International Journal for Modern Trends in Science and Technology, 8(02): 176-179, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0802029
Available online at: http://www.ijmtst.com/vol8issue02.html

Secure Authentication Using 3D Password

Anjana V R* | **Sangeetha J**

Department of Computer science, St. Alberts College (Autonomous) Banerjee Road, Cochin, Kerala.
*Corresponding Author Mail Id: anjanavr876@gmail.com

To Cite this Article
Anjana V R and Sangeetha J. Secure Authentication Using 3D Password. International Journal for Modern Trends in Science and Technology 2022, 8 pp. 176-179. https://doi.org/10.46501/IJMTST0802029

Article Info
Received: 20 January 2022; Accepted: 14 February 2022; Published: 20 February 2022.

ABSTRACT

Textual passwords, biometric scanning, tokens or cards (such as an ATM), and other password models are now available to users. Textual passwords, for the most part, use an encryption method. Biometric scanning serves as your natural signature, while Cards or Tokens serve as proof of your identity. However, some people despise having to carry their cards with them, and others reject to have their retinas exposed to powerful IR (Biometric scanning). Nowadays, most textual passwords are kept basic, such as a phrase from the dictionary or their pet names. Klein used to do these tests and could crack 10-15 passwords every day. With the advancement of technology, fast computers, and a plethora of Internet-based applications, this has become a child's game.As a result, 3D passwords are a more customised and intriguing method of authentication. Passwords are now predicated on the fact that humans have memory. Simple passwords are usually used so that they may be remembered easily. In our concept, the human memory must go through the processes of recognition, recall, biometrics, and token-based authentication. The 3D password GUI appears once you've implemented it and logged in to a secure site. This is a second textual password that the user can type in. A 3D virtual room will appear on the screen after he completes the first authentication. Let's imagine we're talking about a virtual garage. In today's garage, one will find a variety of tools, equipment, and other items.

KEYWORDS:3D password, multi-factor Authentication, Recall, Recognition, Token, Virtual Environment

1. INTRODUCTION

Textual passwords, biometric scanning, tokens or cards (such as an ATM), and other password models are now available to users. Textual passwords, for the most part, use an encryption method. Biometric scanning serves as your natural signature, while Cards or Tokens serve as proof of your identity. However, some people despise having to carry their cards with them, and others reject to have their retinas exposed to powerful IR (Biometric scanning).[2] Nowadays, most textual passwords are kept basic, such as a phrase from the dictionary or their pet names. Klein used to do these tests and could crack 10-15 passwords everyday. With the advancement of technology, fast computers, and a plethora of Internet-based applications, this has become a child's game. As a result, 3D passwords are a more customised and intriguing method of authentication. Passwords are now predicated on the fact that humans have memory. Simple passwords are usually used so that they may be remembered easily. IJSDR (2019) [1] the human memory must go through the processes of recognition, recall, biometrics, and token-based authentication. The 3D password GUI appears once you've implemented it and logged in to a secure site. This is a second textual password that the user can type in. A 3D virtual room will appear on the screen after he completes the first authentication. Let's imagine we're talking about a virtual garage. In today's

garage, one will find a variety of tools, equipment, and other items.Each one has its own set of characteristics. After then, the user will interact with these attributes as needed. In 3D space, any object can be moved around in a (x, y, z) plane. Each object's movement attribute is this. This is a property that all things in the space share. Let's say a user checks in and goes into the garage. He finds a screwdriver and takes it up (starting position in xyz coordinates: 5, 5, 5) and transfers it 5 places to his right (in the XY plane, i.e. (10, 5, 5). This is what is known as authentication. Only a true user comprehends and identifies the thing from which he must choose. This is where human memory's Recall and Recognition functions kick in.

.

STRUCTURE OF PAPER

The paper is organized as follows: In Section 1, the introduction of the paper is provided along with the structure. In Section 2 we have the complete information about 3d password. Section 3 shares information about the working of 3d password and also the state diagram. Section 4 tells us about the methodology and the process description. Section 6 tells us about the future scope and concludes the paper with acknowledgement and references.

OBJECTIVES

When compared to existing authentication schemes, the new technique must provide more secure authentication. It is designed in such a way that it is simple to grasp and very user-friendly authentication approach, giving the user the option of selecting the sort of techniques to be used in password generation. For hackers and crackers, the new method must supply secrets that are easy to remember or memorise while also being difficult to guess. give secrets that are a mix of authentication patterns based on Recall, Recognition, Biometrics, and Tokens, or a mixture of two or more systems. Only authenticated users will be able to update or remove them under the new scheme.

2. RELATED WORK

There are numerous works that have been done related to image processing machine learning algorithms.

[8].Authentication, or the process of confirming the user, is a critical security risk. Human authentication approaches can be categorised into the following categories: 1) Textual based: Recall based techniques require the user to re-create a previously twisted secret. Identification-based methods require the user to classify and be aware of a secret or part of a secret that the user has carefully selectedpreviously[3]. 2) Graphical based: This strategy is suited those who can remember and identify films better than they can words. Some of the graphical password schemes require a significant amount of effort to implement. Furthermore, the majority of graphical password schemes are vulnerable to shoulder surfing attacks.3Token-based: In banking authentication structures, token-based systems are necessary in addition to knowledge-based authentication systems such as textual and graphic-based systems. Many instances have revealed, however, that tokens can be lost, forged, or stolen using easy means [8]. 4) Biometric based: A variety of biometric techniques have been proposed, including fingerprints, face recognition, voice recognition, retina recognition, and palm prints. However, all schemes have their own set of restrictions and downsides, which are determined by a variety of characteristics such as acceptance, distinctiveness, and consistency. One of the major disadvantages of using biometrics is that it is insensitive to a user's personal characteristics [8].

[2] A.B.Gadicha[2]To overcome the benefits and drawbacks of previously available authentication solutions. The new authentication system, which is based on previously existing techniques, is introduced. The "3 Dimensional Password" is a combination of passwords. Which is a multifactor method that combines all of the above-mentioned memory, recognition, graphical, and biometric based schemes, as well as many more. All of these strategies are used to create 3d Password in a virtual three-dimensional world. The user will interact with many virtual things in this virtual environment. A distinct 3D environment will be created for each user, and the environment will vary as the person changes. The 3D password is created by analysing the user's interaction sequences [2].

3. METHODOLOGY

Currently, research on 3D passwords suggests using a virtual environment. International global journal for engineering research (2014) [3] The main concept in this virtual environment is to create a virtual room where everything exists within the screen of a computer or laptop, similar to the environment created when we play video games. Vishal kolhe. (2013) [5] However, as technology advances, we now have access to a variety of electronic devices that can assist us in creating a 3D password system with real-time environment. As a result, the suggested system specifies that the user would have the ability to select the amountof items he wishes to use.Thencan choose the type of thing he wishes to utilise, which may be a cylindrical object, a conical object in the shape ofa cap, or a conical object in the shape of a hat., a cuboidal object, such as an eraser, any real-time object Laptops, duster, marker, and other items are all readily available.Theobjects must then be arranged in a specific order. Barthi (2016) [7] Only the user who needs to go through the process will knowauthentication using a password This set-up would be discovered. We can use a variety of sensors and devices that we have onhand. As a result,The objects can be arranged in an infinite number of ways. Sonker s k (2011) [12] The 3D Password is the best method to provide security which can be used with the combination of all possible password together. It is more efficient than other authentication, hence it is a tightly secured authentication system. Moreover, it shows how the attacker will acquire knowledge of the most possible attacks. Shoulder surfing attacks are still possible and effective against 3D password therefore a possible solution is a field of research.

Working of 3d password

The following diagram is the state diagram of 3d password.

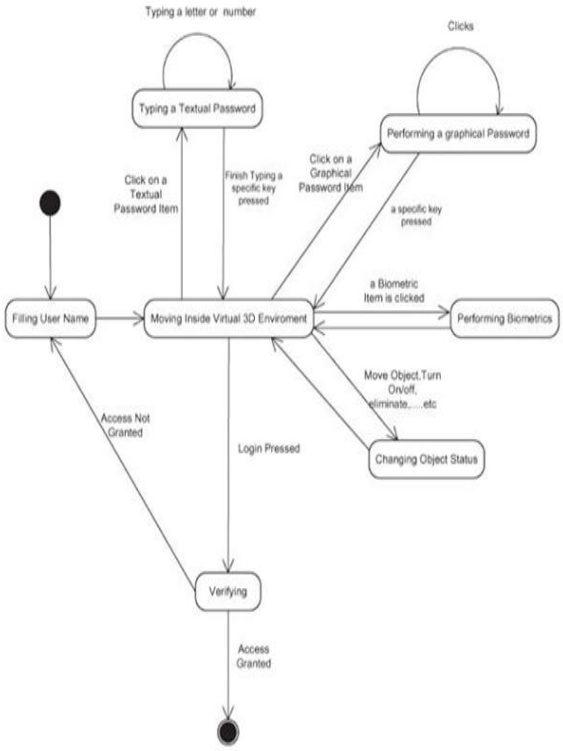

Fig.1 State Diagram of 3d password

- The architecture of the 3D virtual environment and the type of object selected within it decide the 3D password key space.
- Consider the size of a 3D virtual environment space to be G x G x G. In a three-dimensional virtual world, virtual objects are distributed with unique (x,y,z) coordinates[4].
- To give security to the email client system, we are using a three-dimensional password system. To use the mailing services, the user must first create an account. To create an account, the user must fill out personal information such as user id, name, and address, as well as a password that is a 3D password.
- After filling out the profile details, the user travels around in a three-dimensional virtual environment.
- The user will then navigate within the 3D virtual environment and interact with virtual items using any input devices available, such as a keyboard and mouse.
- The user is now in a virtual art gallery in a 3D environment. Many paintings can be found in an art gallery. In that art gallery, the user must choose from a variety of pointer photographs.

- This sequence of points, in which the user has selected or clicked on the items, will be kept in an encrypted text file. The 3 Dimensional password is produced or configured for a specific user in this manner.
- The following objects are available:
- A fingerprint reader that requires the user's fingerprint to function;
- A biometric identification system;
- A piece of paper or a whiteboard on which the user can write, sign, or draw;
- A token-requesting automated teller machine (ATM);
- A light that can be turned on and off
- A television or radio with selectable stations;
- A staple with a punch hole;
- A vehicle capable of being operated;
- A book that can be transported from one location to another is number ten.
- Any real-life object;
- Any graphical password schem

4. FUTURE SCOPE AND CONCLUSION

The most commonly used authentication methods are textual passwords and OTP-based passwords. Both, however, are vulnerable to certain types of attacks. Shoulder surfing assaults and 3D password recording attacks are still possibilities. F. A. Alsulaiman and A. El Saddik. (2008) [11] The 3-D password is a multifactor and multi-password authentication strategy that incorporates several different authentication methods. The design of a 3D virtual world, as well as the selection of things within it, is more secure, as well as easier to use and navigate. It is up to the user to select which 3D object would serve as the Password. A user who has trouble memorising long textual passwords may prefer 3-D passwords. Textual and biometric passwords are far less secure. One of the future works that will lead to system improvement is different background attacks to break the system. Another research goal is to develop a 3-D password for mobile phones.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] April 2019 IJSDR | Volume 4, Issue 4 1Mrs. Ashwini B P, 2Ms. Bhumika J, 3Ms. Chinmayee T S, 4Mr. G M Akshay Bhat, 5Mr. Naveen Kumar N 1Assistant Professor, 2,3,4,5UG Students Department of Computer Science and Engineering

[2] Multifactor Authentication using 3D Password Nirzar Bhaidkar1 Pratik Prasad2 and Aakash Kamble 3Department of Computer Engineering, St. John College of Engineering and Management Kumar, kapil & Goyal, Dr dinesh & Scholar, M.

[3] (2014). 3D Password Based Authentication System Using Multiple Layers. International Global Journal for Engineering Research. 9. 1-2014.

[4] (2008). Three Dimensional Password for More Secure Authentication. Instrumentation and Measurement, IEEE Transaction on. 57. 1929-1938.10.1109/TIM.2008.919905.

[5] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod,"Secure Authentication with 3D Password ",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume2, Issue 2, March 2013

[6] https://www.ijcsmc.com/docs/papers/May2014/V3I5201423.pdf4006.pdf

[7] 3D Password for more Secure Authentication International Journal of Research in Engineering, Science and Management Volume-2, Issue-4, April-2019https://www.ijert.org/more-secured-authentication-3d-password

[8] Bharti, "Design 3D password with session based technique for security in smart phone," International Conference On Green Engineering and Technology, 2016.

[9] Shivani A. Patil, "Improving ATM Security using 3D password," in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2015.

[10] Sahana R. Gadagar, Aditya Pawaskar, Rangeeta B. Pandhare, "3D Password Authentication for Web Security," International Conference on Recent Innovations in Engineering and Management, 2016.

[11] Ashwini A. Khatpe, Sheele T. Patil, Amruta D. More, Dipak V.Waghmare, Ajit S. Shitole, "3D Login for more Secure Authentication," International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[12] F. A. Alsulaiman and A. El Saddik, "Three-Dimensional Password for More Secure Authentication," in IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 9, pp. 1929-1938, Sept. 2008.

[13] Sonker S. K, Ghungrad. S. B, "Minimum Space and Huge Security in 3D Password Scheme," in International Journal of Computer Application, vol. 29, no. 4, September 2011.