International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

GRAPHICAL PASSWORD AUTHENTICATION FOR BANKING SYSTEM

Heera K[1*], Anusuya M[2], Kaviyaa V[3], Lavanya A K[4], Shanthi R[5]

[1,2,3,4]UG Students, Department of Information Technology, SRM Valliammai Engineering College, Kancheepuram, Tamil Nadu, India
Assistant Professor [5], Department of Information Technology, SRM Valliammai Engineering College, Kancheepuram, Tamil Nadu, India

---

Abstract - *A bank plays a vital role in people's life. Security of the customer is the major concern of the bank. The authentication must be secured in order to protect user accounts. The common technique which is used is textual password. The system demonstrates the security of the banking website through the graphical password to provide a promising alternative to the conventional alphanumeric password techniques. As there are a lot of security breaches that can happen to a banking transaction, the system attempts to secure the transactions by implementing two step verification process. The pass point based technique is used to secure the user's account from unauthenticated user during the login process. And the color palette technique is used to provide security to the customer's transaction in the banking system. By this way the chances of fraudulence gets reduced and the transaction becomes more secured. In addition, the functionality of the website is improved by its ability of identifying any unauthenticated user intending to interrupt the transactions. The process of Electronic filing is used to directly forward any irregular activities happening in the system to the authorities. Apart from filing the complaint, it automatically halts the transaction from further process. An authenticated user must be aware of the reasons of terminating the transactions in the middle, in case of any misuse. This is done by generating a message to the registered mobile number, the message states a justification of ending the process.*

Key Words*: *Security, Graphical Password, Pass Point, Color Palette, Click-Points, Authentication, Electronic Filing

1. INTRODUCTION

Bank has an important role in providing secure transactions to the customers and maintaining their details in a confidential manner. Each bank has their own constraints to secure client details and transactions that is both online and offline. Authentication is usually the first step encountered by users for a security-focused system. Authentication plays a vital role as it determines whether the user can be granted access to a particular system or not. The most comon way of authentication is alphanumerical password which have been used for decades. In addition, conventional passwords have significant security issues, due to the difficult combination of keys(which includes uppercase, special characters and numbers). Thus, human felt it so hard to remember those passwords. When they choose a straight forward password, this helps hackers to crack their passwords easily. The creation of a secure graphical password is to provide best possible usability and security. Here, the system follows a two step verification process to validate the authenticated user. In the first step the pass-point based verification is used and the color palette is followed as a next step verification. The user selects an image during the registration process and creates a sequence of click points. During the login process, the user needs to click on the same sequence. To continue with a successful transaction the user needs to enter the valid pin with the help of the color palettes.

1.1 OBJECTIVE

While using the pass-point verification and color palette technique, the system aims to provide Graphical Password as an alternative to the Conventional Alphanumeric password techniques and to provide an efficient way of verification to achieve confidentiality during the transaction. The functionality of the system is improved by the addition of Electronic Filing technique. The process is terminated in case of any fraudulence occurring in the system and to send an automatic notification to the user's registered mobile number in case of halts.

1.2 BENEFITS

The system is user friendly by making it easier for user such that it is not necessary to remember any sequence of items. The proposed system is not vulnerable to traditional attacks such as shoulder surfing, dictionary attacks, spyware attacks and guessing attacks. Details of the customer is maintained confidentially by graphical password technique. The system is less vulnerable to brute force attacks compared to traditional system. The confidentiality is high where the images are uploaded by one user is not visible to others.

1.3 CHALLENGES

Based on the survey, the systems are prone to attacks such as shoulder surfing, dictionary attack, guessing attack. Retrieval of images from the database is tedious and time consuming. Presenting more pictures on the screen, user cannot distinguish the images from one another. The recognition based technique requires more storage space. Crackers can guess the image patterns easily.

2. LITRATURE SURVEY

The systems have encountered many reference papers, this work enabled to understand the graphical password authentication in a better way.

[1] Mudassar Ali Khan, et al.in "g\RAT A Novel Graphical Randomized Authentication Technique" for Consumer Smart Devices, IEEE Transactions on consumer electronics, 2018.

The gRAT system is also a graphical watchword technique that uses photos that unit of measurement bestowed in Associate in Nursing passing 3x3 grid. Among the system the place of pictures changes whenever a user wishes to be real.

[2] Muhammad Ahsan, et al.in "Graphical password Authentication using Image Sequence", International Reseach Journal of Engineering and Technology(IRJET), 2017.

In this methodology, user will transfer photos and it not visible to different users. In Recognition based technique, multiple photos unit of measurement shown to the user in random order.

[3] Weizhi Meng, et al.in "Enhancing the security of FinTech Applications with Map-based Graphical watchword Authentication", ELSEVIER, 2019.

This scheme requires users to make a route on world map as their credentials. The creation of a route is believed to produce hints for users to remember their multiple passwords in a usable way.

[4] Vijayakumari Rodda, et al.in "Multi-level Graphical Password Authentication scheme for cloud(MGPASC)", International Journal of Recent Technology and Engineering(IJRTE), 2019.

An authentication mechanism is the combination of two techniques such as graphical password and textual password. This methodology provides the encrypted format using Caesar cipher technique.

[5] Li and J.du, "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing", Iet information security, 2018.

Particle Swarm Optimization (PSO) is also a computing methodology that optimizes a tangle by iteratively creating an effort to reinforce a candidate resolution with relevancy a given live of quality.

[6] Graphical password Authentication, 2019.

Graphical watchword schemes has been used as a numerous to text based schemes, motivated half by the actual fact that humans can detain mind footage more than text.

3. MODULE DESCRIPTION

(i) REGISTRATION PHASE

The user who is new to the website initially needs to register in this phase by providing all the relevant information. Here, the customer is free to set their own pin.

(ii) LOGIN PHASE

The users are required to provide their registered mobile number as their user name.

(iii) PASS-POINT VERIFICATION

The image which the user selected and generated the click points during the registration phase. The sequence of the click points must not be changed to identify them as an authenticated user.

(iv) PLACE ORDER

This phase works as a normal e-commerce site where the customers place their orders on required products.

(v) MONEY TRANSACTION

User select the person to whom the money is to be sent. After selecting the user, the user is directed to the pin entry phase for the authentication purpose.

(vi) PIN ENTRY

In this step, the user has to select the appropriate pin which was set during the registration phase using the color palette. In case of exceeding three chances of incorrect pin entry, the process is terminated automatically.

(vii) VIEW TRANSACTION DETAILS

Here, the user can view all the transactions performed by them.

4. SYSTEM DESIGN

The user interface is created using html, css, jquery, javascript and the language php is used. The backend process is MySql.

4.1 ARCHITECTURAL DESIGN

The proposed system uses the session password mechanism for providing security to the user's transactions, where in the first step is secured using the pass-point technique. In this technique, the click points in the images generated by the user during the registration process is used to validate the authenticated user. The second step of the verification is carried away with the use of color palettes. Here, instead of the usual number pad, a pair of colors is displayed for each number. And the authenticated user is allowed to proceed with further transaction. When a user exceeds three chances of entering a valid password, then he/she is identified as a misuse and a complaint is filed against them through the Electronic Filing mechanism. In case of any unusual amount transaction, the user is confirmed by sending an one time password.

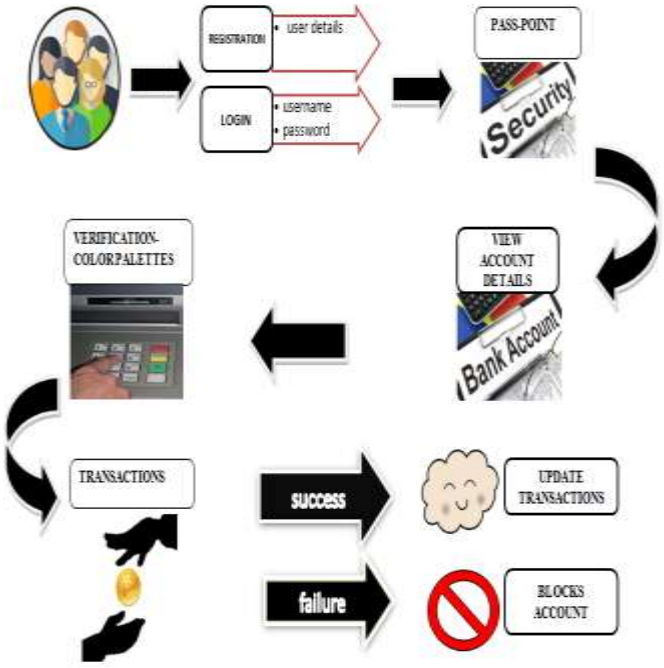

Fig -1: Architecture Diagram

4.2 PROPOSED METHOD

Pass-point Technique

Image submission: The user uploads an image from the system and submit it during the registration phase.

Image password point mark: The user clicks on the various points on the loaded image.

Tolerance calculation: The tolerance value is set to every point and it is measured and verified during the login process.

Authentication: When the points clicked on the same image, during the login process is within the range of tolerance value the user is authenticated.

Fig-2: Pass-Point Verification

Color palette Technique

Color palette technique is implemented when the user proceeds for the transaction process, here the pair of colors will be displayed for each number instead of a numerical keypad. The user selects one of the random color for each pin and randomization of colors is carried out at each pin entry. The user interface is designed with three rows, the first row represents validation box, the next comes the color pad and the last row represents the colored boxes where pin accessing takes place.

Fig3: Color palette implementation: user selects pink color for first pin number 1

Fig 4: color palette implementation: user selects the green color for first pin number 1 to validate it.

1. User needs to select one random color from the pair of colors.

2. The validation of the first pin occurs only after repetition of first step.

3. The above mentioned steps is followed by the user to access other three PIN numbers.

4. When all the PIN entered is validated correctly the order is placed.

Fig 5: Color palette verification: The first pin is validated by clicking the correct color

Electronic –filing: When the user enters the invalid PIN, 3 times the account gets blocked and the IP address of the unauthenticated user is notified and the information is sent to the higher authority through mail.

5. CONCLUSION

In the proposed system, the traditional alphanumeric password is replaced by the graphical password technique. The system provides efficient way of verification to achieve confidentiality. The proposed system provides more security by using two step authentication. The pass-point technique is used to authenticate the authorized user during login phase. After successful authentication, the user may proceed to transaction. The proposed system uses color palette technique during the transaction phase. The Neuro fuzzy methodology is used to generate the random colors at each pin entry. The system has overcome the shoulder surfing attack where the hacker cannot crack password easily. The proposed system provides E-filing and automatically terminates the process in case of any fraudulence detection.

5.1 FUTURE WORK

In future, for a more reliable and less complex system the security of the system can be improved by substituting advanced techniques. This web applications can be implemented in various real-time scenarios like business, telecommunication, military, banking etc. The accuracy can be further increased by adding more click points in the pass point verification process and combination of colors used can also be improved like ($10C_{10}$). In this era, security becomes core of the arising technologies and the computer crime in the banking system will be considerably reduced.

REFERENCES

[1] Mudassar Ali Khan, Ikram ud din∗ senior member ieee, Swayer Ullah Jadoon, Muhammad Khurram Khan∗ senior member ieee, Mohsen Guizani fellow ieee, and Kamran Ahmad Awan, “g-rat | A Unique Graphical Randomised Authentication technique for client good devices” , 2018 ieee.

[2] Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande laptop engneering, rtm Nagpur University, M.I.E.T Bhandara, “Password Authentication Victimisation text and colours “, issn 2278 – 0882 volume four, issue 3, march 2015

[3] M. H. AU, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate Based Mostly (Linkable) Ring Signature,” in proc. inf. security follow expertise conf., 2007, pp. 79–92.

[4] M. H. AU, Y. MU, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious Kgc Attacks In Certificateless Cryptography,” in proc. second acm symp. inf., comput. commun. security, 2007, pp. 302–311.

[5] S. Habib, S. Hauke, S. Ries, and M. Mhlhuser, “Trust As A Helper In Cloud Computing: A Survey,” journal of cloud computing, vol. 1, no. 1, 2012.