ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

Two Level Password Authentication System

Dr. Swapna Borde, Gauri Satish Tambe, Suchita Ramdas Tambade

Abstract*—In this paper, we present a 2-level password authentication scheme, which is a multi-factor authentication system. To be authenticated, this project plans to present a 2-level password system by combining the features of the existing authentication schemes. The two different levels used in the 2-level password authentication scheme are Speech-to-text and the one time password (OTP). Two-level authentication provides a significant increase in security. With use of multilevel authentication system, the hacker or attacker won't be able to get into the main page and access the user's information. The system built is user-friendly and is able to learn quickly and easily understandable. It eliminates the problem related with single level password authentication system.

***Index Terms*— Authentication, multifactor, one time password, Speech to text converter.**

I. INTRODUCTION

Today's widespread use of single-factor authentication is in the midst of change. Both corporate and personal organization are at risk against people trying impersonating users and stealing money and information. Single-factor authentication methods such as the basic username/password combination are no longer safe. In the current state there are many authentication schemes and most of these suffer from weaknesses. Increasing security has always been an issue since Internet and Web Development came into existence, text based passwords is not enough to counter such problems, which is also an anachronistic approach now. Therefore, this demands the need for something more secure along with being more user-friendly.

In a computer security system human factors are considered as the weakest link. However, there are three major areas where human-computer interaction is important: authentication, developing secure systems and security operations. Here the main focus is given to the authentication problem.

Although ID and password are two items, because they belong to the same authentication factor (knowledge), they are single factor authentication (SFA). It is really because of their low cost, ease of implementation and familiarity that passwords that have remained the most common form of SFA. As far as SFA solutions go, ID and password are not the most secure. Multiple challenge-response questions can provide more security, depending on how they are implemented, and standalone biometric verification methods of many kinds can also provide more secure single-factor authentication.

One problem with password-based authentication is that it requires knowledge and diligence to create and remember strong passwords. Passwords also require protection from many inside threats like carelessly discarded password sticky notes and old hard drives and social engineering exploits. Passwords are also prey to external threats such as hackers using brute force, dictionary or rainbow table attacks. Given enough time and resources, an attacker can usually breach password-based security systems. Two-factor authentication is designed to provide additional security.

The objective of 2 Level Password Authentication System is to provide more security so that the attackers won't misused it. The project provides a user-friendly interface to register and login user details and hence providing high security in this attacker's world [5] [6] [7].

II. 2-LEVEL PASSWORD ATHENTICATION SYSTEM

A. Speech to Text Converter

A speech-to-text (or voice recognition) application translates the spoken words into text possible. This converter makes the use of the objects described below. This functionality can be used in many other fields of life, as well as in the healthcare, in-car systems, military, telephony, education or computer gaming. It can be especially useful for people with disabilities [1].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

Objects used in Speech to Text Converter

- Speech Synthesizer Class: Provides access to the functionalities of an installed of speech synthesis engine.
- Prompt Builder Class: It create empty prompts and provide methods for adding contents, selecting voices, controlling voice attributes and also it is used to control the pronounication of spoken words.
- Speech Recognition Engine Class: Provides the means to access and manage and In process speech recognition engine.
- Choices class: A set of alternatives in the constraints of an speech recognition grammar [3].

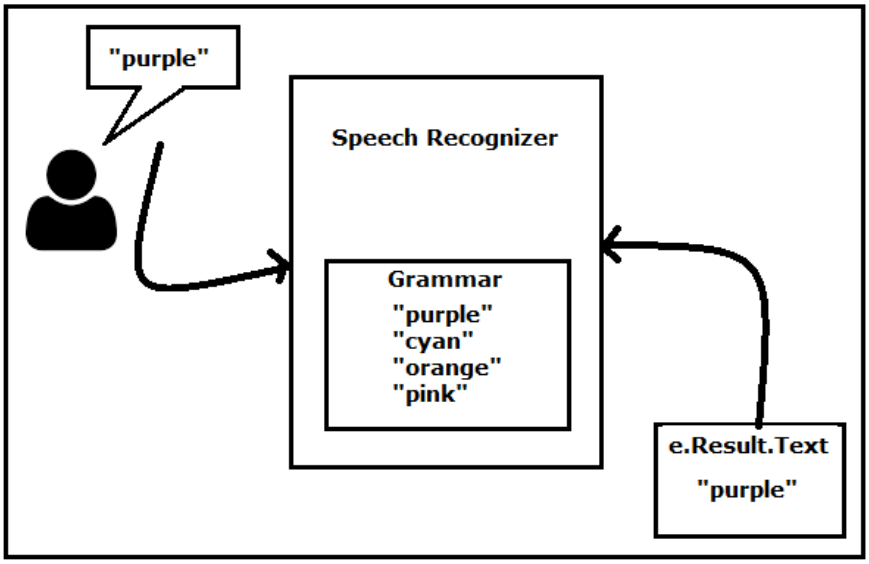

Fig.1 Speech Recognition

Fig.(1) shows the Speech Recognition in which the word spoken by the user is matched with the grammar which is loaded in speech recognition engine. And spoken word is converted into text.

B. One Time Password (OTP)

In the Second level, we make use of one time password (OTP) that is a password which is valid for a single session. We securely generate OTP using Smartphone. The generated OTP can be send to a mobile phone in the form of SMS as SMS messaging has a high potential to reach all the customers with a low total cost of ownership or Smartphone can be used as token or platform for creating OTP. Thus we can call it SMS OTP or OTP generated through Smartphone the OTP generated will be valid only for a short period of time [2] [4].

Objects used in One Time Password:-

- HttpWebRequest Class: Provides an HTTP-specific implementation of the WebRequest Class.
- HttpWebResponse Class: Provides an HTTP-specific implementation of the WebResponse Class.

III. WORKING OF TWO LEVEL PASSWORD AUTHENTICATION SYSTEM

Fig. (2) Shows the working of 2-Level password authentication system as follows:

- The user should register him/her by providing the personal details followed by password using speech to text converter.
- After this, the details of registered user is saved in the database.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

- For the login procedure, the user has to enter his username and password by using the same speech to text converter method.
- Once the user details are confirmed, the OTP will be generated into his/her phone.
- By using that number, the login procedure is completed and user is being directed to the main page.
- This way, the 2 level password authentication system works.

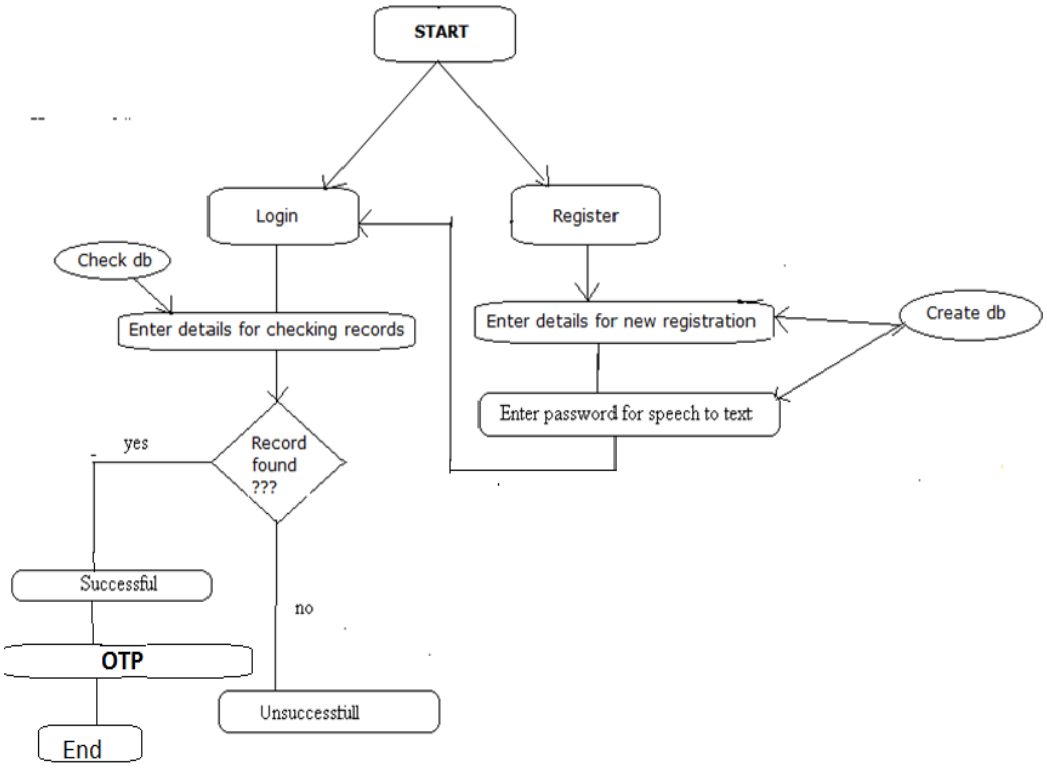

Fig. (2) Data flow diagram

IV. RESULT

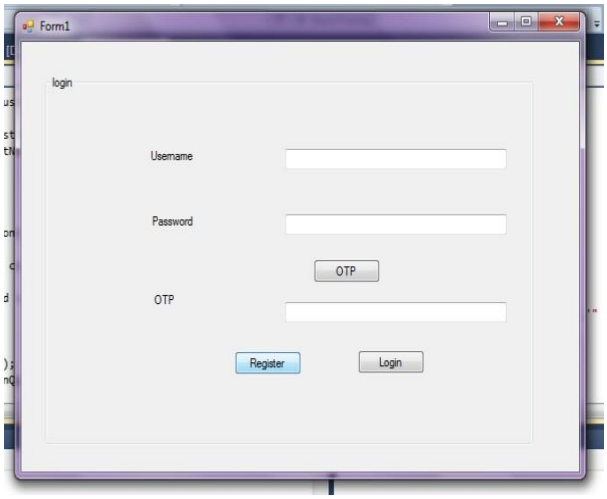

Fig. (a) Login page

Fig.(a) shows the login page which is the opening page of Two-Level password authentication system. Onto this page, user can login to the system by entering same details which we would provide at the time of registration like username (E-mail id) and password (Speech-to-Text password). In case of new user, this opening page i.e., login

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

page provide a "Register" button, by clicking on it new user can register him/her by providing personal details.

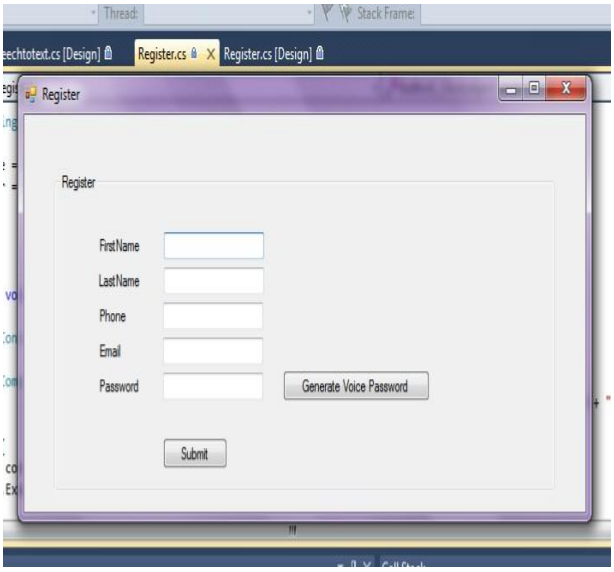

Fig.(b) Registration page

On registration page, new user can register himself/herself by providing details as shown in fig.(b). User should enter following fields:

-First name,
-Last name,
-Contact no. should be correct and active because at the time of login, OTP will get send on this number,
-Email-id, at the time of login user should enter this same Email-id as a username,
-Password, in front of password field we have one button "Generate Voice Password", by clicking on this button we generate a speech-to-text password which is available in grammar.

After filling all the details, click on "submit" button. User details will get save into the database.

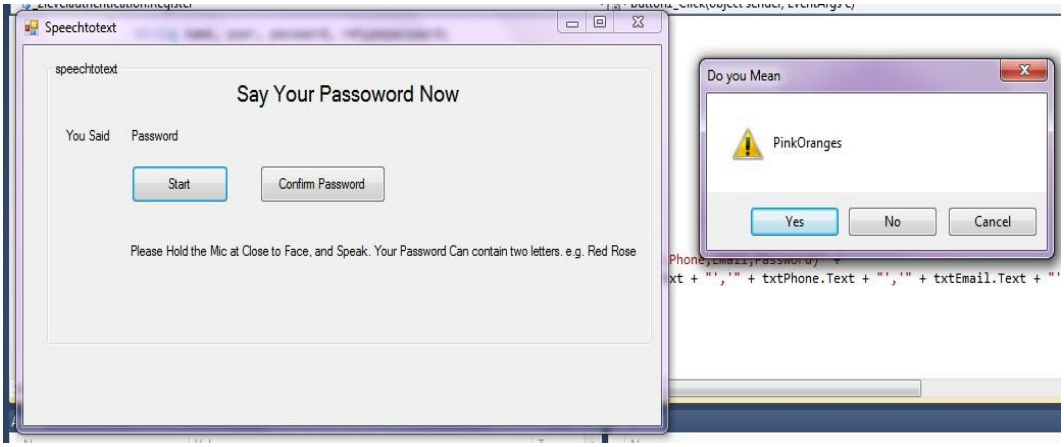

Fig. (c) Speech to text converter

Fig.(c) shows the speech to text converter here first click on "Start" and then user should speak the password which is available in grammar. In this authentication system, password is a combination of two words one is color and another is anything. For eg. RedSun, YellowRose, PinkOranges, etc. Speech to text converter converts a spoken word(password) into text. Second window shows the word spoken by user if it is same then click on "Yes " button. This same note is written on speech to text converter window for user's compatibility.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

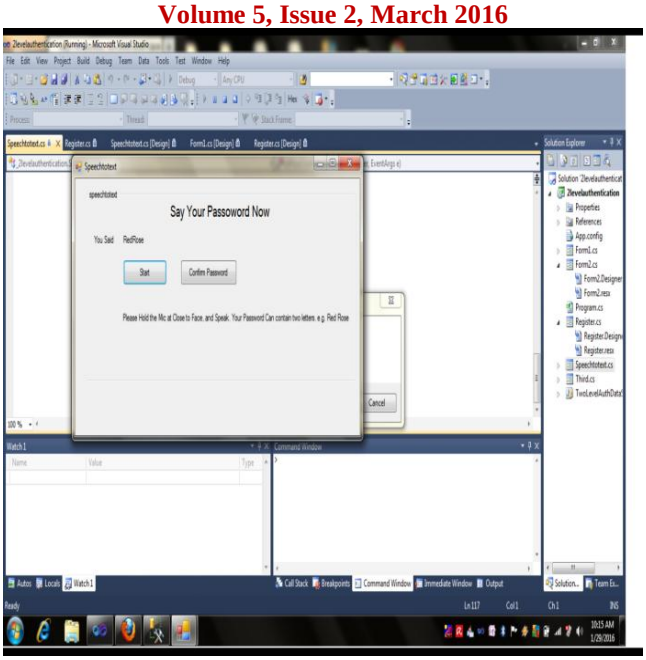

Fig. (d) Choice one password

Fig.(d) shows the window which displays a password spoken by user. If it is same as that of said by user, click "Confirm Password" and then this password will automatically filled in registration page. If it is not correct password, then click on "Start" to reset.

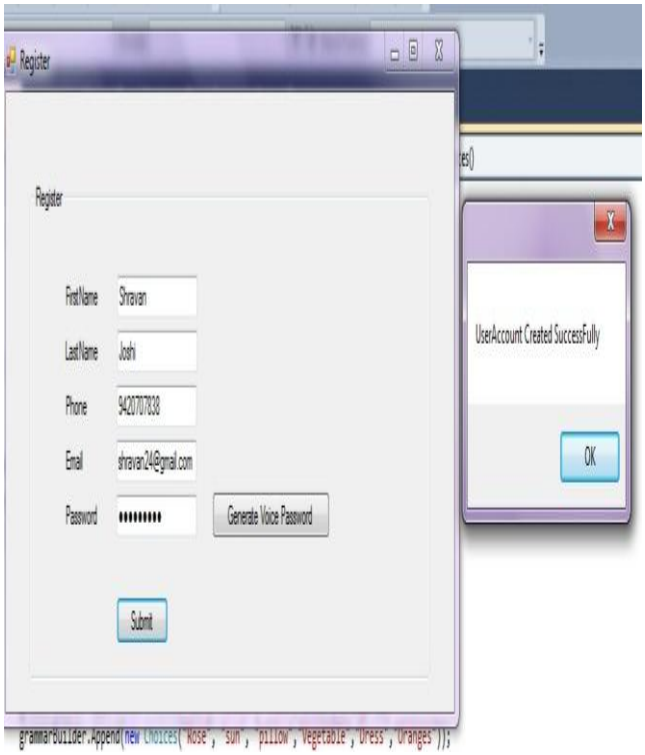

Fig.(e) Registration done

By generating voice password and filling all the details click on "Submit" button, all the details with voice password saved successfully into the database and confirmation for that new window will open which displays the message "User Account Created Successfully".

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

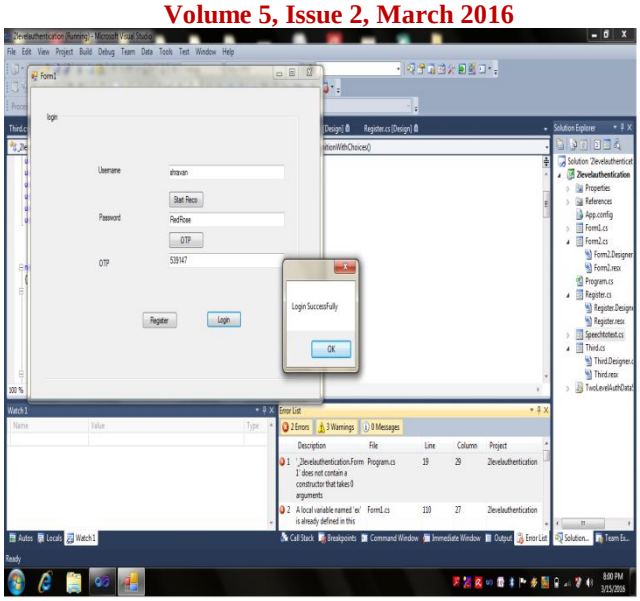

Fig (f) Login after registration

As shown in fig.(f), after registration user can login to the system by entering username which is the Email-id of user and again generate the voice password which is the first level of password authentication system. Second level is OTP, on clicking "OTP" button OTP(One Time Password) will get send on user's same mobile number as local message containing six-digit numeric number. User have to enter the same otp in OTP fileld before it gets expired. Then click on "Login" button ,authentication system verifies all the details according to username, if it is correct then small window displays the message that "Login Successfully". If any one of the detail is not correct then it will display the message "please enter username i.e. email-id (abc@gmail.com), invalid password or invalid OTP".

V. CONCLUSION

The 2-level password is a multifactor authentication scheme that combines the features of various authentication schemes. The first level is the speech to text password, where the user speak password same as in the registration phase.

The most secure level is the second level, which is the generation of one time passwords. The hidden OTP generated in the web part is compared with the OTP generated in the application side and if they are valid i.e., if both the OTPs generated are same , then the generated OTP will be sent to the Smartphone of the user as an SMS, with which the user logs on to the system.

One of the biggest advantage of this authentication system is it is user friendly. It is very easy to understand and learn quickly.

Even though the first level might seemed to hack quickly but the second level won't let to enter into the actual users page due to OTP section.

ACKNOWLEDGMENT

We are grateful to Dr. Swapna Borde from Vidyavardhini's college of engineering and technology, (Mumbai University) for guiding and providing knowledge for the same.

REFERENCES

[1] http://www.wikipedia.org/wiki/Speech_to_text

[2] https://en.wikipedia.org/wiki/One-time_password

[3] http://www.codeproject.com/Articles/380027/Csharp-Speech-to-Text

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

[4] https://www.howtoforge.com/how-to-secure-apache2-with-linotp

[5] http://www.ijrdet.com/files/Volume2Issue4/IJRDET_0414_23.pdf

[6] http://nevonprojects.com/three-level-password-authentication-system/

[7] http://www.eajournals.org/wp-content/uploads/Three-----Level-Password-Authentication.pdf

AUTHOR BIOGRAPHY

Dr. Swapna Borde
Ph.D, Head of Department of Computer Engineering, Vidyavardhini's College of Engineering and Technology, Vasai, India

Gauri Satish Tambe
Bachelor of Computer Engineering, Vidyavardhini's College of Engineering and Technology, Vasai, India

Suchita Ramdas Tambade
Bachelor of Computer Engineering, Vidyavardhini's College of Engineering and Technology, Vasai, India