International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Implementing Authentication, Authorization and Access Technique using Session Password with Pair-based Scheme

Mr. Suraj R. Deulgaonkar
Student of Master of Engineering in (CE),
Sipna College of Engineering and Technology, Amravati, India
surajdeulgaonkar@gmail.com

Prof. Vijaya K. Shandilya
Associate professor
Sipna College of Engineering and Technology, Amravati, India
vkshandilya@rediffmail.com

Prof. Vishwas T. Gaikwad
Associate professor
Sipna College of Engineering and Technology, Amravati, India
vtgaikwad@rediffmail.com

Abstract-*One of the severe issue that is occurring with the todays computing world is with "AAA" that is Authentication, Authorization and Access. Out of which the authentication mechanism is to use alphanumeric usernames and passwords that are most time prone to the dictionary attack, shoulder surfing attack, etc. Instead if the password should get validated with the numerals and special characters, one cannot avoid the above mention attack. So, after some time the literature studies suggested that Graphical password scheme is introduce, that makes the combination of alpha numerals along with images and try to add one more level of security. But still this scheme is also more vulnerable to shoulder surfing attack. So, to address this kinds of issues we will try to propose the new scheme of session password, i.e. the password once user has been entered is not valid for the next login session. And along with this we have choose the pair based scheme to choose our session password which is much more vulnerable to shoulder surfing attack and as the password is valid only for single session and for the next session one has to entered the new password it will definitely add the stronger security to authentication process.In this paper, we have implemented multilevel security framework that support AAA mechanism for providing the security by taking the example of online banking application.*

Keywords:Session Password, Pair-Based Scheme, Shoulder Surfing attack, Authentication Authorization and Access (AAA) Mechanism.

I. INTRODUCTION

From last many years, the most popular user authentication approachis the text-based password scheme in which a user entersa login name and password for getting access to any kind of application on the computer system. After some years we come to know that, despite of its wide usage, thetextual passwords have a number of short comes. Thesimple and straightforward textual passwords are easy toremember, and at the same time they are more vulnerable for attackers tobreak [1]. So to avoid this one should enter the complex and arbitrary passwords that makes the system more secure, resisting the brute forcesearch and dictionary attacks, but the difficulty lies inretaining them [2], as with the growing use of digital activities any single users have many numbers of password. But instead of all that, textual passwords areliable to the shoulder-surfing, hidden cameras, and spywareattacks.

Consequently, after some years literature shows that graphical password strategieshave been introduced as a substitute for textual passwords schemes. As the pictures/images are used in the graphical passwords, which can be easily remembered as compared with words. Furthermore, it also seems difficult toformulate automated attacks for graphical passwords.Moreover the graphical password requires more space as compared to our traditional text-based scheme and hence probably providing a higher level ofsecurity means [3]. With these reasons, many user are intensifying interest in the graphical passwordmethods.However, most of the existing graphicalpassword authentication methods suffer from

shoulder surfing attack, it is a known hazard where an intruder can scrutinizethe password by recording the authentication session orthrough direct surveillance when any user is perform login to his account. Even though there are some of the graphical password that procedures resistant to the shoulder surfing attack, but they also have their own downside like usability issues or consuming additional time for user to login or having some tolerance levels [3] in them also. Along with this issues, the cost of installing the graphical password scheme is much more as compared to our traditional text based scheme.

Based on these and some other reasons pointed out, one of the new scheme for authentication is investigated that is called as session passwords scheme. Session passwords arethose password that can be used only at that particular time instant and for that particular session. Assoon as the session expires, the password is no longervalid for that user to login in his account. As such the user, usesthe distinct passwords eachtime he logs into the session.In this paper, we have designed a project based on the application of online banking whoseobjective is to provide more secureand confidential banking service to all the users of the system [4].Instead of that our proposed scheme of session password using pair based scheme is mostly useful foe any sort of application / organization where security is an acute concern. Here, we have make the use of all the three mechanism of security that are Authentication, Authorization and Access (AAA). For Authentication scheme, we have use the Session password using on the pair-base scheme which is used by the user for each time the user makes login to his account [7]. For providing Authorization, our application project has the administrator module, any user who needs to the access his account has to first get authoriazed by the administrator (admin) of that particular application/organization. And finally the security level of providing access is achieved by both the mechanism that administration authorization and User login using pair based authentication scheme of session password.

The rest of the paper is organized as follows, Section II Gives the introduction of proposed scheme of Session password using pair based mechanism. Proposed project work that takes the example of more secure online banking isdepicted in Section III. Section IV gives conclusion tothe paper. Future Scope is pointed out in Section V.

II. PROPOSED PAIR-BASED AUTHENTICATION SCHEME

Firstly at the time of registration, the user submits his own secret password. The length of the secret password should be any numberbutif it contain even number of characters is very good.During the primary level authentication, when the userchooses the pair-based authentication scheme, aninterface that consisting of 6X6 grid is displayed when there is time to submit your password. The gridcontains both all 26 alphabets and 10 numbers which are placed atrandom and the interface for the keyword changes every time.

The working mechanism involved in the pair-basedauthentication scheme is as follows:

- Firstly, the user hasto consider the secret pass in terms of pairs.
- The firstletter in the pair is used to select the column and the secondletter is used to select the row in the 6X6 grid, respectively in which these letters are come. Theintersection letter of the selected column and row generates the character which is a part of the sessionpassword.
- In this way, the logic is reiterated for all otherpairs in the secret password [6].
- If the secret password entered at the time of registration is of odd characters then the last odd character should be entered as it is, to make successful registration.
- Thereafter, the passwordinputted by the user i.e. the session password is nowverified by the server to authenticate the user.

Consider the following example-If the password is SURAJ, Consider the password selected in pairs.Search for the letter which is in the intersection of the pair of the letters, considering the column of first letter and row of second letter. The session password generated in the output is ‘y0j’.

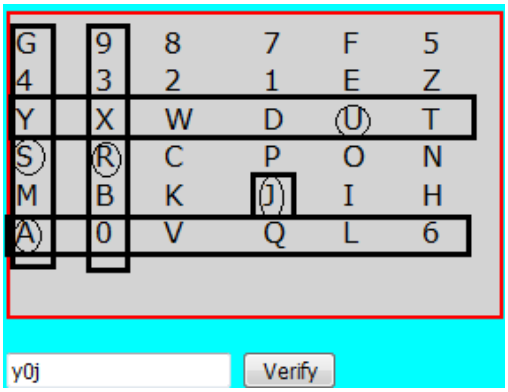

Fig.1: Pair Based Scheme

III. IMPLEMENTATION OF PAIR-BASED SCHEME FOR BANKING APPLICATION

Here, we have designed and implemented the pair based authentication scheme using session password for online banking application, where the security is of paramount importance. As stated earlier that we are creating the multilevel security framework that support AAA mechanism for providing the security. Here at the initial stage the user is performing simple registration to our portal

for using the benefits of online banking. At the time of registration user has to enter his password that can be used as the checksum as authentication parameter for all the time in future when that user performs login to our portal. The simple registration window of our framework is shown in the fig. 2 below.

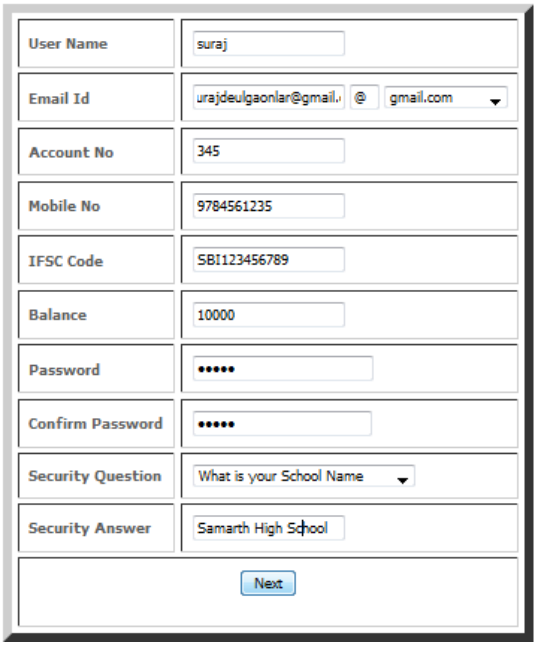

Fig. 2: Simple user registration for online banking

As in the above fig. 2 the user has entered his personal information and password for his account on Online banking portal. After entering his registration information the new user has to be authorized by manager of that bank. The activation of the accountfor newly added user named 'suraj' done by manager of that bank is shown in the fig. 3. Manager also has facility to delete any user from his online banking portal.

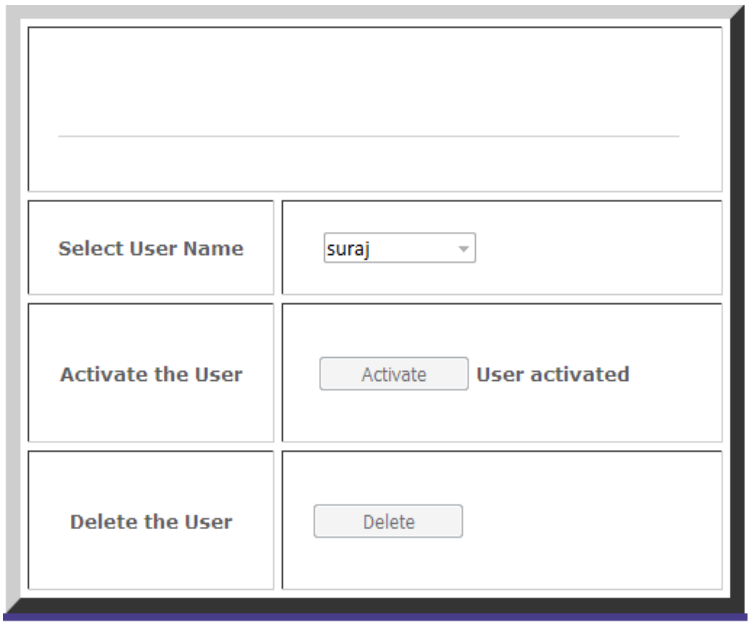

Fig. 3: Admin authorization to newly added user

Now, only after the new user gets authorized by the manager of that bank, he is able to use the facilities provided in our online banking portal. At the time of using our Application software for performing online banking transaction all the registered and authorized user has to login first. So, user come across the login window which is somewhat different than all other web application, because here user has to enter only his User Name first. The simple login window is shown in the fig 4. By checking the user name from the database the page is redirected to the special page for entering the password of that user in the pair-based scheme, which is shown in the fig. 5.

Fig. 4: Simple user login for online banking

In the fig. 3 the user name 'suraj' is performing login to our portal, he is redirected to the page (shown in fig. 4) for entering his password in the pair-based scheme, which is also a session password. The pair-based scheme is work as the steps mention in the proposed methodology. Here, the

password entered by the user named 'suraj' is also 'suraj' that is implemented suing our portal as shown in the fig. 5.

The working of pair – based Authentication scheme for session password in our portal is as follows:

- For the first combination i.e. 'su' –'s' is scanned vertically which we get in the first column and now for 'u' we will scanned the keyboard horizontally we will get it in the third row. For implementing our session password scheme we have taken the combination of both i.e. letter 'y'.
- Now, for the second combination i.e. 'ra' – 'r' is scanned vertically which we get in the second column and now for 'a' we will scanned the keyboard horizontally we will get it in the sixth row. For implementing our session password scheme we have taken the combination of both i.e. number '0'.
- Finally, for the last word as it is the odd numbered word, our scheme uses the last letter of that odd word as it is. Here that last word is 'j', which is taken as it is.
- So, here the combination taken by pair-based scheme for that session as it's password is – "y0j".

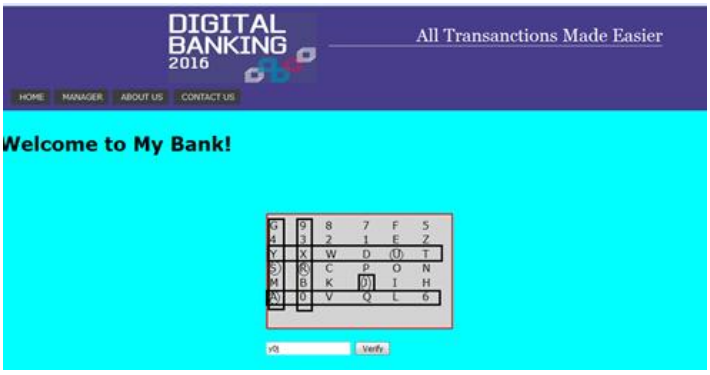

Fig. 5: Entering password using pair-based scheme

As, the user named 'suraj' is successfully logged in after entering his session password using pair-based scheme which is associated with his original password entered at the time of his registration, he will reach to his home page (shown in the fig. 6). In our designed online banking portal user has the facility of checking his balance, perform fund Transfer to any one of his beneficiary account holder and he is able to generate the mini statement of all oh his transaction performed and some other general facilities.

Fig. 6: Home page of online banking portal

Once the user has logged-out from that session., the password entered for the earlier time gets lost. Now, when the user is logging-in for the next time he has to make the working as like earilier. But for this time the keyboard generated to entered his password gets shafaled and hence, the combination of word 'suraj' is also gets changed. It will provide the security form the dictonary attack, shoulder surfing attack and some possible network attacks also. In this way, we are successfully perform the machanism of AAA – Authentication, Authorication and Access in our implemented software application for online banking where security is the formost requirement.

IV. SALIENT FEATURES AND PERFORMANCE

Our scheme enjoys the following features:

- The scheme prevents the scenario of online facilities users, Even if user'spassword is leaked or the user has revealed his password, the adversary cannot login to Authenticated System withoutthe correct password ones he has entered at the time of registration.

- It should be noted that, if the user has logout for once after successfullogin, the login session would immediately expire. And now if the user has to login again, the password that user has typed on the keyboard for the earlier time has changed for this time, so shoulder surfing attack is not possible.

- It is the most user friendly security and password verification scheme, for providing security to the user accounts like, bank account, personal social account, etc.

- This feature greatly reduces the network traffic and overhead onremote servers to store the password information instead of password is changing for all the time when user is perform login.

- Here the verification from the database server is required during the authentication process. But this may lead to avoiding the risk ofdictionary attack, shoulder surfing attack, since the user does not type theactual passwordfor user authentication.

V. CONCLUSION

Here, we have concluded that our proposed and implemented scheme is useful for avoiding different types of attack like shoulder surfing, brute force and dictionary attacks. We have proposed a simple pair-based scheme for entering password at the time of user login which is also valid for that session, in whichthe user can efficiently, easily complete the login process without attacks. The operation of the proposedscheme is very simple, easy to learn and easy to use for all the users once they familiarized with that scheme. Theuser can easily or efficiently perform login to the system without using any physical keyboard. Along with this our implemented application software for online banking also execute this pair-based scheme along with AAA-Authentication, Authorization and Access mechanism of security.

REFERENCES

[1] SanketPrabhu ,Vaibhav Shah ,"Authentication Using Session Based Password" Science Direct, International Conference on Advanced Computing Technologies and Applications 2015.The University of Texas at Dallas, Dallas
.

[2] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and WaqasHaider, 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication, World Applied Sciences Journal, 19(4): 439-444.

[5] A.A.Doke, D.B. Wagh ,S.H.Shekh , S.S.Gawali "Graphical and Pair Based Scheme for Authentication Using Session Password" International Journal of Advanced Foundation and Research in Science and Engineering 2015.

[3] S. Rajarajan, K. Maheswari, R. Hemapriya, S. Sriharilakshmi "Shoulder Surfing Resistant Virtual Keyboard for Internet Banking"World Applied Sciences Journal 31 (7): 1297-1304, 2014.

[4] Usman, Ahmad Kabir and Mahmood Hussain Shah 2013. "Critical Success Factors for Preventing e-Banking Fraud." Journal of Internet Banking and Commerce, 18: 2.

[6] ReshmaDilipKadam,SwapnilDilipKoshti,AmolRajendraGawde , Prashant ChandrakantKambale ,Prof.BogiriNagaraju, "Authentication scheme for session passwords using hybrid and Pair Based Technique", Multidisciplinary Journal of research in engineering and technology".

[7]S.Man.D. Hong and M. Mathews, "A Shoulder Surfing resistant graphical password scheme,"in proceedings of international conference on security and management. Las Vegas, NV, 2003.