THE USE OF SECURITY IMAGES IN INTERNET BANKING

Sanchayani Gaikwad[1], Kalpana Gawali[2], Pallavi Kanawade[3], Ankita Karajkar[4]

[1] *Bachelor of Engineering, Computer, AVCOE, Maharashtra, India*
[2] *Bachelor of Engineering, Computer, AVCOE, Maharashtra, India*
[3] *Bachelor of Engineering, Computer, AVCOE, Maharashtra, India*
[4] *Bachelor of Engineering, Computer, AVCOE, Maharashtra, India*

ABSTRACT

Internet banking websites often use security images as part of the login process, in that they can help foil phishing attacks. Previous studies, however, have yielded inconsistent results about users ability to notice that a security image is missing. This project describes an online study of users that attempts to clarify the extent to which users notice and react to the absence of security images. Most participants entered their password when the security image and caption were removed. The authors found that changing the appearance and other characteristics of the security image generally had little enact on whether users logged in when the security image was absent. Additionally, they subjected the passwords created by participants to a password-cracking algorithm and found that participants with stronger password were less likely to enter their passwords when the security image was missing. In Mail, messaging, data sharing and computational services are shared under the Internet environment. User *access on the services is allowed with reference to the user account information. So,User ID and passwords are applied in the user verification process. In this,Graphical passwords are used to verify the users. Captcha techniques are employed to identify the request is received from the machine or human. Captcha as Graphical Passwords (CaRP) technique integrates the Captcha and Graphical passwords methods. Therefore,pixel location and color based pattern analysis methods are employed to control guessing attacks. Cryptography and data integrity verification methods are used to handle directory attacks and transmission attacks.*

Keyword:-*Sitekey,Security,Onlinebanking,Authentication,Variable,token,Human-ComputerInteraction,IT Security.*

1. INTRODUCTION

Internet banking is a self-service that allows customers to perform financial activities over the Internet. Internet banking is the latest delivery channel for financial services. Software and building architects have many similar issues to address, and so it as natural for software architects to take interest in patterns as architectural tools.There is not a singled basic definition of Internet banking that is being used universally.It is also commonly commonly known as online banking or banking. So far limited studies have tried to deal with this problem. Therefore, this research investigated factors that influence individuals' acceptance of Internet banking services, and used the sampling frame.There has been a lack of consensus in the definition given by researchers. Regardless of the differences in definition, Internet banking refers to many kinds of electronic services through which bank customers can request information and get most of the retail banking services via a computer. Internet banking has been

defined from different school of thoughts by various researchers depending on their experience, nature and study environment .For this research, Internet banking is defined as a self-service that enable bank customers to get access to their accounts and the latest general information on bank products and services, and conduct all financial transactions anytime from anywhere through the use of a bank's website[8].

.1.1 Verification:

Verification module is used to verify user identity. It consists of two types of verification:

1) Images Selection :

The user is responsible for selecting the various images from cloud to verify his authentication.

2) OTP Verification:

The OTP is send to the user who is completely authorized.This verification is two way authentication[2].

1.2 AES Operation:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations)[1].

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix .

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

2. RELATED WORK

Most current graphical password schemes require users to enter the password directly,typically by clicking or drawing. Hence, passwords are easily exposed to a third party who has the opportunity to record a successful authentication session. There have been a few graphical password schemes devoted to secure passwords against spyware attacks .In the following, several representatives will be described. Man, et al proposed that users remember a number of text strings as well as several images as pass-objects. To pass the authentication, users should enter the unique codes corresponding to the displayed pass-object variants and a code indicating the relative location of the pass-objects in reference to a pair of eyes. It is relatively hard to crack this kind of password, but the complex memory requirement is an obstacle to its popularity[11].

3. SYSTEM ARCHITECTURE

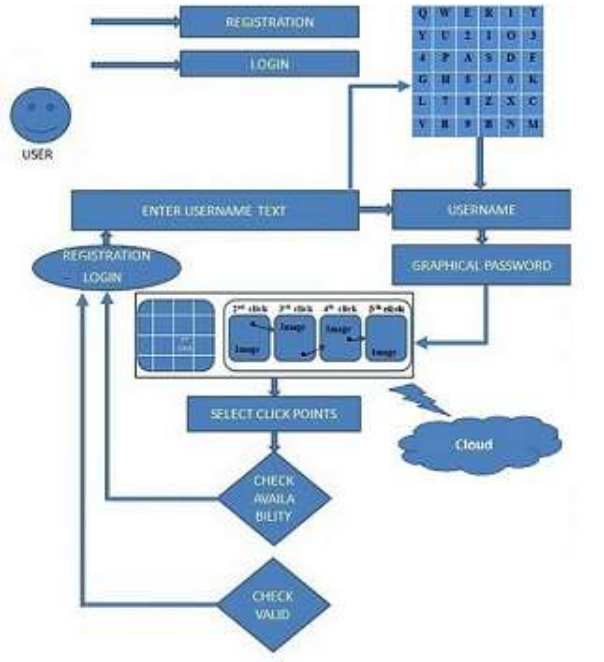

Fig-1: System Architecture

During registration phase user submits the username. Minimum length of the username is 4 and it can be called as secret username. The username should be of characters or numbers or combination of both. During the login phase, the user enters his secret username using the grid-based interface display. The grid is of size 6 x 6 and it consists of letters and digits. The letters are in upper case and small case to provide more options. The letters and digits are randomly placed on the grid and the interface changes every time. As the grid gets shuffle at every time, it prevents from the attacks like shoulder surfing.

4. SYSTEM CONCEPTS

In this system, there are two types of authentication:
1. Two way authentication
2. Short time password using cryptography

The above two approaches are explained below in fig1 and fig2.The fig 3 illustrates the in general working of system where as fig 4 shows that how each use cases in system is connected to end user use cases. The fig 5 illustrates how the data is flow from one end to another end[9].

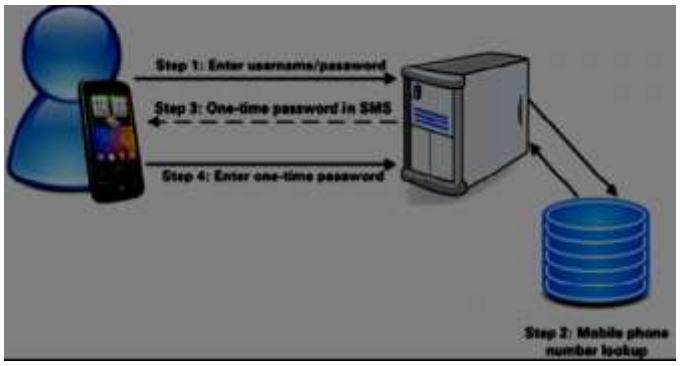

Fig-2: Two Way Authentication

Two factor authentication approach uses two things. Things can be user knows, user possesses and user has, to give a much stronger level of authentication. The first factor is something user knows, in this case username and password. The second factor is something user has, in this case your phone or app-running tablet[1].

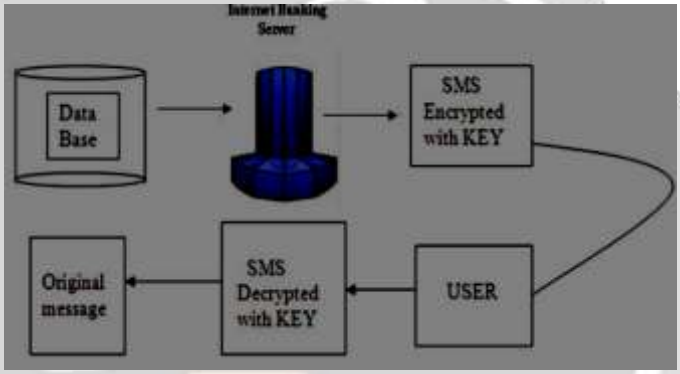

Fig-3: Short time password authentication

Short-time password authentication method using symmetric cryptography in combination with a Software Security Model is a one approach for authentication. In this approach encryption and decryption is performed.

5.IMPLEMENTATION

1.SignIn-

Sign in modules includes all details about bank as well as personal information of customer.The major task over this module is selecting the correct sequence of images which will be follow during signup process to provide security.

Fig 4: Sign Up

2.Login:

The sign in module includes user name and password used after the registration is completed. This module used for authendication.

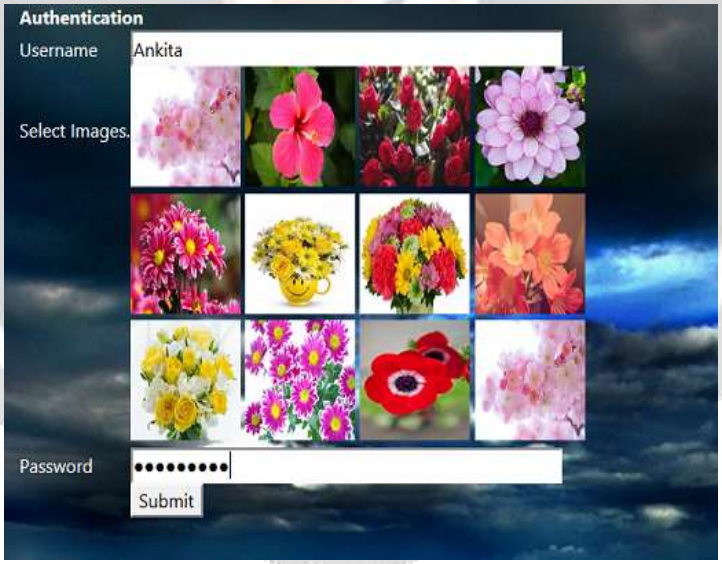

Fig 5: Login

6. CONCLUSION

The vulnerabilities of textual password to method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics.

7. ACKNOWLEDGEMENT

We have a great pleasure in presenting paper "**THE USE OF SECURITY IMAGES IN INTERNET BANKING**". under the guidance of **Ms.K.U.Rahane** the faculty which has always been a source of inspiration and a power house for all the enthusiasm. Thank you for always correcting us whenever and wherever necessary.

8. REFERENCES

[1]. Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle "Graphical Password Authentication Using Cued Click Points"School of Computer Science, Carleton University, Ottawa, Canada.

[2]. Ms. Arati A. Gadgil "Do Security Toolbars Actually Prevent Phishing Attacks"Authentication Approaches for Online-Banking(Nov,2012)

[3]. Ian Jermyn, Alain Mayer "The design and analysis of graphical passwords" Proceedings of the 8th USENIX Security Symposium(1999)

[4]. www.sbi.com

[5].Susan Wiedenbeck "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice "Computer Science Department.