Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secured Transaction Using Secured Image

MR.K.Shankar[1] , L.Nachammai[2], V.Rizwana[3] , G.Umamageshwari[4]
[1] Assistant professor-I, [2,3,4]Student , Department of Computer Science
Prathyusha Engineering College, Chennai, India

Abstract: ***The Image processing is manipulating the image to provide a high quality of it.To improve the security in internet banking. The internet banking system has login using password and user id which can be captured in internet centre or by hackers. The main disadvantage of existing system is security is missing during transaction of money through internet.In this system the security is provided by giving captcha image during registration and asking user to select it any one and it will be asked for each and every time during sign in.Not only captcha we use a secured image and ask user to select any two co-ordinate points during registration which will be used during transaction process.The advantage of the proposed system is the user can use internet for transaction of money with security and no one hack our account.***

I. INTRODUCTION

Internet banking system provides many security measures for safety purpose. But it is not efficient. Initially banking system uses only user id and password for security but it can be hacked by any hackers easily. These issues are overcomes in the existing system. The existing system uses secure images for safety and the users are notice that secure images are missing or incorrect whenever the login into it. But 73% of user's are simply logging into it without noticing the secure image and the biggest disadvantage is that we are using security in banking to safeguard our money. But in the existing system the secure image nowhere deals with money transaction. It is the biggest drawback in the existing system.

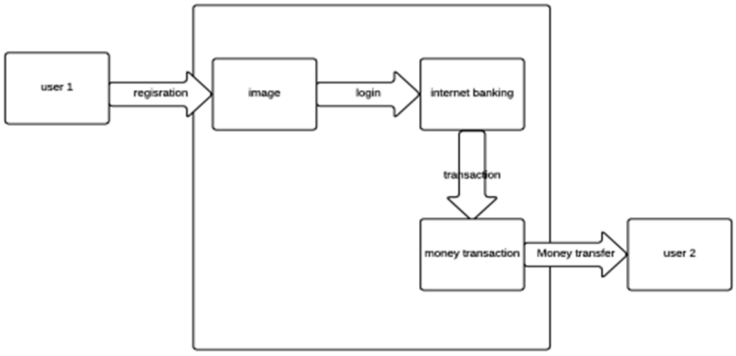

Fig 1 System architecture for Existing system

II. PROPOSED SYSTEM

These problems are overcomes in the proposed system. The proposed system use secure image and Captcha for security purpose. In the registration process user are asked to enter the user id and password. Then the user is displayed with the Captcha and users are instructed to select one Captcha from the given 3 Captcha. The selected Captcha should be entered and clicked. After that user will be provided with an secure image and user have to select two position. The selected position are converted to pixel to identify the exact position. The pixel are stored in x and y co-ordinates. Then the user have to click register button and the registration will be successful. After registration the admin will give user the authority to access your account then only the user can access the account. If the user want log in to his/her account he/she should enter the user id, password and also the recorded Captcha which the user have selected during the registration process and during money transaction the user will be displayed with the same image which he/she have selected during registration process and he/she have to select the exact same position which he/she had selected during the registration process and user have to record it.If some tries to hack your account he/she will not be able to select the same captcha which you have selected.If they hacked your captcha and log in to it during money transaction they have to select the exact same position which you have selected during the registration.But its critical for the hacker if once the hacker have selected the wrong position user account will be blocked and the user will get a mail that your account is deactivated.Then after informing the admin the admin only has the authority to unblock a particular account.It will be the best safety for the user. If the user itself

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

wrongly clicked the captcha or the position the account will be blocked and you will get the a mail that your account is block to that mail you have to send a reply mail that its user and user have to request for the position.

III. ARCHITECTURE DIAGRAM

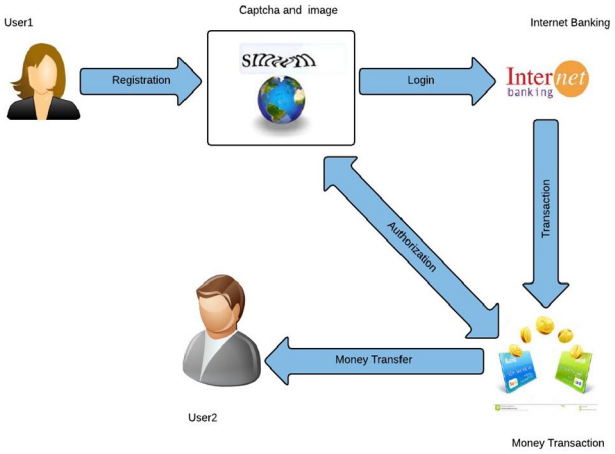

Fig 2 System Architecture for proposed system

IV. ALGORITHM

We are using two algorithms in this project one is for Captcha generation and another is for image co-ordination. Initially we are storing nearly 200 Captcha in the database. While the user he/she will be provided with the Captcha which is taken from the database in random manner using a random method.

```
anum = (Math.floor(Math.random()*191))+1;

imgid = parseInt(anum);

document.getElementById("txt").value=anum;
```

For Image co-ordination we have stored the default image in database for e.g. picture of Tajmahal. Whenever the user register he/she will be provided with the default image which we had stored in database. Then the user is instructed to click the two points in the image, the co-ordinates of the points are calculated using X and Y co-ordination algorithm.

```
for( var posX = 0, posY = 0; oElement; oElement = oElement.offsetParent )
  {
   posX += oElement.offsetLeft;
   posY += oElement.offsetTop;
  }
  return [ posX, posY ];
```

V. AUTHENTICATION AND AUTHORIZATION

In this module first user have to register then only She/he can access the online banking. During registration user will provided with Captcha and he has to select any one of it .Not only Captcha we has to select security image from list and select any two co-ordinate points. During login user has to give correct captcha if he gives wrong captcha the account will be blocked. The

authentication and authorization will provide system to protect itself and protect against un authorized usage.

VI. GRANT ACCESS

Admin will give permission to user accounts, once the user registered.Admin can Block and Unblock the user accounts.The user account will be blocked, if the user chooses wrong Captcha.Admin is the only person who can unblock the account.

VII. BANK MANIPULATION

We can do any manipulation like any other Banking Web sites such as deposit, transaction, withdrawal, Balance Checking etc.The user can create Savings or Current Account.The user can deposit amount, withdrawal amount from their account. If the withdrawal amount is higher than the Balance amount, the user will not able to withdrawal the amount.

VIII. IMAGE CO-ORDINATION

When the user try to transact the amount to other accounts, then they have to authorized using image co-ordination.The user should enter correct image coordination to transfer the amount.She/he cannot transfer the amount using incorrect image co-ordination.It helps the user to secure the overall banking experience.

IX. CONCLUSION

In that prior work, participants were particularly alert to phishing attacks. We believe our study, particularly helps the users efficiently by means of whenever hackers tries to hack our account and transact the money immediately the user account will be blocked and user will receive a mail that their account is deactivated which helps the user to find that someone had tried to hack their account. It will alert the user and make them to react immediately to the consequences which will helps the users account to be secured. In the low scale our project will be more effective among all users.

X. FUTURE ENHANCEMENT

In Security in internet banking using secured image provide authentication to the user by checking where the co-ordinate generated by user is matched against the co-ordinates stored in database. The co-ordinate are generated from the image which was uploaded only by admin not by the user which will be easy for hackers to transact the money by using some probability of image co-ordinates. So the security can be provided at high degree by using the image uploaded by the user.

REFERENCES

[1] Bank of America (2013) “Site Key FAQs”
[2] A.Herzberg and R.Margulies. “Forcing Johny to login safely”,in Proceedings of 16th European Symposium on Research in Computer Security,2011
[3] M.Wu.R.C.Miller and S.L.Garfinkel, “Do security toolbars actually prevent phishing attacks?”,in Proceedings of the SIGCHI Conference on/human factors in Computing Systems,2010
[4] J.Sunshine,S.Egelmann,H.Almuhimedi,N.Atri,L.F.Cranor, “Crying wolf:An Emperical study of SSL warning effectiveness,” in Proceedings of the 18th USENIX security Symposium,2009
[5] I.Jermyn,A.Mayer,F.Monrose,M.K.Reiter and A.D.Rubin, “The design and analysis of graphical passwords,” in Proceedings of the 8th USENIX Security Symposium,1999