TEST Engineering & Management

May-June 2020
ISSN: 0193-4120 Page No. 5313-5315

A Revamp Authentication System for E-Banking

[1]S. Christy, [2]A. Gayathri, [3]J. Rama

[1]Assistant Professor, Department of Information Technology,
[2]Associate Professor, [3]Assistant Professor, Department of Computer Science and Engineering,
[1,2,3]Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science,
Chennai, Tamil Nadu, India
[1]Christys.sse@saveetha.com, [2]Gayathribala.sse@saveetha.com

Article Info
Volume 83
Page Number: 5313-5315
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24February 2020*
Publication: *16 May 2020*

Abstract

Security plays an important role in any transactions in E-Banking. The main objective of this paper is to propose the smart way to authenticate the user in the bank and access the account through the pictorial password. This is achieved by providing the indirect pin. The pin should predict the original password. Previously the server provide the pre-defined image as a password image and the users used to upload or select the image. But that was having some limitation. There is no security to the user's account if any intruder provides some password to the user's account. This system is designed by introducing the OTP in an image method. An effective E-banking service is achieved by using the E-pay. It also provide security to the customer's account from an unauthorised person. This is done by identifying the person who enters the wrong password frequently. This system provides a proper way to transfer the amount from one user to another user. The methods used in the system are to be provided to ensure the security for the banking sectors.

Keywords**:** *OTP, Image Processing, Encoding, KHMAC Algorithms.*

1. Introduction

The information is protected from theft and damages only by the help of cyber security. The system is designed to propose the smart way to authenticate the user to access the bank account. The password is hidden inside the picture can be obtained with the help of indirect pin. This helps to get the original password using temporary login indicator. Using this the account holder can login and get access to banking features. The server will provide a password by uploading the predefined image whenever the user needs to authenticate. The user has to select an image as password. The selected image is processed by the server by splitting the image into 10x14 grids and display all the grid images to the user. The user has to select the single grid as a password grid for a particular image. Then the user gets number of images as needed by the user and he has to select the each grid as a password for an image. When the server identified the user is an authenticated person send the login indicator. The user can login with the help of login indicator. The proximity sensor in user device hold the screen in circle image protecting the password.

2. System Design

The user is provided with the password image.

The image can be splited into 10x14 grids and display the gridded images to the user. Then the user has to select a single grid as a password grid in that particular image. The system user has to choose one grid as a password for an image. When the user is login with the provided login indicator, the login indicator is visible when the user is holding the proximity sensor of the user device. The user can move the horizontal and vertical bars using navigation keys available. The user has to

May-June 2020
ISSN: 0193-4120 Page No. 5313-5315

choose the correct password grid and press ok button. Like this the user has to select the correct password image grid in all the provided images. These images are sent based on the images chosen at the time of registration.

3. System Architecture

The E-Banking system is the system that provides security and efficient services to the customers. It is possible to get the password if the user forgot it. The password can be sent to the user to his personal mail after asking so many questions to the user. If an unauthorised person try to access the password can be identified and intimated to the account holder. This system provides high security.

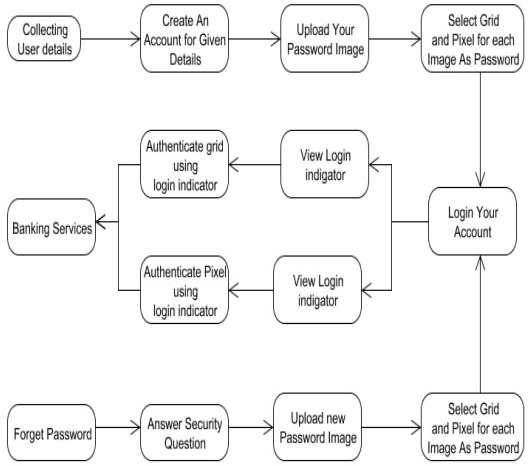

Figure 1: System Architecture

4. Methodology Used

There are two Algorithms used in the system. They are Encoding and KHMAC algorithms.

Encoding Algorithm

Encoding algorithm is a group of binary to text encoding schemes. The set of characters used to represent the members of the encoding protect the information. The information systems, Multipurpose Internet Mail Extension (MIME)'s also uses the encoding algorithm.

KHMAC Algorithms

A Keyed-Hash Message Authentication Code (KHMAC) is a cryptographic hash function and it provides a secret cryptographic key. The data integrity and the authentication of a message is verified by Message authentication code. The cryptographic robust of the KHMAC depends upon hash function and the size of its hash output. The KHMAC varies when the size and quality of the key changes. The message is broken into fixed sized blocks. An iterative compression hash function is used to breaks up a message into fixed sized blocks.

5. Method Description

Security is ensured by providing the new login indicator and gridded password image. The image is appeared with movable horizontal bar and vertical numeric bar. The movable horizontal bar and denotes the alphabetic value and movable vertical bar denotes the numeric values. Based on the grid values the server confirms that the grid will be authenticated, and checks with new login indicator. Once when the user is completing all image authentications, the services will be provided to the user.

Authentication Using Proposed Graphical Authentication

After seeing the login indicator with numeric values, the authentication process started. The user will upload the image with the numeric values scattered in the image. The user has to drag the numbers and place the numbers in the password field. The image in which the numbers are hidden is specified during the time of registration.

Recovery Module

The recovery module is used to support the user in case if he forgot his password. This can be rectified by asking problem can be rectified by asking security questions about the user and confirmed that he is the right user. This helps him access his account with the new password given by the bank authority.

E-Banking Services

Now a days the entire world is suffered by COVID-19. Everybody got lock down inside their house to avoid the spreading of the virus. E-Banking services plays a vital role and providing all sort of money transactions through online.

6. Results

The E-Banking system supports the user by providing friendly and an interactive environment to the user. This E-banking service provides high security to the authentication system so that unauthorised person cannot be able to access the customer accounts. Entering the password is also a complicated task, to maintain the security. Every application has its own merits and demerits. Changing the existing modules or adding new module scan appends improvements. Further enhancements can be made to the application, so that the website functions very attractive and useful manner than the present one.

7. Conclusion

The system is working perfectly after testing with various data. Using encoding and KHMAC algorithms, the message can be secretly transferred to the user. Authenticated user only can access the bank and the forget password can be recovered from this system. This system can be extended further by getting messages if unauthorised user tries to access the account. The system has covered almost all the requirements of the user and works efficiently.

May-June 2020
ISSN: 0193-4120 Page No. 5313-5315

8. Images

Figure 2: Upload Image

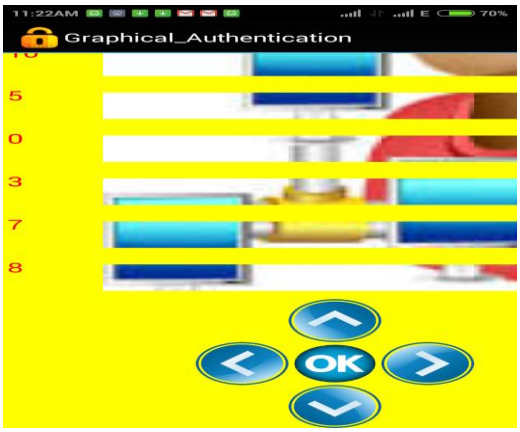

Figure 3: Image Grid Authentication

References

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings ofthe 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[5] "Realuser," http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63,no. 1-2, pp. 102–127, 2005.

[8] A. Paivio, T. Rogers, and P. Smyth, "Why are pictures easier to recall than words?"Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology:Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[10] S. Brostoff and M. Sasses, "Are passfaces more usable than passwords? a field trial investigation, "PEOPLE AND COMPUTERS, pp. 405–424, 2000.

[11] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "VIP: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.

[12] B. Ives, K. Walsh, and H. Schneider, "The domino effect of password reuse," Communications of theACM, vol. 47, no. 4, pp. 75–78, 2004.

[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.

[14] T. Kwon, S. Shin, and S. Na, "Covert attention shoulder surfing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6,pp. 716–727, June 2014.

[15] "Google glass snoopers can steal your passcode with a glance," http://www.wired.com/2014/06/google-glass-snoopers-cansteal-your-passcode-with-a-glance/.