IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12463

Implementation of a Password less Multifactor Authentication Scheme

Ramalingam H M[1],

Vismita Kuppayya Naik[2], Sushan S Hegde[3], Sharon Joyel Lobo[4] , Rithin M[5]

Assistant Professor, Electronics & Communication Engineering, MITE, Moodabidri, India[1]

Student, Electronics & Communication Engineering, MITE, Moodabidri, India[2-5]

Abstract: Today web services are used by billions of people for various purposes like news, E-mail, and browsing information. Nowadays people have several accounts in email, social networks, and many services. All of these employ traditional authentication method such as password authentication. Having different or various kinds of passwords for different accounts and remembering or memorizing those passwords is very difficult. So, the user ends up with a simple password. But this will become easy for hackers, especially during the transaction. For these problems, this project provides a password less multifactor authentication system. This includes face authentication, voice authentication, and hardware authentication method.

Keywords: MFA, Passwordless, Attiny85, USB

I. INTRODUCTION

The continuous growth in the number of smart devices has impacted mobile services immensely around the globe. In such a connected world to keep the transmitted data secured most important thing is authentication. Authentication provides access to control for systems by checking, with the help of the user's credentials. The authentication process enables organizations to keep their network secure by permitting only authenticated users to protect the resource. Initially, only one factor was used for authentication Single Factor Authentication was majorly used by people due to its user-friendliness and simplicity. Also, it is the simplest form of authentication. As an example, the use of a password to confirm the ownership of the user ID could be considered. This was the weak level of the authentication method. By knowing the password, anyone can easily hack the account. For this, users increase the complexity of the password and use two-factor authentication. It uses the same username or password in addition to verifying the user with the help of a device like a mobile. It couples the representative data with the factor of personal ownership. But the problem is he always keeps the mobile with him [1]. Then, Multi-Factor Authentication [2][3] provides a higher level of security and also facilitates continuous protection of computing devices and also other strategic services from unauthorized access by using multiple categories of authorization. This authentication requires the user to provide two or more authenticators [4][6].MFA is based on biometrics or behavioral, which is the automated recognition of individuals based on their biological and behavioral characteristics without using passwords [5]. This helps to improve the level of security as the users were required to present evidence of their identity, which relied on two or more different factors like face, voice, fingerprint, etc.

Face authentication [7][8] is the technology that matches the face of a human against the database of faces. It is a regular and effortless task. In face recognition, the first step is face detection which includes several factors profile pose, chin, and facial expression. Then extracting [9][10] the features from the face, and after that, it compares the face with the face that is stored in the database. Voice authentication [11][12] is a method to identify or verify the user's voice for security. Because a person's voice is uniquely characterized by one other [13]. And it is a fast and secure method. Speech recognition is done by breaking down the recording into frequency segments. To provide more security, multifactor authentication is combined with hardware authentication. Hardware authentications are like digital signatures [14][15], atm cards, attiny85, etc. A hardware authentication includes the hardware device that acts as an identity verifier or security token including a USB stick or embedded circuit within an external device.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12463

Fig.1 Attiny 85 hardware device

II. METHODOLOGY

This project provides a multifactor authentication that is face recognition, voice recognition, and hardware authentication. Multifactor authentication provides a high level of security to users and the resources that users can access. This project consists of two to three authentication methods for the user to pass during the login process. For the first stage during signup, the system checks the face of the user if it is matching with the data stored in the database then it allows another authentication mechanism like voice authentication Once it is complete with the above authentication then it goes for the next step of authentication which is hardware authentication. The hardware authentication consists of a Hardware device like a USB. In the hardware authentication method, the password is not. Once the hardware is plugged into the system it directly accesses the password. The technique of Human face recognition is a biometric identification that uses the unique characteristics of an individual's human face. This can be done by using the machine learning algorithm. The first step is to detect the face from the haar cascade classifier which is a machine-learning algorithm that trained positive and negative images. Once faces have been detected, the next step is to extract the feature from them by using a computer convolution network. CNNs learn to extract the features from images such as the texture of the skin, shape of the nose, etc and use features to classify the images into different categories. Then extract the feature from the image. The last step is to match the extracted feature of a face with faces in the database. Voice authentication is done by using the Gaussian mixture algorithm, to verify a person's identity; the biometric voice recognition system captures a new speech sample, creates a template from the sample, and compares it against the enrollment template. A strong match between templates indicates that the same person spoke both samples, thus verifying the person's identity. Hardware authentication including the hardware device that acts as an identity verifier or security token including a USB. A user plugs the hardware device into the system for authentication. Here, a USB device is similar to a rubber ducky. The rubber ducky is used to hack or steal the password. But here we are doing the reverse process that is hardware device is used for a security mechanism.

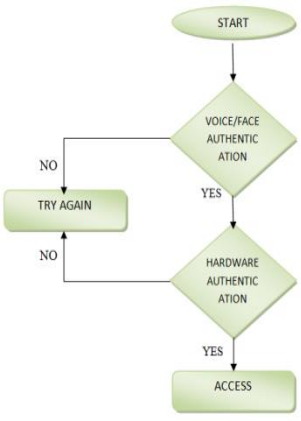


Fig.2 Two factor authentication

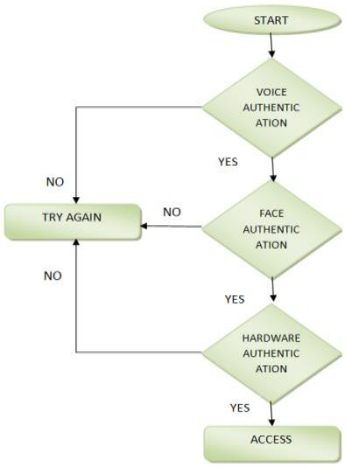


Fig.3 Multifactor authentication

III. RESULTS

This project combine different authentication methods to provide an easy, faster, better, and more secure mechanism for authentication and to replace traditional authentication systems based on passwords. And provide a high degree of security and Reduce the risk from unauthorized person.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12463

Below Fig.4 explains the training the user voice to the system and detection of the voice of the user in voice authentication.

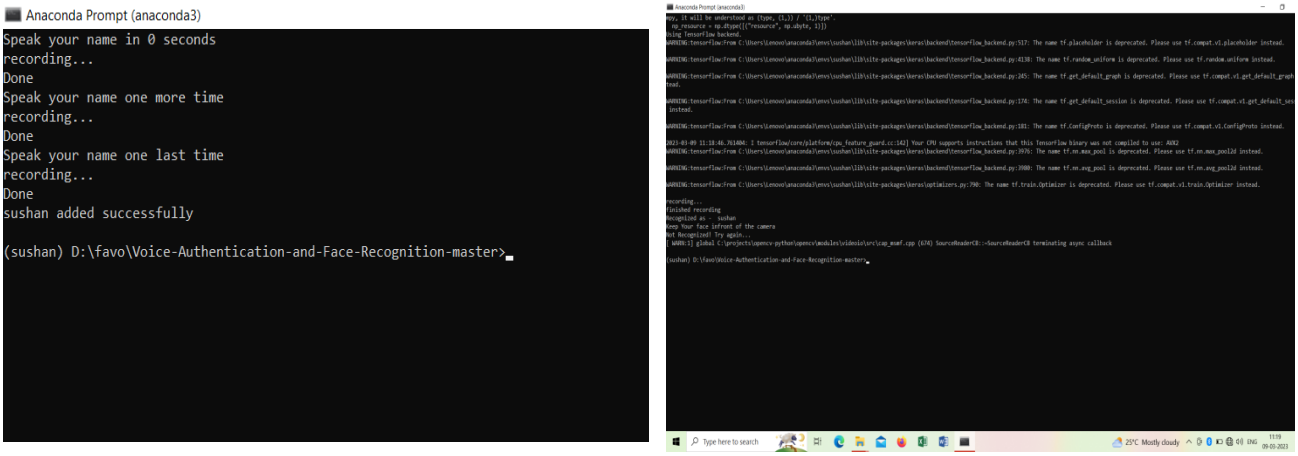
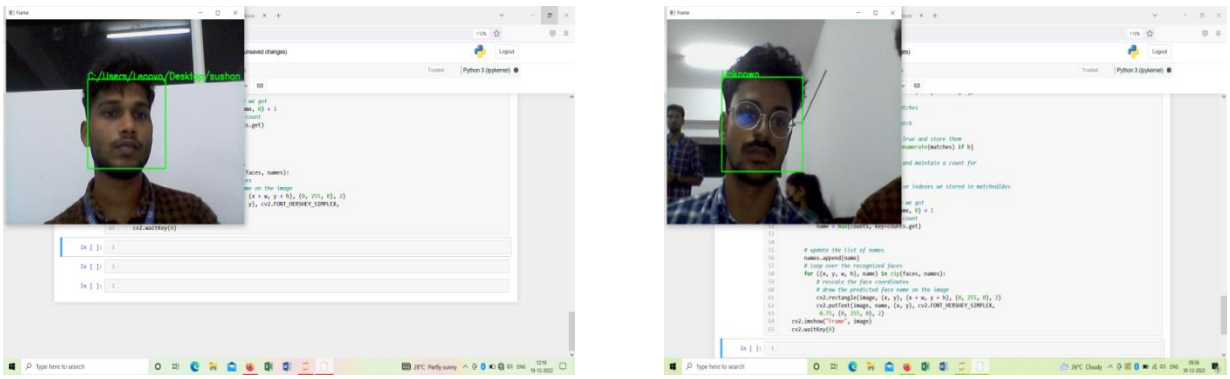


Fig.4 Voice authentication

Below Fig.5 tells about the face authentication, Identifying the authorised user (a) and unauthorized user (b) with the help of computer convolution algorithm in face authentication



(a) (b)

Fig.5 Face authentication

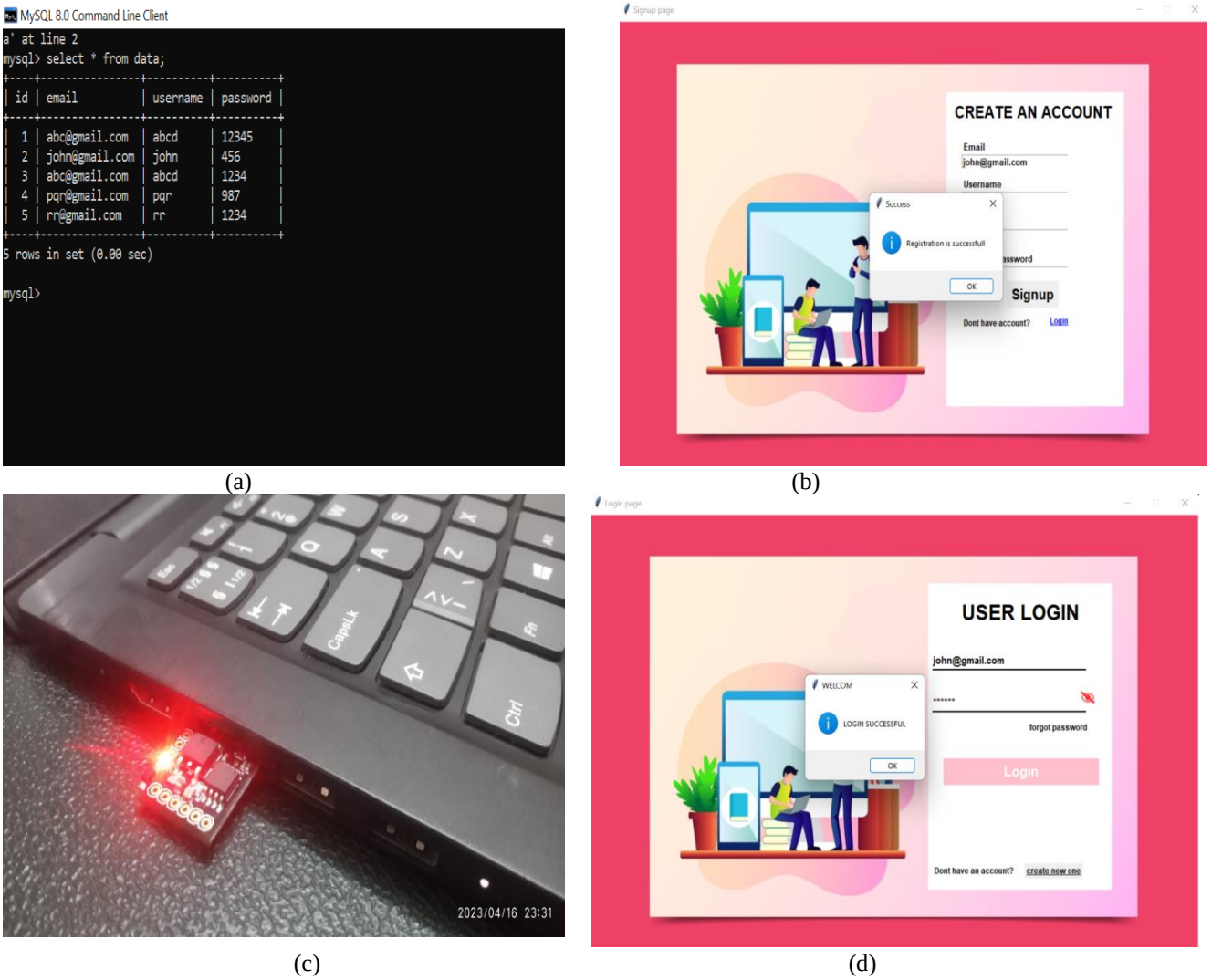
Fig.6 tells about hardware authentication by using hardware device attiny85, for that create the database of username and password in mysql database(a) and create a webpage for registering the user(b) and login (d). for enter the password, insert the hardware device in to system USB port(c)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12463



(a) (b)

(c) (d)

Fig.6 Hardware authentication

IV. CONCLUSION

Multifactor authentication is a secure authentication technique. In this paper, the authentication method used is face authentication, voice authentication, and hardware authentication. And also tell about the recovery mechanism in the hardware authentication. Here proposed a solution composed of two to three authentication methods during the login process. During the initial stage, the user can select the authentication at his/her convenience. In future work, to increase security also use behavioural authentication. Behavioural authentications like keystroke mechanism, retina recognition. Which provide a more security.

REFERENCES

[1] A. Nath, “Issues and Challenges in Two Factor Authentication Algorithms Article in,” 2016. [Online]. Available: https://www.researchgate.net/publication/292392168

[2] G. S, S. RK, Prof. F. Jaison, and Dr. M. Aadil, “A Study on Three Step Multifactor Authentication System for Modern Security,” Int J Res Appl Sci Eng Technol, vol. 10, no. 3, pp. 10–12, Mar. 2022, doi: 10.22214/IJRASET.2022.40532.

DOI: 10.17148/IJARCCE.2023.12463

[3] M. A. B. Z. Elizabeth C. Donald, "A CASE STUDY IN SELECTION AND DEPLOYMENT OF A MULTI-FACTOR AUTHENTICATION SOLUTION," Issues In Information Systems, 2021, doi: 10.48009/3_iis_2021_69-80.

[4] C. Singh and T. D. Singh, "A Systemic Review of Various Multifactor Authentication Schemes," International Journal of Computer Sciences and Engineering, vol. 7, no. 2, pp. 503–510, Feb. 2019, doi: 10.26438/ijcse/v7i2.503510.

[5] S. K. Ravi and S. E. T, "IJARCCE Study on Framework for Password-less Authentication," International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 2, 2016, doi: 10.17148/IJARCCE.2016.52149.

[6] M. Aldwairi and S. Aldhanhani, "Multi-Factor Authentication System FLUKES: Automated log threat extractor tool View project Multi-Factor Authentication View project," 2017. [Online]. Available: https://www.researchgate.net/publication/319312344

[7] M. Tamilselvi, Dr, and S. Karthikeyan, "A Literature Survey in Face Recognition Techniques," 2017. [Online]. Available: http://www.ijpam.eu

[8] M. Mahmood Hussein et al., "Face recognition," p. 12006, 2021, doi: 10.1088/1742-6596/1755/1/012006.

[9] Akanksha et al., "Face detection and Recognition: A review," 6th International Conference on Advancements in Engineering & Technology (ICAET-2018, Feb. 2018.

[10] K. Dilip Pandya, "Face Detection-A Literature Survey," International Journal of Computer Techniques, vol. 3, 2016, [Online]. Available: http://www.ijctjournal.org

[11] A. H. K. M. K. and P. S. Aithal, "Voice Biometric Systems for User Identification and Authentication – A Literature Review," International Journal of Applied Engineering and Management Letters, pp. 198–209, Apr. 2022, doi: 10.47992/ijaeml.2581.7000.0131.

[12] D. R. Chandran and D. R. Chandran, "Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices," Journal of Computer and Communications, vol. 10, no. 6, pp. 11–21, Jun. 2022, doi: 10.4236/JCC.2022.106002.

[13] N. Singh, A. Agrawal, and R. A. Khan, "Voice Biometric: A Technology for Voice Based Authentication," Adv Sci Eng Med, vol. 10, no. 7, pp. 754–759, Oct. 2018, doi: 10.1166/ASEM.2018.2219.

[14] R. Sultana and T. Shahid, "A Survey on Digital Signatures," 2021. [Online]. Available: www.ijrpr.com

[15] J. Chandrashekhara, A. v B, P. H, and R. B R, "A COMPREHENSIVE STUDY ON DIGITAL SIGNATURE," International Journal of Innovative Research in Computer Science & Technology, vol. 9, no. 3, May 2021, doi: 10.21276/IJIRCST.2021.9.3.7.