

# Examining the Authentication of a user using 3D Password

Mrs. Afsha Firdose<sup>1</sup>, Mrs. Nischitha A R<sup>2</sup>, Mr. Dhruva M S<sup>3</sup>, Mr. Smitha A S<sup>4</sup> and Mr. Balaji B S<sup>5</sup>

<sup>1-2</sup>Asst Prof., Dept. of Information Science and Engg, ACU, BGSIT, India

Email: afshafirdosecse@gmail.com, nischitha.ar@gmail.com

<sup>3</sup>Asst Prof., Dept. of Computer Science and Engg, ACU, BGSIT, India

Email: msdhruva@gmail.com

<sup>4-5</sup>Asst Prof., Dept. of Electronics & Communication Engg, ACU, BGSIT, India

Email: drsmithaas@bgsit.ac.in, balajibs2011bgsit@gmail.com

**Abstract**—Realtime authentication using 3D passwords represents a novel approach to enhancing security by leveraging the complexity and versatility of three-dimensional virtual environments. Unlike traditional alphanumeric passwords, 3D passwords involve a sequence of user interactions and either internet or mobile connection. This work explores an approach to real-time authentication using 3D passwords by integrating fingerprint, facial expression and other inputs.

Extensive experimental results demonstrate an authentication accuracy of approximately 85%, showcasing the potential of this multi-modal approach in providing a robust and secure authentication mechanism. This method offers several advantages, including increased security through unique and hard-to-replicate passwords, improved user engagement, and flexibility in password creation.

## I. INTRODUCTION

With the increasing prevalence of cyber threats and the limitations of traditional password systems, the need for more secure and robust authentication methods has become paramount. Realtime authentication using 3D passwords presents an innovative solution that enhances security by incorporating complex and dynamic user interactions within a three-dimensional virtual environment. This method leverages a combination of biometric and behavioural factors, such as facial expressions, eye-ball movements, and keyboard inputs, to create a unique and hard-to-replicate password.

The traditional password systems rely primarily on static alphanumeric characters, which are vulnerable to various forms of attacks, including brute force, phishing, and keylogging. Despite advancements like two-factor authentication (2FA) and biometric verification, these methods often face usability and security challenges. The concept of 3D passwords offers an advanced alternative by integrating multi-modal inputs that increase the complexity and uniqueness of the authentication process. The 3D password concept explores an innovative approach to Realtime authentication using 3D passwords by integrating finger-print, facial expressions and keyboard inputs. These biometric and behavioural factors are collated and normalized to form a comprehensive 3D password, which is subsequently validated for user authentication. The proposed method leverages the complexity and uniqueness of individual user interactions to enhance security beyond traditional passwords. Extensive experimental results demonstrate an authentication accuracy of approximately 80%, showcasing the

potential of this multi-modal approach in providing a robust and secure authentication mechanism. The findings suggest that integrating diverse biometric and behavioural inputs can significantly improve the reliability and security of authentication systems.

## II. ANALYSIS OF RELATED METHODS

Existing authentication systems primarily rely on traditional methods such as passwords, PINs, and more recently, biometric techniques like fingerprint and facial recognition. While these systems have served well over the years, they present several vulnerabilities and limitations, prompting the need for more advanced and secure solutions like 3D password authentication.

### A. Traditional Passwords and PINs

The traditional password and PIN work on the principle of knowledge-based authentication, where access is granted based on something the user knows. This traditional passwords and PINs, while widely used for authentication, have several notable drawbacks like weak security, poor management and high maintenance.

### B. Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) enhances security by requiring two different forms of identification before granting access to an account or system. This process involves two layers of verification, typically categorized as “something you know” (like a password) and “something you have” (like a mobile device or hardware token). This two-Factor Authentication (2FA) method significantly improves security by adding an extra layer of verification, but it also introduces challenges related to convenience, accessibility, cost, and potential security vulnerabilities.

### C. Biometric Authentication

Biometric authentication utilizes unique biological characteristics of individuals for identity verification. It relies on the premise that certain physiological or behavioural traits are distinctive to each person, such as fingerprints, iris patterns, facial features, voice patterns, or even typing rhythms. In this method we face challenges related to privacy, cost, accessibility, environmental factors, security risks, legal issues, and technology limitations.

### D. Behavioural Authentication

Behavioural authentication is a method of identity verification that analyses patterns in an individual’s behaviour or actions to authenticate their identity. Unlike biometric authentication, which focuses on physical characteristics, behavioural authentication relies on behavioural traits that are unique to each person. While behavioural authentication offers a non-intrusive and continuous method of verifying identity, it also faces challenges related to variability in behaviour, privacy concerns, implementation complexity, accuracy, user acceptance, environmental factors, security, and cost.

## III. PROPOSED 3D PASSWORD AUTHENTICATION METHODOLOGY

3D password authentication involves creating and using a password within a three-dimensional virtual environment. This method leverages the complexity and versatility of 3D interactions to enhance security. Unlike traditional passwords, 3D passwords have included a combination of actions such as navigating through virtual spaces, manipulating objects, and performing specific gestures.

### A. 3D Password generation

Generating a 3D password using fingerprint, facial expression, and input involves capturing and combining biometric and behavioural data within a virtual 3D environment.

Firstly design the 3D environment using 3D modeling software to create a virtual environment for capturing fingerprint data, facial expressions, and other inputs. Using the biometric sensor capture the user's fingerprint data. Using facial recognition software detect and analyse the user's facial expressions, such as smiling, frowning, or blinking.

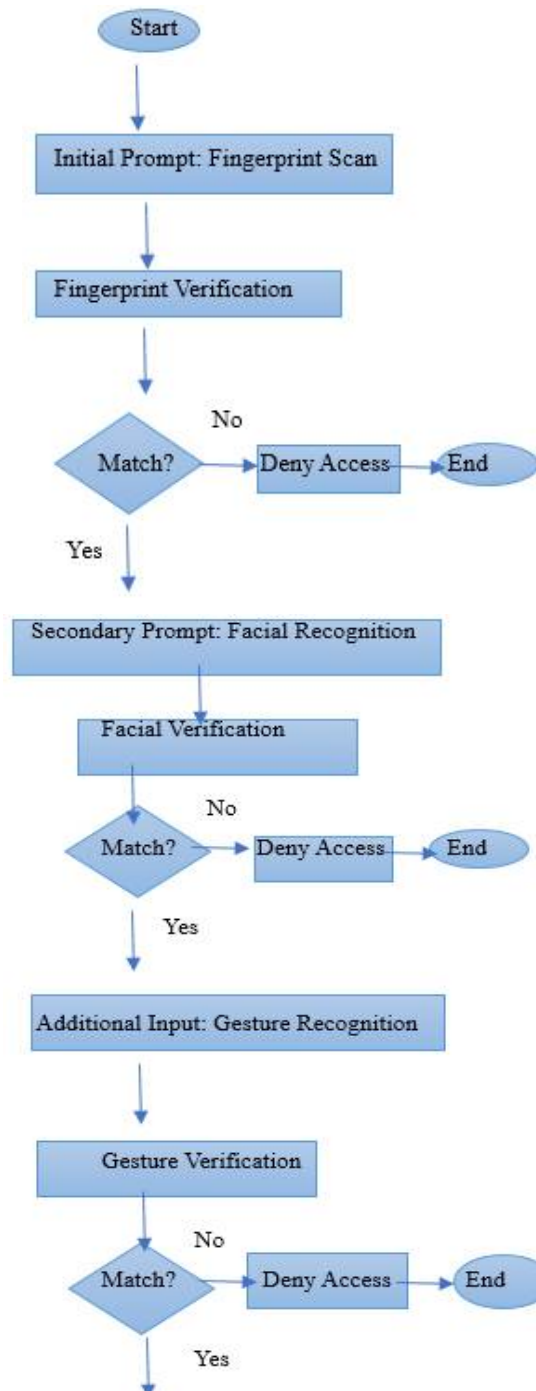
For other input, integrate facial recognition libraries, collision detection, virtual keyboard interface within the 3D environment to assign specific actions such as touching objects, making facial expressions, or typing on a virtual keyboard.

### B. 3D Password Detection

The password generated in real time is compared with standardized value. Also Provide real-time feedback to the user during the authentication process to confirm successful verification or prompt for additional actions.

### C. Benefits of using 3D Password:

Using a 3D password system, which combines fingerprint, facial expression, and other input data, provides enhanced security through multi-layered authentication, increased difficulty for attackers, improved convenience for users, continuous authentication capabilities, resilience to common attacks, versatility, and reduced password fatigue. These advantages make 3D passwords a robust and user-friendly solution for secure authentication.



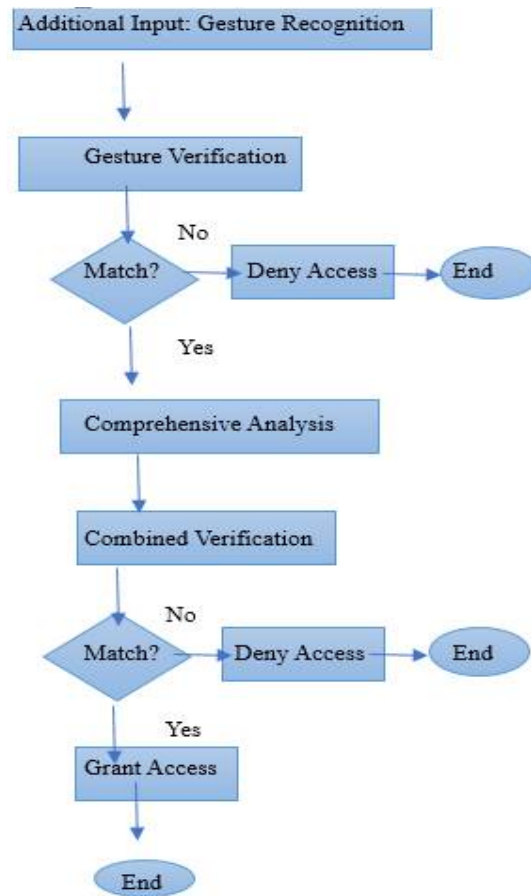


Fig. 1: Flow Chart

#### IV. RESULT

A simulation is performed to test the proposed scheme. The average of ten sample set for finger print, Facial Expression, and other Input. The proposed system achieved an 85% high level of accuracy in verifying users' identities using the 3D password method.

TABLE I: AUTHENTICATION METHOD

| Method                | Security | User Convenience | Cost | Privacy | Accuracy |
|-----------------------|----------|------------------|------|---------|----------|
| Traditional Passwords | 5        | 7                | 4    | 6       | 6        |
| Fingerprint Only      | 7        | 8                | 6    | 5       | 8        |
| Facial Recognition    | 7        | 8                | 6    | 5       | 8        |
| 3D Password           | 10       | 7                | 7    | 4       | 9        |

#### V. CONCLUSION

The concept of using a 3D password for authentication represents a novel approach to enhancing security in user authentication systems. By leveraging a three-dimensional environment, this method incorporates multifactor

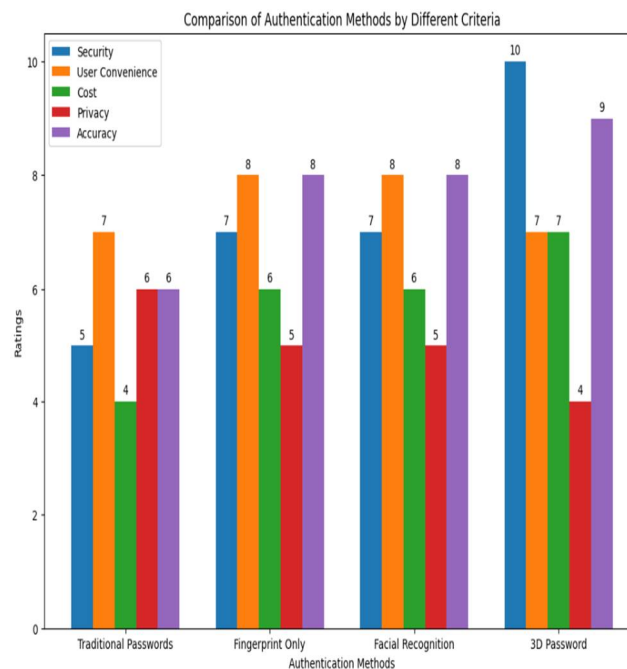


Fig. 2: Results of 3 D Authentication

authentication such as fingerprint, facial expression and other inputs like touching objects, making facial expressions, or typing on a virtual keyboard. This 3D method is worthwhile for environments where high security is paramount. As technology continues to evolve, the 3D password system could become a more practical and widely adopted solution in the future.

#### REFERENCES

- [1] Patil, A., & Shah, P. (2015). "Security Analysis of 3D Password." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 1. IJARCCCE.
- [2] hurana, A., & Sharma, P. (2015). "Analysis of 3D Password Authentication System Using K-NN Algorithm." International Journal of Engineering and Technical Research (IJETR), Vol. 3, Issue 6. IJETR.
- [3] Alka, A., Pravin, S., & Roopali, J. (2017). "A Survey on 3D Password Authentication System." International Journal of Advanced Research in Computer and Communication Engineering. IJARCCCE.
- [4] Alsulaiman, F. A., & El Saddik, A. (2008). "Three-Dimensional Password for More Secure Authentication." IEEE Transactions on Instrumentation and Measurement, 57(9), 1929-1938. IEEE Xplore
- [5] Bhosale, V., & Vaidya, D. (2012). "Evaluation of 3D Password." International Journal of Soft Computing and Engineering, 2(2), 137-141. IJSCE.
- [6] Duo Security, "The Guide to Modern Multi-Factor Authentication," <https://duo.com/resources/ebooks/the-guide-to-modern-multi-factor-authentication>.
- [7] A.B. Gadicha and V.B. Gadicha, "Virtual Realization using 3D Password", International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222).
- [8] Dhatri Raval and Abhilash Shukla, "Security using 3D Password", CMPICA CHARUSAT Changa International Journal of Computer Applications (0975-8887), vol. 120, no. 7, June 2015.
- [9] H A Dinesha and V K Agrawal, "Multi -level Authentication Techniques for Accessing Cloud Services", CORI Bangalore. Karnataka Tanvi Naik Sheetal Koul Multi-Dimensional and Multi-Level Authentication Techniques Information Technology SKNCOE Pune.
- [10] Jianhua Song, Degang Wang, Zhongyue Yun and Xiao Han, Alphapwd: APassword Generation Strategy Based on mnemonic Shape, Hubei Wuhan 430062:School of Computer Science and Information Engineering, Hubei University.
- [11] Swati Bilapatte and Sumit Bhattacharjee, "3D Password: A novel approach for more secure authentication", International Journal of Computer Science and Engineering Technology (IJCSET).
- [12] Aakansha S. Gokhalea and Vijaya S. Waghmareb, "The Shoulder Surfing Resistant Graphical Password Authentication Technique", 7th International Conference on communication Computing and Virtualization published by Elesvier, vol. 79, 2016.
- [13] Neha and Vinod Saroha, "Hybrid Approach of 3D PASSWORD Using Naive Bayes Classification", IJCSMC, vol. 5, no. 6, June 2016.

- [14] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruene-feld, et al., "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization", Proc. CHI 2021, 2021.
- [15] Ilam Vazhuthi P Paruthi, M Geetha and S Parthiban, "A Survey on the Use of 3D Password in Security", International Journal for Research in Applied, vol. 3, no. II, February 2015, ISSN 2321-9653.
- [16] Priya Matta and Bhasker Pant, "TCpC: a graphical password scheme en-suring authentication for IoT resources" in Bharati Vidyapeeth's Institute of Computer Applications and Management, Springer, 2018.
- [17] P. Kürtünlüoğlu, B. Akdik and E. Karaarslan, Security of virtual reality authentication methods in Metaverse: An overview, 2022.
- [18] T. Mustafa, R. Matovu, A. Serwadda and N. Muirhead, "Unsure how to authenticate on your VR headset? Come on use your head!", Proc. IWSPA, 2018.
- [19] M. Yadav and M. Breja, "Secure dna and morse code based profile access control models for cloud computing environment", Proc. ICCIDS, 2019.
- [20] Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu and X. Zhou, "Behavesense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics", Ad Hoc Networks, vol. 84, pp. 9-18, 2019.