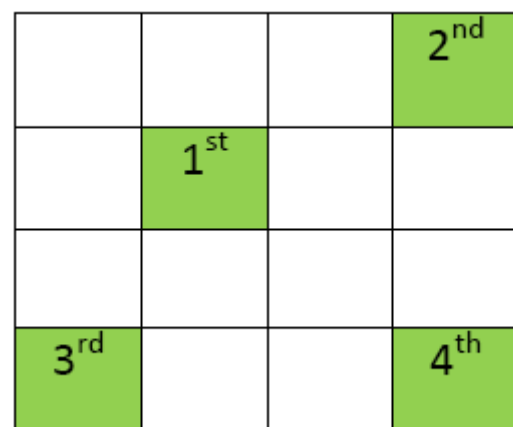
4.2 Security Images

The security images mentioned in Fig 2 falls under the security category. The security categories are like the Birds, Fruits, Flowers and Animals. The user can choose any of one the categories and the nine images based on that category are shown from those options. The user can select the first security image, next to that the other nine images of mandatory category are shown from that user can choose second security image. For the Birds category of user's choice the mandatory category is Places. Thus the category pairs are Birds-Trees, Fruits-Chocolates, Flowers-Places, Animals-Planets. The user can login by using username and password along with the selection of security image category followed by choosing of first and second security image. It allows only two wrong attempts a day. The account will be

locked if wrong attempts are made more than two times then the user has to visit the bank to unlock his/her account. Thus providing extra security in the login phase.

4.3 Security Patterns

Registration process of the security pattern is first the 4 x 4 grid is shown where the user can select up to four desired indexes. The indexes in the chosen order are stored as the security pattern. Whenever the user accesses the account for transaction in payment section using the device without webcam, this Graphical OTP verification [1] is done. The 4 x 4 random number grid is sent to the user's mail. The numbers in the registered indexes are the required one time password. After the verification of graphical OTP the users can proceed to the transaction phase. If the verification is failed the transaction fails.



			2 nd
	1 st		
3 rd			4 th

Fig 1-Registering Indexes

For example: Fig 1 is the registered security pattern of a user. Similar to the figure a 4 x 4 grid is displayed to the user in the registration portal. There the user can select their password. Later this is stored as the password. The users can change their password i.e. indexes frequently. But they can make changes only in the bank.

This helps to improve security. The users have to recall their registered indexes and then give the numbers present in those registered indexes in the same order. This password is verified and then only they are allowed to enter into the next transaction phase.

Each time the user attempts to enter into transaction phase the Graphical OTP authentication is done. A new 4 x 4 grid is sent to user's mail. If we display the grid in the online portal it may be watched by some third persons. As the hackers also can record the password from the user's screen, the grid itself is sent to the user.

6	7	1	0
9	8	3	2
4	1	9	5
3	2	7	5

Fig 1.1-Grid of Random numbers sent to user’s mail.

2	3	7	8
5	2	1	5
0	3	6	4
3	2	9	6

Fig 1.2- Sent next time to user

Fig 1.1 is the random grid sent to the user’s mail. Now the one time password is the values in the registered indexes i.e.8035.If next time the user wants to transfer money again another random grid like fig1.2 is sent to the user’s mail. For this time the password is 2836, it changes each time. This is one of the enhancements proposed for strengthening the Graphical OTP, thus security is improved by applying this method in online transaction process.

4.4 Face Recognition using Python

The user’s face is recorded and stored. The system is trained with the user image dataset. Whenever the user accesses the account for the payment section using the device with a webcam, face recognition is done. After the successful verification the user can proceed to the transaction phase. If the verification fails, the transaction fails. The face recognition process is that the user face is recorded, this face image is converted into gray scale and stored. This is the input image and dataset for training the face recognition model. It ignores any scars or damages in the user’s face caused accidentally. During recognition the webcam is activated and the model recognizes the user, a rectangle is drawn around the user’s face and name of the user is displayed if the verification is successful otherwise it displays unknown user and the transaction fails.

4.5 Security Questions

The user registers the answers for the ten security questions like “What is your childhood nickname? What is the name of your primary school?” that are listed. In the transaction phase next to the face recognition/Graphical OTP verification the user can add the beneficiary details. Before completion of transaction two security questions are asked randomly from the registered questions. The answers are verified, next to that OTP is verified and then transaction completes.

5. ARCHITECTURE DIAGRAM

Fig2 is the architecture diagram. Initially the registration process takes place in the bank. The users are allowed to register in the registration portal. First the user chooses the security image category from the available four categories according to their wish. Then from the available nine images the user selects desired one this is first security image it is followed by selecting second security image from available nine images of mandatory category, these two images are the security image password of the user. Then there are about ten security questions listed, the user set answers for all the listed security questions. Next the security pattern is registered by the user, the 4 x 4 grid is displayed where the user can choose up to four indexes of their wish. The security pattern of that user is the indexes selected in the order. Last step in the registration process is the recording of the user's face. The user is asked to look at the webcam and the face is captured. After the completion of this process by the user, the security credentials are set to the user and online banking service is enabled to that user. Now the user can avail the online banking service anywhere. Each time the user wants to access his/her account the username, password is verified first, this is step1 verification. Step2 is the selection of security category followed by first security image and second security image verification. The user can view the account details, view the transaction summary and make transactions. Transactions can be done in the payment section. Whenever the user attempts to enter into the payment section, if webcam is available in the device then it requires face recognition if webcam is not available then it requires Graphical OTP authentication [1]. In face recognition technique the user in front of the webcam is validated and then the user can proceed further. In Graphical OTP authentication method the 4 x 4 grid of random numbers is sent to the user’s mail. It asks for OTP and validates according to the user’s security pattern, after validating the user can proceed further. The user adds the beneficiary details to make a transaction at that time two security questions are asked and answers are validated then OTP is verified and transaction completes successfully. Thus secure electronic transactions are carried out.

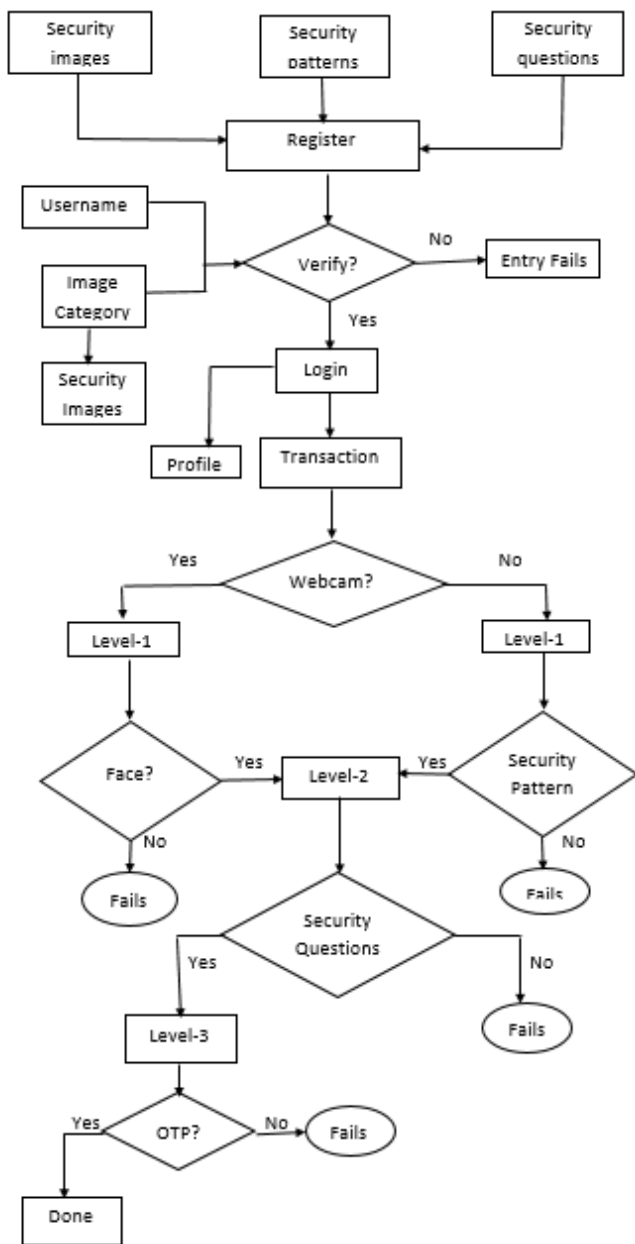


Fig2-Architecture Diagram

6. MERITS

Online banking services facilitate the users to do transactions. It comes with several edges, such as:

Convenience: Customers may use e-commerce web sites at any time. They merely would like an online connected device.

Costs saving: Data charges only applied from customers for each and every transaction.

Manage the customer’s account easily and editable. For each transaction, OTP will generate through email.

7. CONCLUSION

In this paper, we have reviewed various security electronic transaction techniques which are enhanced for better performance. The objective of the paper is to overcome the challenges associated with online banking security as well as

to realize the rising technologies. The electronic fund transfer is a major part of a financial function or transaction and it attracts extensive interest. Still, it needs to be converted into a regular approach for making payments. Though, the technologies used in payments through online are enhanced and also going through a noteworthy development in terms of security and service availability enhancement.

REFERENCES

- [1] Ravi Jhavar, Philip Inglesant, Nicolas Courtois, M. Angela Sasse, “Make mine a quadruple: Strengthening the security of Graphical OTP Authentication” University college London, Gower Street_London WC1E 6BT, UK.
- [2] V.Manju et al, “Improving Net Banking Security with Face Recognition Based Biometric Verification” Int J Sci Res CSE & IT. May-June-2019.
- [3] Jeonil Kang, Member, IEEE and DaeHunNyang, Member, IEEE “A Privacy-preserving mobile payment system for Mass Transit”, 1524-9050 © 2016 IEEE.
- [4] Mohammad Wazid, Sherali Zeadally and Ashok Kumar Das, “Mobile Banking: Evolution and Threats” IEEE Consumer Electronics Magazine_March 2019.
- [5] Nikhil Khandare, B.B.Meshram, "Security of Online Electronic Payments", for data retrieval easily and stores customer data by E-wallet.
- [6] S.Kiljan, K.Simoens, D.D.Cock, M.V.Eekelen and H.Vranken, “A survey of authentication and communications security in online banking,” ACM Comput. Surv., vol. 49, no. 4, pp. 61:1–61:35, 2016.
- [7] S.Roy, “Mobile banking in US to exceed 100 million by 2016,” Online Marketing Trends. Accessed on: May 2017.
- [8] R.Biddle, S.Chiasson and P.C.Van Oorschot. Graphical passwords: Learning from the first generation. Technical Report TR-09-09, 2009.
- [9] M. Bond. Comments on gridsure authentication. 2008.
- [10] S.Brostoff, P.G.Inglesant and M.A.Sasse. Evaluating the usability and security of a graphical one-time pin system. Conference on Human Computer Interaction BCS, 2010