Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Technophilia-2018.

Volume 5, Special Issue 04, Feb.-2018 (UGC Approved)

AN IMPROVED GRAPHICAL AUTHENTICATION SYSTEM TO RESIST THE SHOULDER SUFFERING ATTACK

[1]Gawali R.R, [2]Thorve K.B, [3]Hande P.V, [4]Londhe U.Y, [5]Mr.Khemnar D.S.

Computer, Jaihind Polytechnic, Kuran

Abstract — *Textual password are the most regular procedure used for authentication. The proposed of session password plan uses text and colors for generating assembly password. But textual password are vulnerable to eves leak dictionary attack socials engineering and shoulder suffering graphical password are introduced as alternative technique to textual password To make safe on those confidential application such as banking, business application and personal data, password is provided to upgrade privacy. The forget password module and banking service module is added which could be experimental and an powerful idea to authenticate the proposed system.*

Keywords- *Pair Based Authentication, session password .*

I. INTRODUCTION

There are many other graphical password suggestion but most of these schemes suffer form shoulder surfing which is becoming quite a big problem. Authentication is the main step to access any social website where user have to put username and password. Many schemes and ability are available to provide authentication. The use hybrid textual authentication scheme and pair based authentication scheme. The user for select the password as a color or alphanumerical grid. We have focused on text password and graphical password. At the time of registration user has to enter password. The minimum length of password is 8 characters. User login we create session password based on users original password entered at the registration time. It consists of the string of alphabets and numeric. The various authentication techniques textual password is popular. Today for authentication username and password is use the basically so the safety must be provided in order to verify hackers the authentication must be secure in order to screen users account. The steps which have to be followed so as enter the password. The user makes the pair of password first user verify for the row and then column.

II. GOALS AND OBJECTIVE

By using this application you can provide the security of any application , document also.Ex. Cotation of product. When the user is register at that time user gives the data like username , password, mobile number etc. If user forgot the password then he can receives password through message. User can handle the system easily and perfectly.

III. EXISTING SYSTEM

The most repeated method used for authentication is textual password. The breakability of this method like eves position, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. Studies have shown that users tend to collect short passwords or passwords that are easy to remember. These passwords can be easily guessed or cracked. The different techniques are graphical passwords.

IV. PROPOSED SYSTEM

Personal Digital Assistants are being used by the people to store their personal and particular information like passwords and PIN numbers. Authentication technique consist of three phases registration phase, login phase and verification phase. During registration user enter his password in first method or select the color in the second method the login phase user has to enter the password based on the interface displayed on the screen to the user the system validate the password enter by comparing with contain of the password generated during the registration process.

V. ARCHITECTURE DIAGRAM

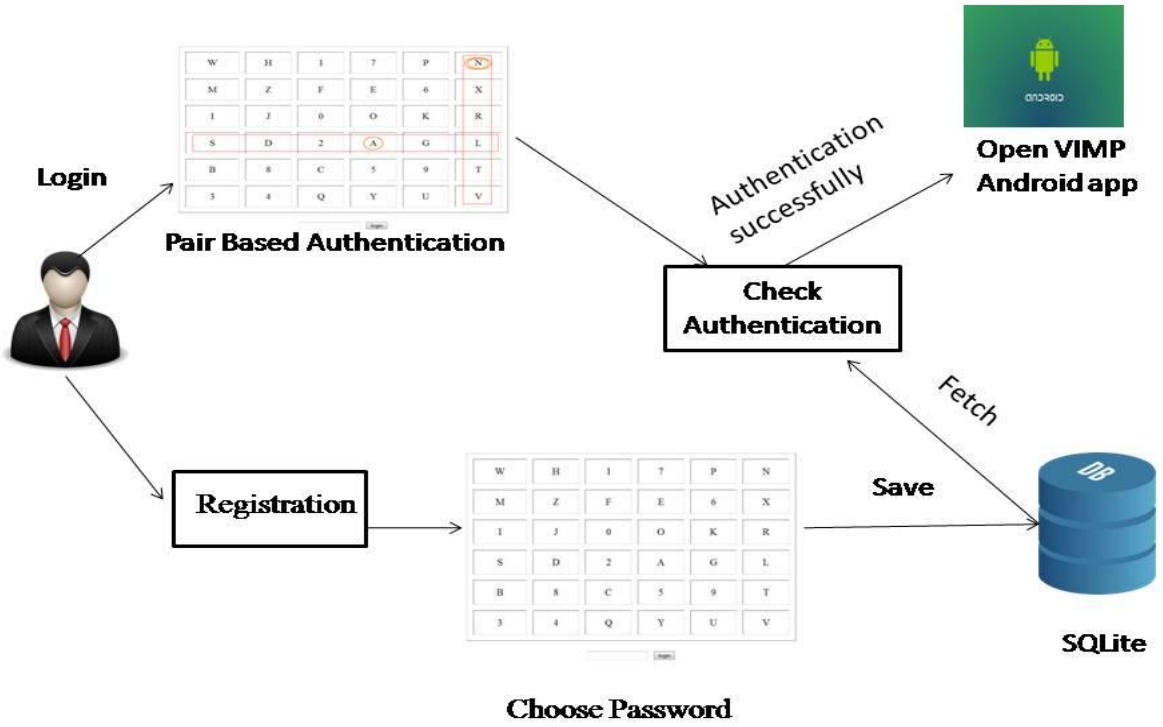

Figure 1 Architecture Of System

The secret password should contain even number of character. The user enters his user name an interface consisting of a grid displayed the grid is size 6*6 and it consist of alphabets and numbers the system verifies the password enter by comparing with content of password generated during registration.

VI. CONCLUSION

It is resistant to many attacks and provides high protection level the implemented authentication scheme is faster and more secured compare to the other procedure in the market the textual passwords are the simplest way to handle the login process. authentication techniques should be verified extensively for usability and effectiveness.

VII. REFERENCES

[1] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010

[2] R. Dhamija, and A. perrig, Déjà vu: Pair Based authentication using dynamic grid in 9th unisex security symposium

[3] Grid Based Authentication Password Using Hash Technique (IJNSA), Vol.3, No.3,May 2011.

[4] G. E. Blonder," Authentication scheme for session password using hybrid and pair based authentication.in Lucnt technologies, Inc.