National College of Ireland

Speech based OTP system to prevent shoulder surfing.

MSc Research Project
Cyber Security

Anmol Geer Bava
Student ID: 18195792

School of Computing
National College of Ireland

Supervisor: Prof. Michael Pantridge

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Anmol Geer Bava
Student ID:	18195792
Programme:	Cyber Security
Year:	2020
Module:	MSc Research Project
Supervisor:	Prof. Michael Pantridge
Submission Due Date:	17/08/2020
Project Title:	Speech based OTP system to prevent shoulder surfing.
Word Count:	4639
Page Count:	17

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	August 17, 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Speech based OTP system to prevent shoulder surfing.

Anmol Geer Bava
18195792

Abstract

Nowadays authentication schemes are being introduced with additional schemes to the traditional password based authentication systems. Additional schemes include passphrases, token based one- time passwords, token based cards, graphical based systems, and other biometric based schemes. Even with the introduction of new layers of security in authentication schemes, human beings still are the weakest link to even the most secure authentication systems. Although many social engineering techniques can be used to crack an authentication scheme, the most effective and easiest to implement is the shoulder surfing attack. The proposed scheme reduces the probability of shoulder surfing, bruteforce and keylogger based attacks significantly. The paper proposes a novel approach of speech recognition to the traditional otp based system which increases the usability as well as the security of the otp scheme. Although there have been many speech recognition modules produced, the proposed system comprises of the Google Speech recognition module which perfectly fits the requirements of the proposed authentication scheme.
Keywords: Authentication, Speech Recognition, Shoulder surfing, Key logging, OTP

1 Introduction

Authentication is the procedure of determining an individual's identity or verifying an individual's identity, who is pretending to be the authorized person. Authentication systems are used for controlling access or authorizing only the valid users should have access to the services present after the system. Traditionally users have been authorized to access services by saving their user credentials in a database and verifying the user's credentials being inserted with the credentials in the database.

Authentication schemes have been used for securing critical applications such as social media applications, banking applications and other online services that use online accounts to keep tabs on the users accessing the application. Over the past years, primary authentication systems such as password based authentication systems such as password or passphrase have been equipped with additional layer of security with integration of new forms of security including the one-time passwords, token based authentication scheme, biometric schemes, graphical schemes and captcha based schemes. The fundamental principles on which every authentication scheme is based on things the user might own or possess and something that a user might know or remember. For example, in the case of password, the user should remember the keyword that was assigned as a password to the respective authentication scheme. Currently, authentication schemes have been proposed which have a two or three fold approach towards authenticating the user. The

multi fold or also known as multi-factor authentication schemes combine the two principles of possession and memorization. For example, passwords have been integrated to one time password and CAPTCHA based schemes for the user to remember the password and possess the otp with CAPTCHA being an additional form of security to prevent bots executing attacks such as denial of service. Over the years, many attacks have been devised to break authentication schemes such as bruteforce attack, SQL injection, cross site scripting, rainbow table attack, Man in the middle attack, session hijacking, command injection and directory traversal attack. In addition to the attacks mentioned, there have been other attacks such as social engineering attacks which take advantage of an individual's psychology in order to extract vital information such as passwords or keywords that might lead an attacker to the passwords. One such attack is the shoulder surfing attack in which the attacker has constant visual contact with the target's device and waits for the target to enter the keyword. As the target enters the password the attacker steals the password and logs into the target's account maliciously.

The paper proposes an authentication scheme which combines the token based one time password scheme and speech recognition to prevent attacks such as shoulder surfing, bruteforce attack and keylogger attack. Although many speech recognition products have been created by various companies, Google speech recognition module has been used to convert speech to text. The one time password generation works on the concept of pseudo random number generator which generates an otp after every login attempt in a random manner. The pseudo random number generator module can be used to define ranges of 0000 to 5555, which would give the exact digit count of the otp as required. The proposed solution prevents shoulder surfing as the authentication scheme does not allow the user to enter the otp by inserting the otp manually on screen, instead the user needs to use speech as a medium to insert the otp into the system thus preventing any shoulder surfing. In addition, the reaction time taken by the user to enter the otp is much less than that of an attacker trying to replicate the same procedure as that of the user while logging in.

1.1 Research Question

Can shoulder surfing be prevented with a speech based OTP system?

The following research paper has been structured in the following manner. Section 1 consists of an Introduction to the domain and topic with the motivation behind the selection of the topic. The introduction also contains brief insights about the working of the proposed model. Section 2 consists of literature review where research papers studied to gain an insight towards the topic have been critically analyzed. Section 2 contains all papers that were referred during the research. Section 3 contains the research methodology which contains the steps followed in doing research and every decision taken towards the completion of research. This section also contains the tools and programming language used for developing the artifact. Section 4 contains a component by component graphical representation or the architecture of the proposed model. UML diagrams, Sequence diagrams and use case diagram have been shown in the section. Section 5 contains the implementation stage where the final artifact and functionalities of the component is briefly described in this stage. Stage 6 is the Evaluation phase, where the certain scenarios and evaluation criteria have been used to analyze the efficiency of the proposed model. Section 7 contains the conclusion of the paper by highlighting the important points in the paper and also the scope of improvements that can be implemented in the future to

further improve the efficiency of the proposed model. The last section contains the list of references that have been used for the paper.

2 Related Work

Various authentication schemes have been proposed over the years that were used to authenticate the user. Types of user authentication schemes are based on passwords, passphrases, voice, biometrics or token based. In this section, each type of an authentication scheme is discussed, each having its own characteristics, advantages and disadvantages. The foundation of any authentication remains the same, something the user might have or something the user might own or something a user might know. Firstly we discuss about the various passwords based authentication schemes present. The common disadvantage of having one factor password authentication is the susceptibility to attacks such as shoulder surfing, man in the middle attack, SQL injection, Cross site scripting and brute force attacks. The paper [1] "password authentication describes the use of password scheme and its vulnerabilities". The paper discusses three attacks on the password based scheme. The first attack discussed is when the password is read by the attacker from a file, stored in plaintext. The second attack discussed in [1] is the man in the middle attack where the attacker steals the password by the listening on the communication line. The last attack discussed in [1] is the guessable password attack where the attacker can guess a password since it is very easy to predict. The paper [1] proposes a solution for the eavesdropping or man in the middle attack by using public key encryption to encrypt the password, thus making it secure while transferring the password through an unsecure communication line[1]. However, [2] paper discusses about the attacks that makes password based authentication scheme vulnerable to attacks. The system proposed in [2] indicates the password scheme proposed by Xu-Zhu in [3] is susceptible to attacks such as rainbow table, brute force attack, internal and imitation of the user attack[3].

In addition to the problems faced by the password based authentication schemes proposed by [1][2][3], another factor that hampers the use of passwords is memorability. Passwords are supposed to be memorable to the user, as well as distinct for every account. As stated by Anne Adams and Martina Sasse in [4], which discusses the problems faced by the users to remember multiple passwords for multiple applications[4]. Bik-Lam,TaibJoshuaCookbE.Eugene Schultzc et.al, state the effects on security by having multiple parameters that have to be satisfied by the user while using distinct passwords for every account[4]. The results stated are intriguing as adding more parameters hampers with the ability of the user to remember the password and through experiments conducted it was found that lesser passwords allowed better usage and better ability to remember the passwords[5].

2.1 Passphrase Authentication

In order to tackle the problems mentioned in the above subsection, passphrases were introduced as a replacement for passwords. Through research it has been stated that users have been more efficient in changing their keywords in passphrases from short term memory into long term memory[6][7]. As indicated by [6], users find it easier to memorize keywords from passphrases than using random keywords as passwords[6]. Passphrases are supposed be normal sentences that can be used as passwords having advantages such as high memorization when compared to passwords. However, passphrase authentication

scheme suffer due to the sheer size of the input that the user has to remember. The use of passphrase has been discussed in [8], the paper indicates that the entropy level of a three to four word passphrase is the same as choosing four keywords for a password[8]. The paper also indicates about the impact of stringent password policies set for the passphrases. Experiments done in [8] indicate that the memorization of the user takes a toll when strict password policies are implemented for passphrase authentication[8]. Passphrase authentication scheme when implemented with strict policies implemented resulted in more error logins, spelling mistakes and memory confusion impacting the performance of the authentication schemes[8]. To eradicate some of the problems passphrase authentication schemes can be implemented with hint giving mechanisms such as [9]. The paper uses geographic locations as hints for the user's convenience to remind him/her about the passphrase[9].

2.2 Graphical Authentication

Another alternative authentication scheme which can be used instead of passwords and passphrase are the use of images. The basic advantage of a graphical authentication scheme is that the user does not need to type anything which saves a lot of time while logging in, giving better usability to the user. In addition, images or graphics when used in an authentication system have been easily recallable by the user as compared to the password or passphrase authentication schemes[10]. Graphical authentication systems proposed in [11], indicates that the use of images can be used to prevent attacks such as brute force attack, shoulder surfing attack and keylogging attacks. Graphical authentication schemes can be categorized into three kinds. Recall based, cued points based and recognition based graphical authentication[10]. The advantage of using a graphical scheme is that images are easily recallable and replaceable, this means that images can be changed after a certain number of login, thus resulting in increase of security as the images can be changed more often so that attacks such as shoulder surfing would have less impact. The main limitation of the graphical scheme is the use of images itself. Unlike its text based counter parts graphical authentication systems deal with images which increases the computational power needed for processing the images. In addition, to the large use of power, the transfer of images has to done in a secure manner which has to be done with encryption algorithm, thus increasing the need for more computational power. Thus graphical scheme would require high speed internet due to the size of the images and images need to be encrypted before transmission, also would require decryption at the backend of the application which would result in more resources being needed for a single login attempt.

2.3 Token based Authentication

Token authentication has been used as an additional form of security to the text based authentication schemes. Token based authentication schemes are dynamic in nature. For example one time password is used with passwords as text based schemes are more static. In an attack scenario if the attacker guesses the password, he/she still has to bypass the one time password authentication which keeps on changing with every login making it difficult to bypass. As indicated by [11], one time password was introduced to increase entropy or randomness of the authentication system[11]. Entropy refers to the degree of randomness that is present in the authentication, higher the entropy more secure the

authentication scheme. As shown in [11], randomness has a direct affect in the attacker's ability to predict the authentication scheme's input and output values thus making it difficult to bypass the system[11].

2.4 One Time Password

Over the years various improvements have been proposed to the one time password scheme making it more dynamic in nature. One time passwords were first introduced by Lamport in [12]. Lamport in [12] suggested a dynamic password which was hash based. Building on Lamport's paper[12], Groza in [13] proposed a fresh approach of using integers instead of hashes(proposed by Lamport). The integers would be an outcome of a function which would repeat in a cyclic manner[13]. This proposed system by Groza in [13] would result in a more dynamic authentication scheme as random integers being produced with the help of the function would result in a more sets of passwords which would amount to increased difficulty to bypass the system. However, the only disadvantage of the system proposed in [13] is the use of additional resources and time consumption in authenticating the user as the increase in the set of passwords and randomness of the authentication system. Another proposed solution to Lamport's deficiencies in [12] was introduced by Eldefrway et al in[14]. The proposed solution consisted of two layers hash producing functions, one function was responsible for seed values and the other function was responsible for producing OTP's in a cyclic manner. The proposed solution in [14] checks the seed value(seed values are values that are input into the function), these values need to be checked to make sure the function does not produce redundant values, thus increasing the randomness or entropy of the proposed solution[14]. However, the proposed solution needs a protocol initiation from the user which makes it inconvenient. To improve on the proposed solution in [14], Gong et al. in [15] proposed an dynamic authentication scheme which makes use of mutual user server challenge response systems. The proposed solution uses sub-passwords which are created with the help of algebraic computations integrated with hashes[15]. Another OTP scheme was proposed by Yassin et.al, which introduced a cloud based OTP scheme which does not require any additional device for otp authentication[16]. The scheme makes use of RSA encryption with asymmetric encryption and both providers OTP as well as service provider would be in a single component in the architecture[16]. However, to overcome single device dependency issues, Cheng [17] proposed an OTP scheme which made use of both the worlds, mobile as well as cloud. In the proposed solution proxy servers are used for storing public keys and OTP are created through the otp generation server[17]. In addition additional hardware such as cards such as token have been used to provide an additional form of security[17].

Another voice based system was proposed by B. Cha, N. Kim and J. Kim in[18], which combined the two techniques of one time password and voice recognition[18]. The paper provides a solution to the shoulder surfing problem by generating the otp keys with the help of user's voice samples[18]. However, it was seen that a lot of focus had to be given to making the graph of voice to be smooth, even though the voice graph can be normalized with the help of reducing the dispersion, the process of normalization of the voice and combining the chaos signal and voice signal in[18] would be a huge challenge. In addition, the normalization would vary depending on the noise levels which would indeed result in consumption of huge amount of time and resources.

Thus, after analyzing the existing authentication schemes mentioned in the current section, it is quite evident that there are shortcomings in authentications such as the

password and passphrase schemes require memorization, as well as these schemes are susceptible to shoulder surfing attack. Even though, Graphical based schemes increase usability and are more secure than the two counterparts, they are still susceptible to shoulder surfing attack. In addition to the susceptibility, graphical based schemes consume a lot of resources that hamper the time taken during login as shown in [19]. Thus there is a need for an authentication scheme that would act as an extra layer of security as well as combines two techniques such as token based(OTP) scheme and Speech Recognition to prevent shoulder surfing attack.

3 Methodology

It was an essential requirement for this project to have research in a particular field of cyber security. There are various areas in which research can be done in the field of cyber security. This paper extends and builds on the foundation of the research done in the domain of authentication. The proposed solution has been devised to overcome attacks such as shoulder surfing and keylogging attack. The proposed solution is voice recognition based one-time password authentication scheme that works in two components. One component converts the user's voice into text and the second component checks the authenticity of the user by extracting user's voice features. However in order to devise a solution such as an authentication scheme two major factors have to be taken into consideration. First factor to be accounted for would be security and the second factor would be the ease of use. Balance between both factors should be taken into account when proposing a solution. The two factors mentioned above have taken into account as the basic evaluation parameters for the research. In order to measure security false positives have been taken into account where person A registers and person B tries to login into the account. Person B in this case will pretend to be person A and access the account of Person A by reading out the OTP sent to person A's email address. The usability factor will be measured with the help of average login time taken, login errors and potential attacks that can be used to bypass the authentication scheme have been discussed in the evaluation section of the paper.

3.1 One Time Password

The reason for the selection of OTP was fairly straight forward as they provide fast usability and enough dynamic nature or entropy to provide the security aspect as discussed in [13]. In this paper, the use of One Time Password has been done during the user login phase. During the registration phase user selects an email id, which is used to send the otp. During the login phase, the user calls out the otp and the otp is verified for the user to login.

3.2 Speech Recognition Module

The user's voice is converted into text with the help of Google speech recognition module. Although there were several options for a text speech tool in python such as Sphinx converter which converts speech to text on the system itself. However, results given by sphinx converter have not been convincing. Other options to convert speech to text are google cloud speech api, Wit, IBM speech to text, Houndify API.

3.3 Development Kit Used

The implementation of the proposed solution was done on an Ubuntu 20.04 operating system. The dependency tools or softwares such as Pyaudio, Python speech recognition and python otp module etc was taken care by the pipenv. Pipenv creates a python based virtual environment which takes care of the software's that have version compatibility issues with each other.

In addition, the authentication scheme was made as a web application to demonstrate the working of the proposed solution django framework in python has been used to implement the web application based authentication system.

3.4 Random Number Function

Random number generation has been used to issue One Time Password for the users to log in. In order to check whether numbers generated are completely random and cannot be predicted, the seed values have to be checked. The digits used in the proposed solution for generating the otp can set from defining a range from 0000 to 9999 for a four digit otp number or for a five digit otp 00000 to 99999 has to be used.

4 Design Specification

This section consists of the architecture of the proposed solution. The following diagrams give a brief idea about the components that are a part of the architecture. The architecture contains six components, user accessing the authentication scheme, registration module, login module, OTP module, speech recognition module and the service user has access to.

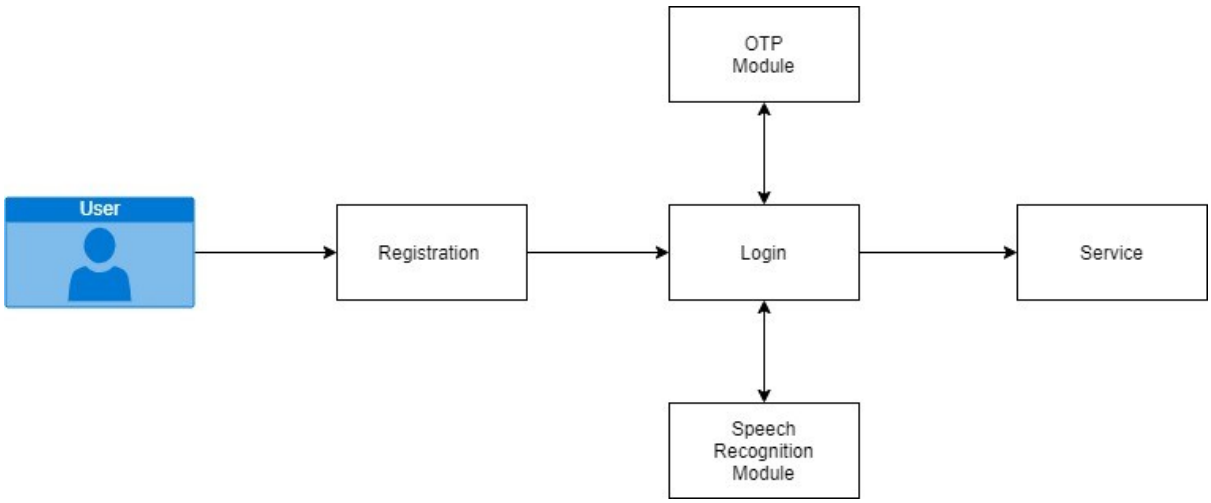

Figure 1: Figure Proposed Architecture

The function of each component has been briefly explained in the next section of implementation. The OTP generated for this project is a 4 digit otp ranging from 0000 to 9999 with the help of random function in math module which has to be imported in the program.

4.1 UML Diagram

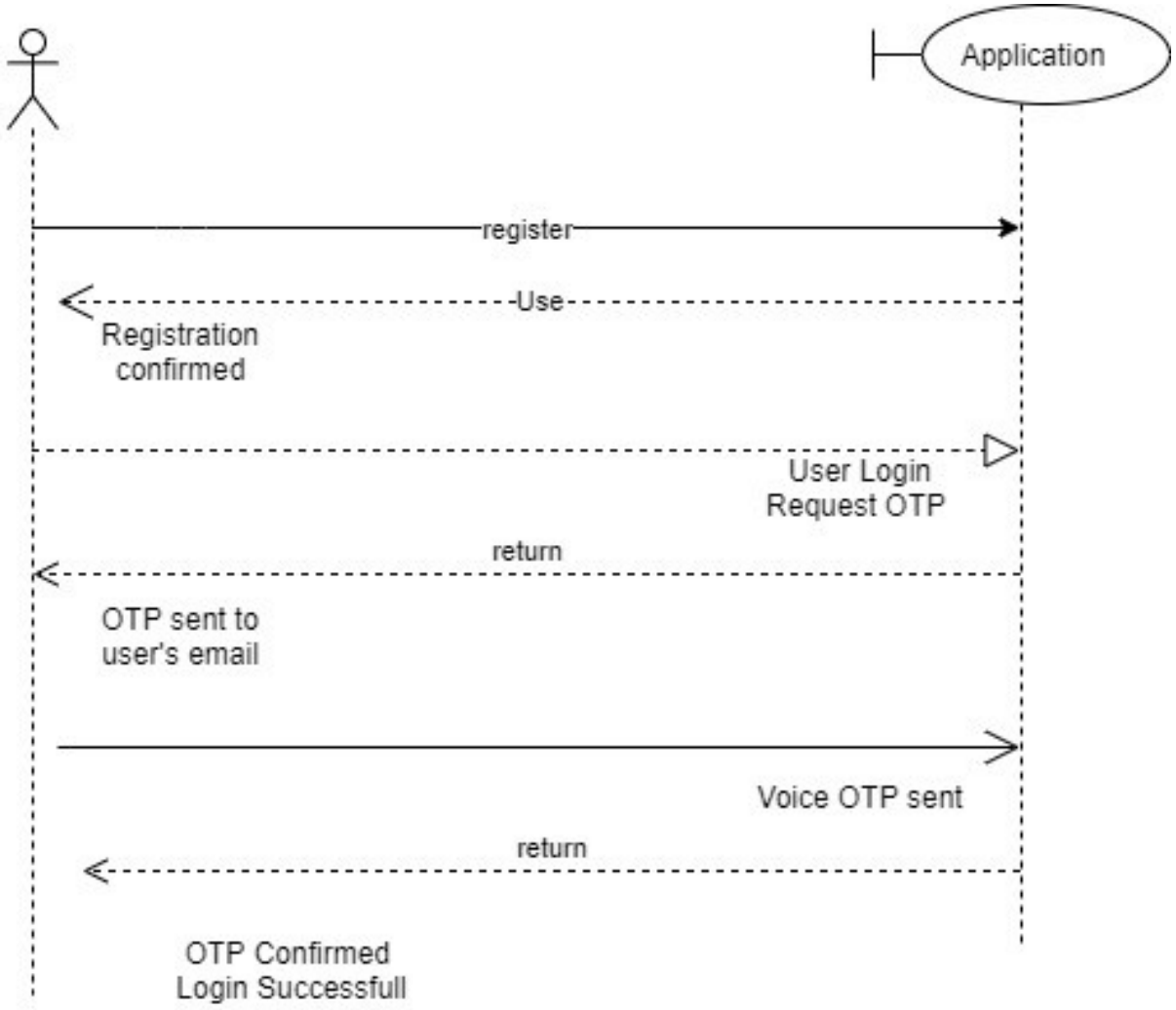

Figure 2: UML Diagram

4.2 Sequence Diagram

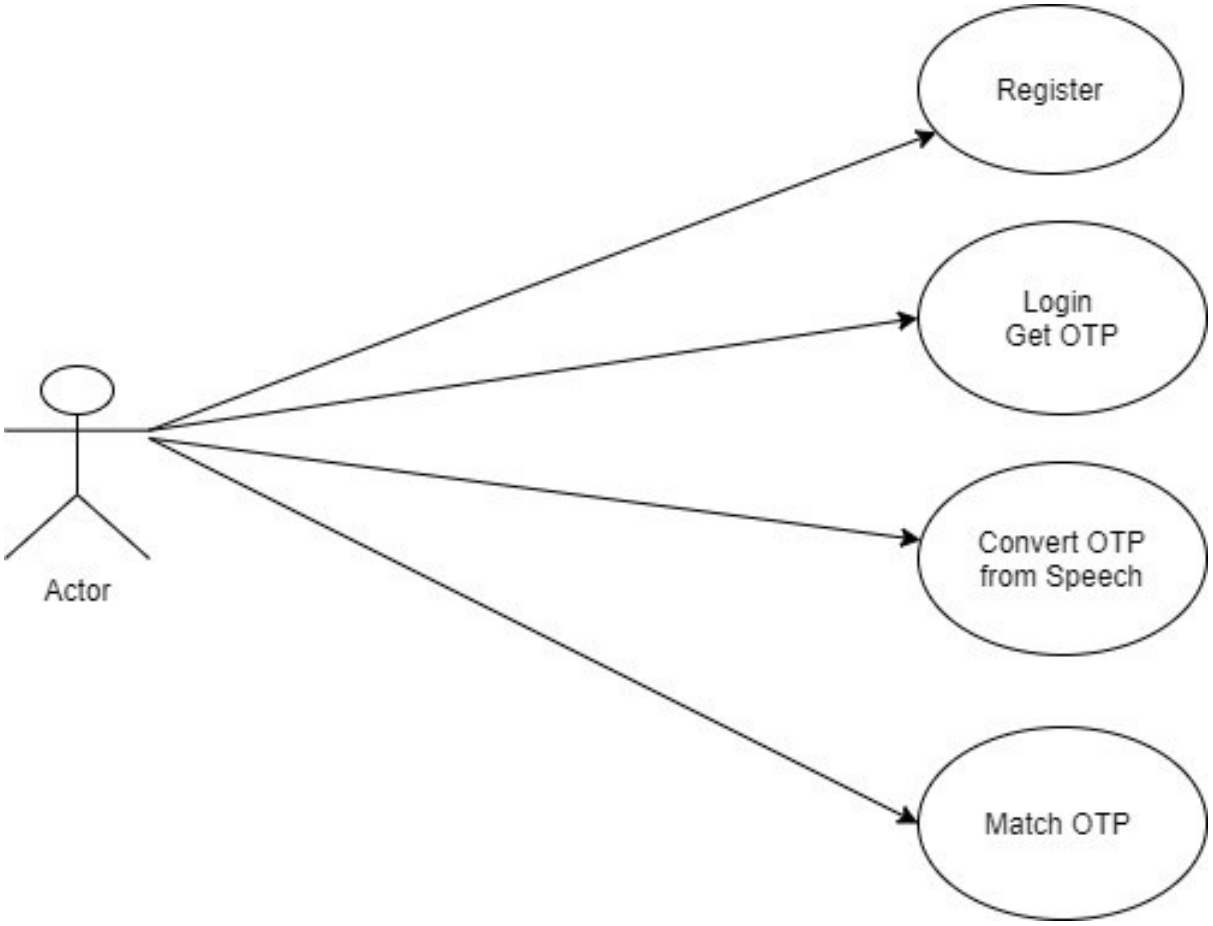

Figure 3: Sequence Diagram

5 Implementation

This section briefly describes each component of the proposed authentication scheme. Each component works in a methodological manner, in which each component depends on the output of the previous component. The proposed solution is divided in three phases which need user input. The phases are as follows:

1. Registration Phase
2. 2. Login Phase(Speech Recognition)

5.1 Registration Phase

This is the initial phase of the authentication system in which the user register's for the service. The form takes username and user's email id. The user's information is saved in the database and is used to map the user with their respective email id. Since the otp is sent on user's email it was very important to tie the username with the email id of the

user, as there might be a possibility of two users having the same username but every user has a unique email id which is used by the scheme to distinguish users and avoid OTP collisions.

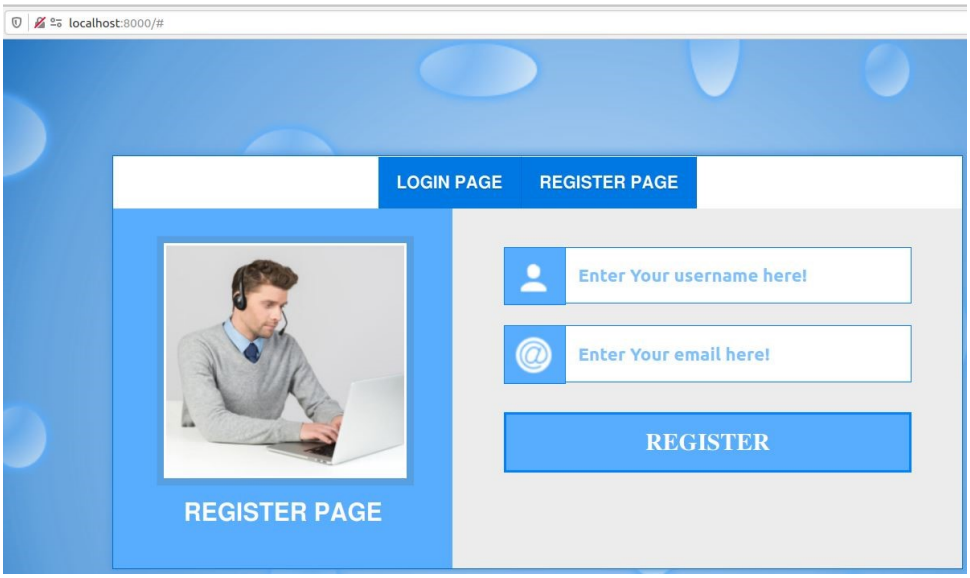

Figure 4: Registration Page

- Registration Successful

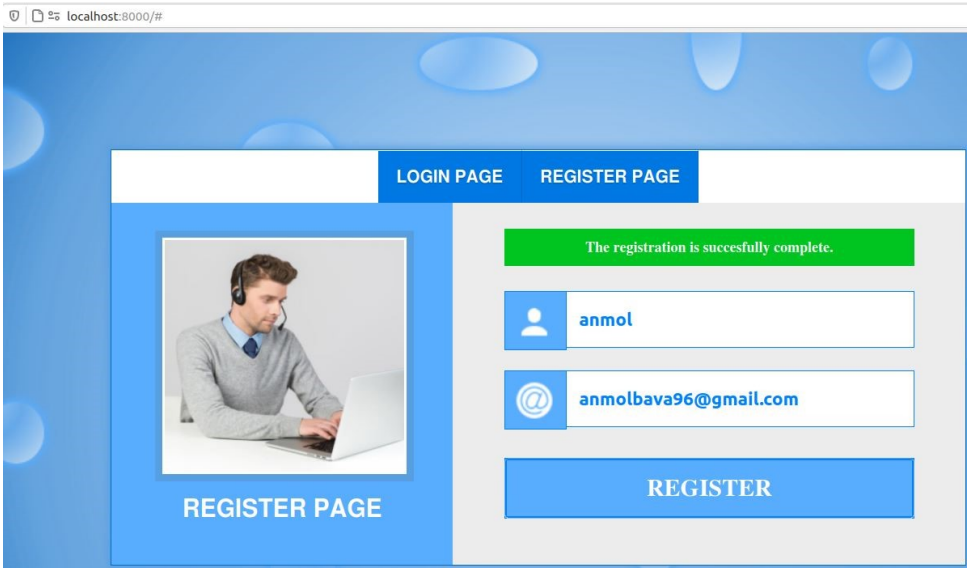

Figure 5: Registration Successful

5.2 Login Phase(Speech Recognition)

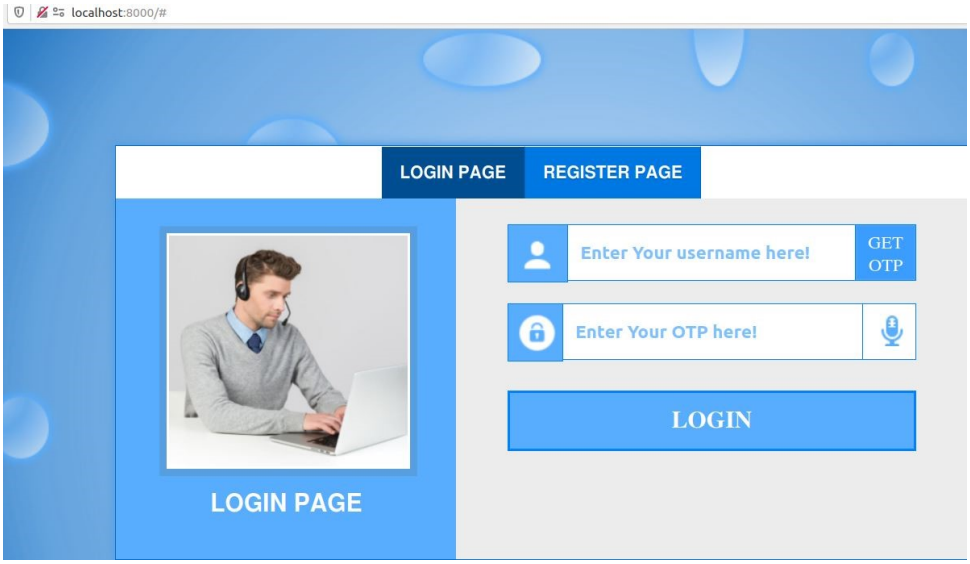

Figure 6: Login Page

- Step 1: Enter email id of user and click on get otp

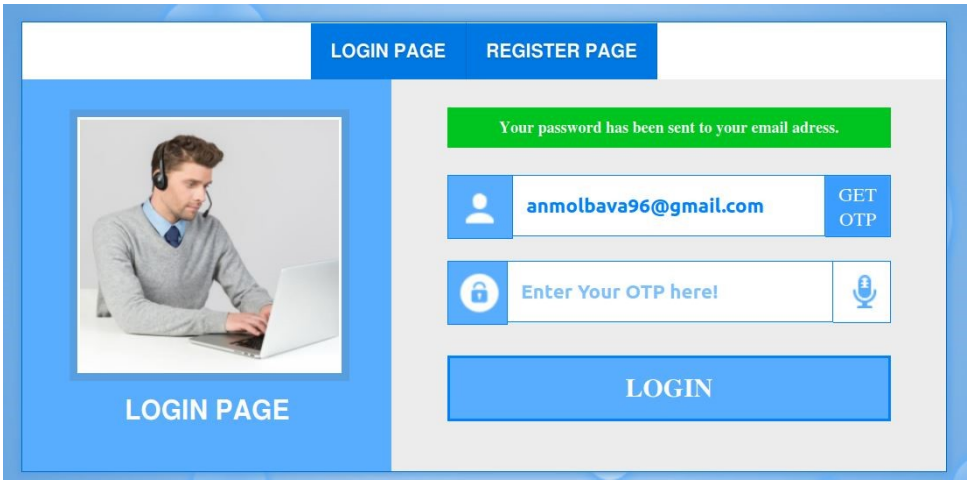

Figure 7: OTP Generation

- Step 2: Check email account for OTP

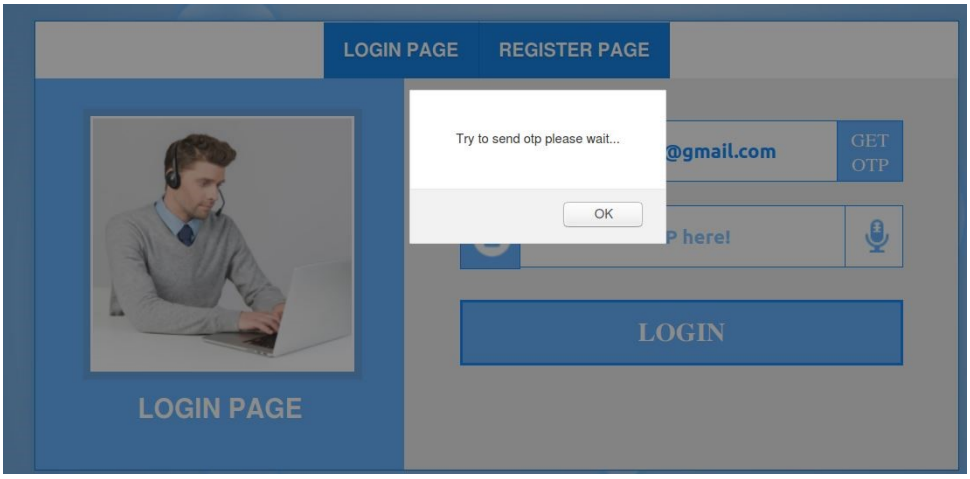

Figure 8: Sending OTP to Email

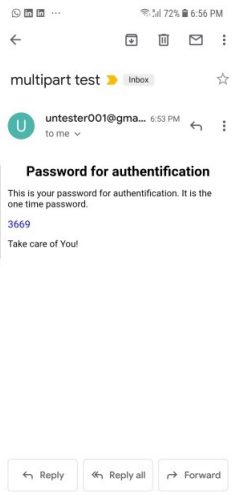

Figure 9: OTP received in email

- Step 3: enter OTP via speech console check

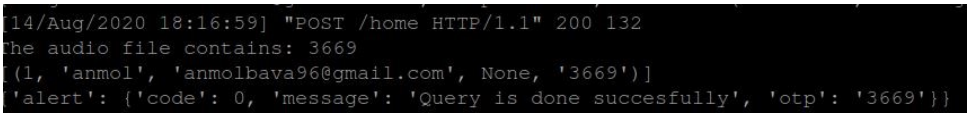

Figure 10: Otp converted from speech to text successfully

- Step 4: User Logged in successfully for the service

Figure 11: Successful Login

Once the user clicks on the register button, they become eligible to use the service provided by the web application. Once the user is registered and the user decides to login, the user will have to type the email id that was used to register in the system. The user then has click on GET OTP button which would initiate the process of generating and sending the otp to the user's email.

Once the user receives the otp on email, the user's needs to initiate the microphone symbol on the application and give permission to the web application to use the microphone. Once the microphone is initiated, the user's would speak the digits of the otp and the speech is then converted into the digits or integers. The user's speech is converted into digits or text with the help of PyAudio function in Speech_Recognition module which can be imported in Python and can be integrated in Django. Once the digits are processed they are sent to the backend of the web application where they are checked cross checked with the digits of the otp sent to the user's email.

6 Evaluation

6.1 Evaluation of Speech Recognition Modules

At first we need to evaluate the different types of speech recognition modules available. This comparison is critical to the evaluation of our proposed solution as determination

of the efficiency of speech recognition module will ultimately increase the success of the proposed authentication scheme.

Every speech recognition module converts speech to text in a different manner. Here we will determine the efficiency with which the module converts a set of sentences from speech to text will be tested. In order to test the speech recognition modules, 5 phrases have been taken which are listed down as follows below. Identification results of each of the modules are listed below.

- Phrase 1 = It is a good day to take a walk
- Phrase 2 = This is a notebook
- Phrase 3 = National college of Ireland
- Phrase 4 = Tommorow can be a bright sunny day

Table 1: Accuracy of STT modules

Speech to text Modules	**Phrase 1**	**Phrase 2**	**Phrase 3**	**Phrase 4**
Google Speech Recognition	Yes	Yes	Yes	Yes
Sphinx CMU	Incorrect	Yes	Yes	Yes
Houndify	Yes	Yes	Yes	Yes
Bing Voice Recognition	Yes	Yes	Yes	Incorrect

Thus, from the comparison a conclusion can be drawn about the stability of the speech recognition modules. For the proposed solution, Google speech recognition API module has been integrated. Even though other modules were equivalent, Google speech recognition is said to have more stablility.

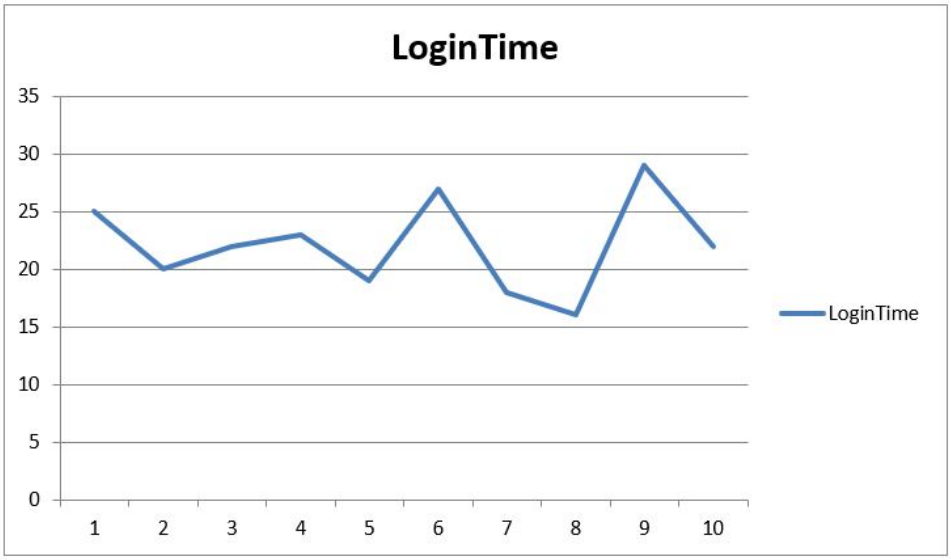

Figure 12: Average login time taken by the candidates

The X axis represents the number of seconds and Y axis represents the time taken to login by the user. A total census of 10 candidates was taken in which average login time was recorded. The average time taken for a candidate to login was 21 seconds ranging from 17 to 30 seconds. The time recording has been started from the moment the user hits the Get Otp button till a successful login page has been reached.

6.2 Discussion

The section represents the efficiency of the proposed authentication scheme. The research on an authentication system has been performed and the section evaluates the output from various parameters. The results of the proposed system have been determined by comparing speech recognition modules, penetration testing and a user survey. The user survey was conducted on people who work with laptops more often.

7 Conclusion and Future Work

Authentication is an important domain in the field of cyber security. Authentication systems are integrated to a service, to make sure the person trying to access the service is authorized. Authentication systems implement access control with the help of two things that is, things that the user might have memorized or have possession in. The proposed solution has two advantages that have been heighted in Section 6. One factor that has significantly improved is the ease of access as the project is speech based. Secondly, the security of the otp scheme has increased as the user will have to speak and reaction time for the user to enter the otp decreases, hence giving less time to the attacker to shoulder surf and enter the otp. The speech based otp also prevents attacks such as keylogger based attacks and bruteforce attacks. The proposed solution is divided into two part, registration and login parts. The speech recognition module is activated in the login part to convert speech into text. The speech recognition part is used to convert the digits of the otp spoken by the user into text. Then the application will check the converted otp against the otp that was originally sent to the user. If both the otps match, the user has access to the service.

The evaluation of the proposed model has been done with three parameters user survey, attack scenario and comparison between the speech synthesis model. All parameters prove that the proposed model has high efficiency. The only limitation with the proposed model was that there was no technique implemented that could tie the user's voice with email id. Also the transmission of between the user and the application should be encrypted to secure the voice samples and protect the otp from man in the middle attack.

References

[1] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, p. 770–772, Nov. 1981. [Online]. Available: https://doi.org/10.1145/358790.358797

[2] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards Interfaces*, vol. 32, pp. 321–325, 10 2010.

[3] S. Sood, "An improved and secure smart card-based authentication scheme," *Int. J. of Multimedia Intelligence and Security*, vol. 2, pp. 75 – 89, 01 2011.

[4] A. Adams and A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40–46, 12 1999.

[5] K.-P. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," *International Journal of Human-Computer Studies*, vol. 65, pp. 744–757, 08 2007.

[6] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security & privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[7] G. Nielsen, M. Vedel, and C. D. Jensen, "Improving usability of passphrase authentication," in *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 2014, pp. 189–198.

[8] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct horse battery staple: Exploring the usability of system-assigned passphrases," in *Symposium on Usable Privacy and Security (SOUPS)*, 2012.

[9] A. Addas, J. Thorpe, and A. Salehi-Abari, "Geographic hints for passphrase authentication."

[10] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, pp. 1–41, 2012.

[11] F. A. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641–644, 2009.

[12] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[13] B. Groza and D. Petrica, "One-time passwords for uncertain number of authentications," *Proceedings of CSCS15*, 2005.

[14] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T.-H. Kim, and H. Elkamchouchi, "Mobile one-time passwords: two-factor authentication using mobile phones," *Security and Communication Networks*, vol. 5, no. 5, pp. 508–516, 2012.

[15] L. Gong, J. Pan, B. Liu, and S. Zhao, "A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords," *Journal of Computer and System Sciences*, vol. 79, no. 1, pp. 122–130, 2013.

[16] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud authentication based on anonymous one-time password," in *Ubiquitous Information Technologies and Applications*. Springer, 2013, pp. 423–431.

[17] F. Cheng, "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm," *Mobile Networks and Applications*, vol. 16, no. 3, pp. 304–336, 2011.

[18] B. Cha, N. Kim, and J. Kim, "Prototype analysis of otp key-generation based on mobile device using voice characteristics," in *2011 International Conference on Information Science and Applications*. IEEE, 2011, pp. 1–5.

[19] S. Phatak, "Implementing colour shuffling with otp as a defence against shoulder surfing," Ph.D. dissertation, Dublin, National College of Ireland, 2019.