

RECALL BASED TEXTUAL PASSWORDS

¹ Revathi Gompa, ² Praveen Dasari

¹ M.Tech, Final year student, ² Assistant Professor

¹ Department of Computer Science and Engineering (CSE)

¹ Gayatri Vidya Parishad College of Engineering, Visakhapatnam, India

Abstract : *The vast majority of user's authentication is accomplished using text passwords. Textual passwords are easy to remember and hard to guess. Sometimes users forget password, to recollect the forgotten password several authentication mechanisms are available to the users, even though some of them are unable to recall the forgotten passwords. We proposed a system to recollect the password by displaying the hint without revealing any information to the user. By displaying hints the numbers of failed login attempts were decreased and memory recall of textual passwords is increased.*

Keywords - Authentication, Password, recall textual passwords, password hint, password strength, Salt and peppering function.

I.INTRODUCTION

In majority of the authentication systems, textual password schemes have the major choice to authenticate end users. By considering the present scenario, inconvenience is incurred by the end users in remembering multiple passwords for multiple accounts. And also users choose passwords which are easy to remember. While selecting the password the end users should remember the strength of the password [2] for security convenience. And there are hundreds and millions of stolen names and passwords of various accounts. For example, a massive 272.3 million stolen user names and passwords were recently traded on the internet, including some from the biggest email providers (e.g., Google, Yahoo, and Microsoft)[8]. End user should aware of choosing the password. However the end users should take care while choosing the password and the strength of that password. End users are aware to choose "strong passwords" like meters.

The passwords which are trivial to guess or those likely to be cracked by using dictionary attacks are the weak passwords. The lack of existing password schemes providing users to narrow down the range of candidates passwords as users are only provided with All-or-nothing. It leads to the legitimate users with no choice but to guess their passwords with "trial and error" process to access their accounts.

By existing literature there are many alternative to password and some of them are adopted as commercial use but no one is became more popular and friendly then textual passwords. In many authentication systems the technique user recall passwords is widely used to help users by using password hints (e.g., windows) .when creating the account the user is requested to submit some text (e.g., either a word or a sentence) in most of hint schemes.

The main need about such a password hint is that the user's chosen password hint will reveals more information regarding to the password, or an attacker can guess the password by using hint. A good password hint not only helps to recalling a password but also reveals little or no information regarding the password.

This paper proposes recall the forgotten password by using hints which makes use of users contact list , it contains the familiar information about the user and it automatically generate easy-to-remember passwords. There is no additional set up is required for new user account. The main aim of this paper is to *minimize the number of failed login attempts and recall the passwords easily.*

II.RESEARCH METHODOLOGY

2.1 The research methodology followed for our work is mentioned as below:

- Reading already published work in the same field.
- Browse on the topics of the research work.
- Attend the related workshops and conferences.
- Understand the technical aspects of the system implemented.
- Implement the system on machine
- Analyse the results of the system.

III.PROPOSED SYSTEM

The proposed schema is developed with the password-hint mechanism that allows the minimum length required to trigger the password hint. For example, when the password encounters the fourth character, the hint starts to display. And in addition to this, for security, question will be raised after matching the security question and the hint will be displayed.

3.1 The proposed password hint scheme consist of following components

Registration:

It is a collection of data about the user which contains the name, user name, email –id , address , etc., these information is used to generate hint.

Pepper function:

To protect the passwords pepper function can be appended to the passwords. Pepper is a random number added to the password, such that the stored value is hash (pepper||password). Pepper is not stored at all therefore all possible values of pepper need to be tested when trying to log in.

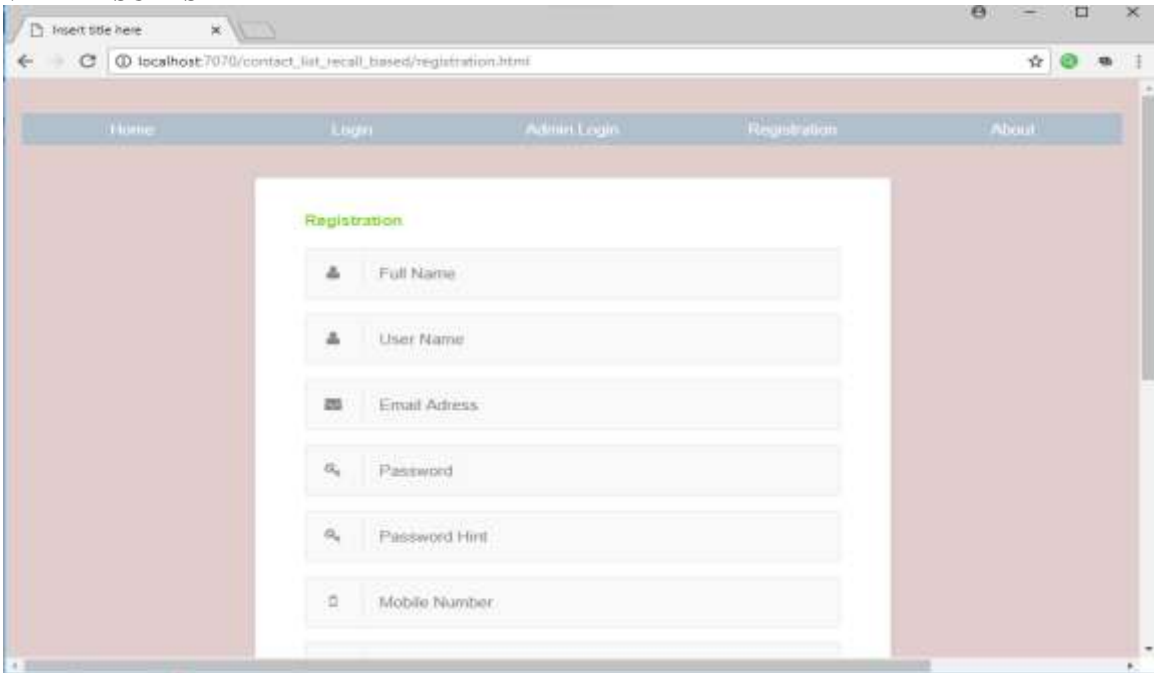
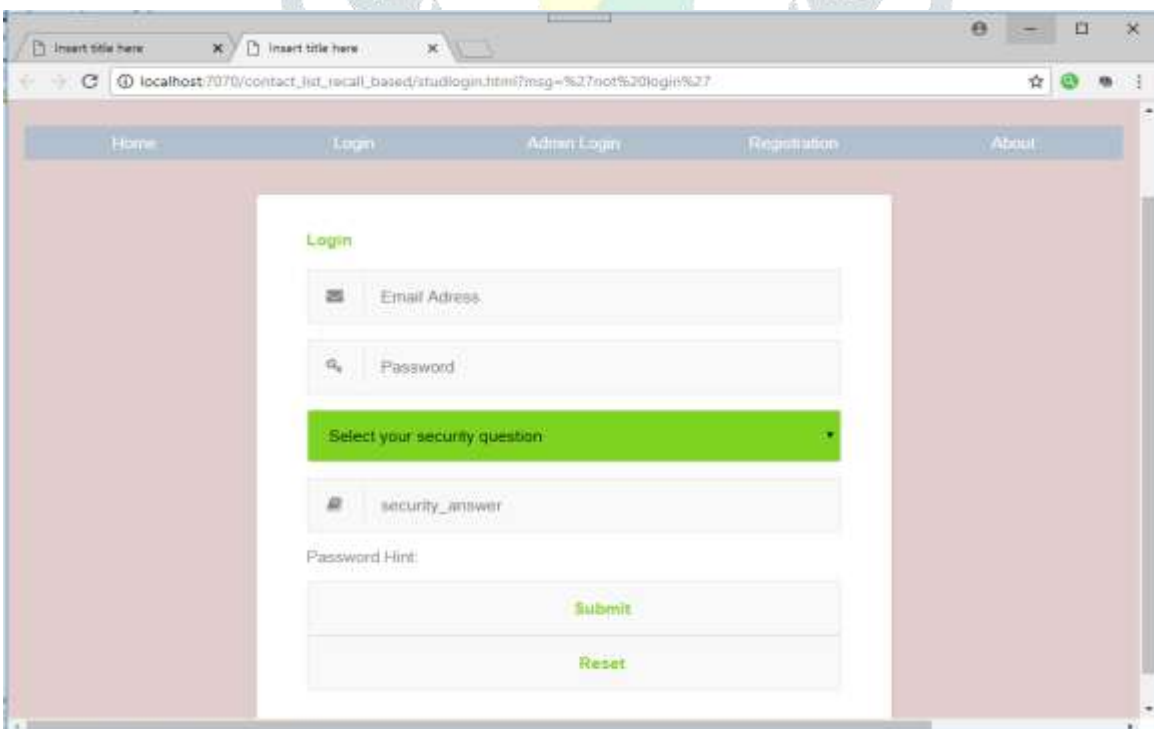
Cryptographic one way hash function:

Cryptographic hash function is a hash function which takes an input(message) and returns a fixed size alphanumeric string . The string is called 'Hash value', message digest'. It is externally easy to calculate a hash for any given data. Unlikely that two different messages will have the same hash . The third party who knowing the hash value is unable to know the original message. so , it is called as a one way hash function. The secure hash algorithm (SHA) it also family of cryptographic hash function

3.2 Maintaining information:

Edit registration: given the dynamic nature of registration if needed to alter the data , then there is a chance to change the information like phone number, address. Shown in **figure:4.5**.

Edit password: when user login is correct, if it necessary to change the password then there is an option for old password, new password, and confirm password.

IV.EXPRIMENTAL RESULTS**Figure 4.1: Registration form****Figure 4.2: Login form**

In above figure 4.1 the user gives the information for the given fields and stored in a particular storage area. After given the information click on 'submit' button. Then go to login form shown in figure 4.2 enter email-id and password and also given a security question for avoiding unauthorised users.

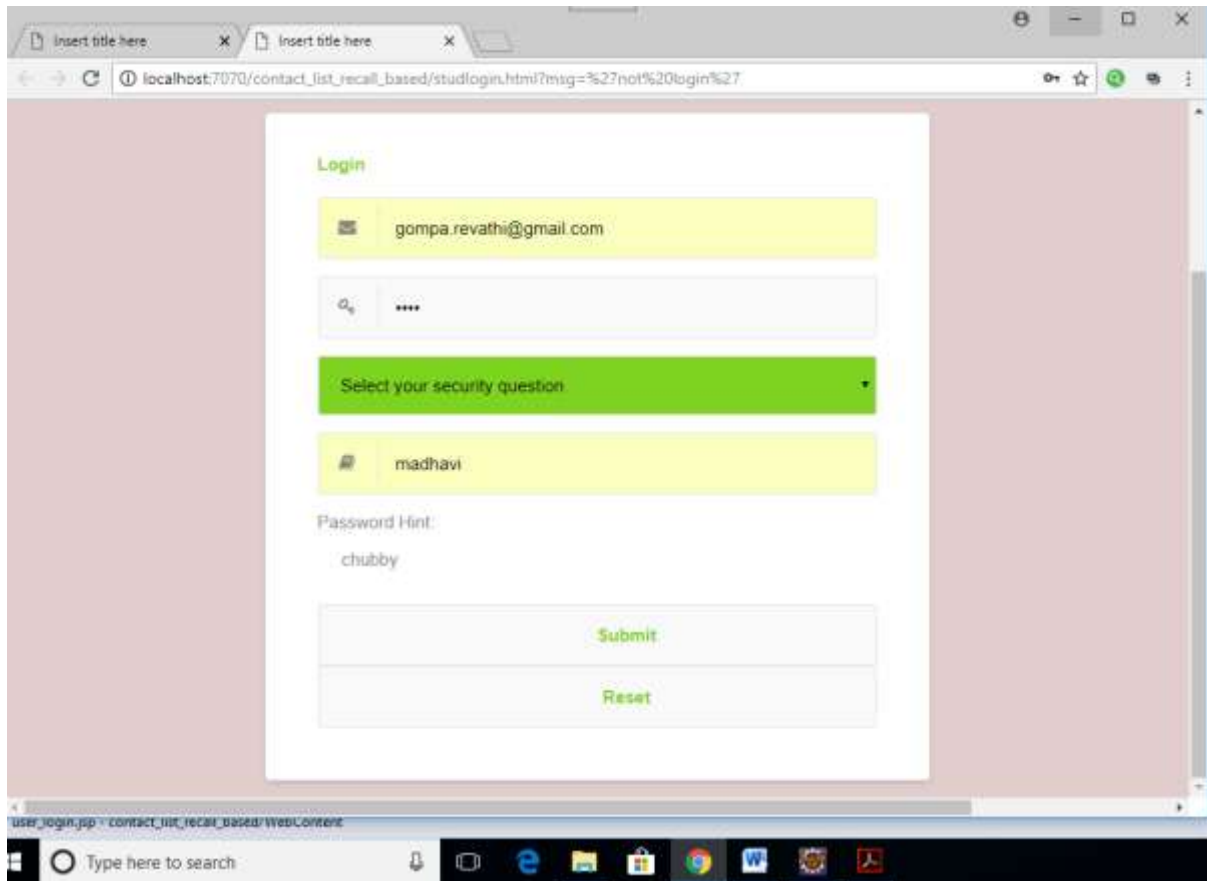


Figure 4.3: displaying hint

When enter the password after entering the fourth character the hint will be displayed at the location 'password Hint' in figure 4.3. If the entering password is wrong, in the location password Hint it displays a message 'wrong password'.

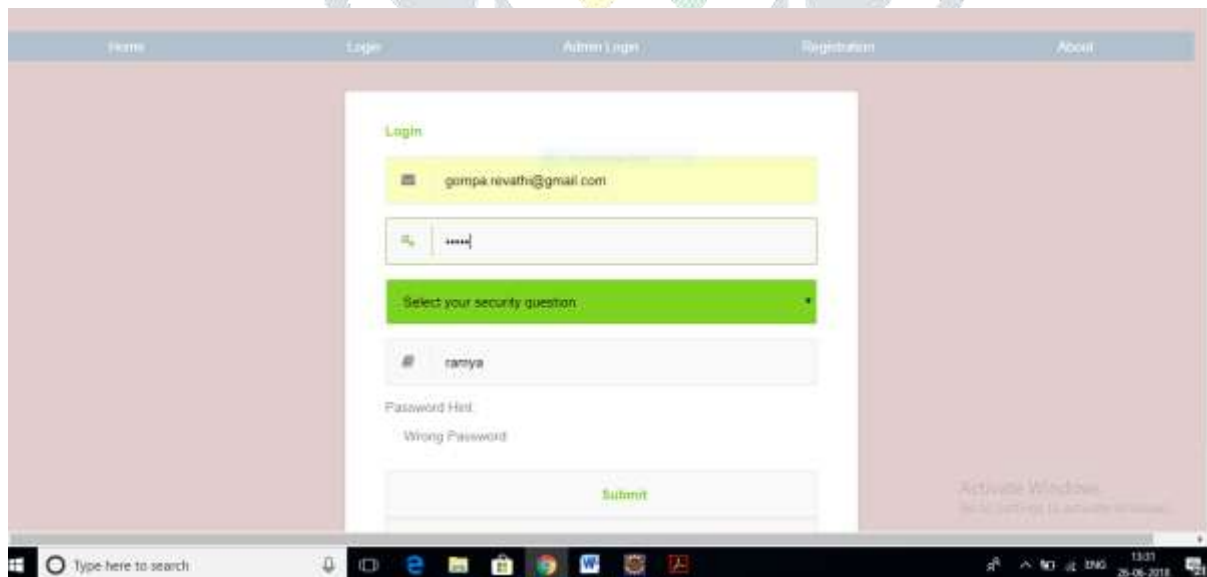


Figure 4.4 informing wrong password before submission

Figure: 4.5 Edit password and edit profile

V.CONCLUSION

The implementation of this paper work is based on textual passwords, and many of people they get confused with the usage of different accounts of same user and while at the time of account login. Due to that number of incorrect login attempts the server side burden will be increased and the server utilization will be decreased. So before sending a request to server for password checking and login, password hint displays 'wrong password' then there is no need to send a request to server so that the server time will be allocated to some other request. So that the number of failed login attempts were decreased.

VII.REFERENCES

- [1] M. L. Mazurek *et al.*, "Measuring password guess ability for an entire university," in *Proc. ACM SIGSAC Conf. Compute. Commun. Secur.*, 2013, pp. 173–186.
- [2] R. Shay *et al.*, "Encountering stronger password requirements: User attitudes and behaviors," in *Proc. 6th Symp. Usable Privacy Secure.* 2010, p. 2.
- [3] J. Bonneau, "The science of guessing: Analysing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 538–552.
- [4] M. E. Moy, "Computer security apparatus with password hints," U.S. Patent 5 425 102, Jun. 13, 1995.
- [5] J. Fontana, *Another Breach, Another Dollar: Is it Time to Kill the Password?* Accessed on May 10, 2016. [Online]. Available: <http://zd.net/1QT593G>
- [6] Cloud Security Alliance. *IDENTITY SOLUTIONS: Security Beyond the Perimeter*, accessed on May 5, 2016. [Online]. Available: <http://goo.gl/NkbMDX>
- [7] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proc. 17th ACM Conf. Compute. Commune. secure.* 2010, pp. 162–175.
- [8] J. Fontana, *Another Breach, Another Dollar: Is it Time to Kill the Password?* accessed on May 10, 2016. [Online]. Available: <http://zd.net/1QT593G>