IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

A Secured Authentication Technique-3D Password

Vrushali M. Thakur[1], Nandini N. Gaikwad[2], Pooja P. Thakur[3]
Assistant Professor, Department of Information Technology, M. P. A. S. C. College, Panvel, India[1,3]
Assistant Professor, Head, Department of Information Technology, M. P. A. S. C. College, Panvel, India[2]
Corresponding Emil ID: vrushalithakur296@gmail.com[1]

Abstract: *A user's identity ensures by the process of Authentication. Authentication is an important security service provided to the system by the different authentication algorithms. The algorithm includes Text password, Graphical password, Biometric password, Token authentication, etc. Text password mostly includes simple text like names, etc. And text passwords can be easily cracked. Biometric identifiers include fingerprints, etc. In Graphical password, the user selects images in a specific order, presented in a GUI. And tokens are smart cards like credit cards etc. But cards can be stolen, and some people don't want to carry their cards. Therefore, the secure authentication scheme introduced called 3D PASSWORD". It is a combination of all these schemes that is Recognition + Recall + Token + Biometric. 3D password is a multi-factor authentication technique that has a virtual environment that looks like a real-time environment, but it is not a real-time environment. It is more secure than other schemes of authentication.*

Keywords: Authentication, 3D Password, Algorithm

I. INTRODUCTION

There is an authentication technique that ensures that and confirms a user's identity. Providing Authentication to any system leads to providing more security to that system. For improving authentication and avoiding password hacking with management policies that are enforced by password expiration, length, and complexity requirements. Username and password systems are among the oldest forms of digital authentication. To protect any system authentication must be provided, so that only authorized persons can have the right to use or handle that system & data securely. There are many authentication algorithms are available some are effective & secure but There are some authentication techniques are as follows.

1.1 Types of Authentications

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

Figure: Types of Authentications

1. **Simple Password:** Password Protection is a security process that protects information accessible via computers that need to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.
2. **Token-Based:** A token is a piece of data created by a server and contains information to identify a particular user and token validity. The token will contain the user's information and a special token code. that code user can pass to the server with every method that supports authentication, instead of passing a username and password directly. Examples Credit Cards, ATM Cards, Master cards, etc.
3. **Biometric Authentication:** Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some internal characteristic of that user. It depends on the measurement of some unique attributes of the user. They estimate that these user characteristics are unique, that they may not be recorded and reproductions provided later, and that the sampling device is tamper-proof. Biometric samples include fingerprints, retinal scans, face recognition, voiceprints and even typing patterns.
4. **Graphical Password:** In this user need to identify, recognize password created before. Identification-based authentication can be used in the graphical password. Generally, this technique is not used much more as Recall based is used. Still, both recall-based & recognition-based authentication techniques have some drawbacks & limitations when they are used separately or used single authentication scheme at a time. But to improve the security we are introducing 3D passwords as current schemes have many of the flows. 3D password has a virtual environment that looks real. A virtual 3D password provides means to the user or programmer to combine all the permutations & combinations of an existing system into a 3D virtual environment. 3D password technique is very flexible gives users to create an infinite number of passwords possible. It is easy to remember and difficult to hack.

II. EXISTING SYSTEM

The authentication schemes we are using nowadays suffer from many weaknesses. The existing System includes techniques like text password, graphical password, and biometric, token-based authentication. As the text password is simple text it can be easily hacked with the help of brute force attacks. A graphical password has a space that is less than or equal to the textual password space. Tokens including different kinds of smart cards can be stolen. Therefore, biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Besides, biometrics cannot be revoked. Therefore, the 3D password technique has been proposed. It is a multi-factor authentication scheme. It combines multiple authentication techniques in one 3D virtual environment. It is a combination of recall, recognition, token, and biometrics. 3D password provides an extremely high degree of security to the user.

III. PROPOSED SYSTEM

The proposed 3D password is a multi-factor authentication technique that has a virtual environment containing the user interface which looks like a real-time environment, but it is not a real-time environment. This system makes use of all the positive aspects of the existing authentication systems. Users are provided the suppleness to choose between an application of 3D password by being just recall-based, recognition-based, and token-based, biometric-based. It can also combine two or more of the above types as a 3D password. Therefore, it confirms that higher acceptability by the user with such a system can mold in his way of convenience. The secure authentication technique called 3D password is a combination of all these schemes that is Recognition + Recall + Token + Biometric. This can be done by tracing a 3D virtual environment that contains objects that request information to be recollected, information to be recognized, tokens to be presented, and biometric data to be verified.

The 3D password is the sequence of interactions with the virtual objects that is

1. Pre created
2. Pre stored
3. Verified by the user.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

This kind of interaction in a 3D environment overhanging on a 2D environment is termed a pass action.

3.1 Objectives

- **Flexibility:** In 3D password technology, a 3D password provides multifactor authentication such as biometric and textual passwords can be embedded in it.
- **Strength:** It provides almost endless password possibilities.
- **Easy to Remember:** it can be kept in mind easily as a short story.
- **Privacy:** organizers have an option. The administrator can choose authentication designs that respect the user's privacy.
- Therefore, this system makes interaction with only those objects that perform the acquisition of information from the user that he is comfortable to provide. It neglects interaction with the rest of the objects that might demand the information which the user might not want to provide to the system.

We may have the following objects:

1. By computer input system the user can type;
2. The user's fingerprints can be recognized by a fingerprint reader;
3. Need a biometric recognition device;
4. Need a paper or a whiteboard that a user can write, sign, or draw on;

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

5. An automated teller machine (ATM) which requests a token;
6. A light that can be switched on/off;
7. A television or radio where channels can be selected
8. Staple that can be punched;
9. Car that can be driven;
10. A book that can be moved from one place to another;
11. Whichever graphical password scheme;
12. Whichever real-life object;
13. Whichever upcoming authentication schemes.

IV. WORKING

Consider a three-dimensional virtual atmosphere space that is of the size G x G x G. Each point in the three-dimensional atmosphere space is represented by the coordinates. (x, y, z) [1...G] x [1...G] x [1...G]. The entities are distributed in the 3-dimensional virtual atmosphere. Every entity has its x, y, and z coordinates. Assume the user can navigate and walk through the 3-dimensional virtual atmosphere and can see the entities and interact with the entities. The input device for interactions with entities may be a mouse, a keyboard, stylus, a card reader, a microphone...etc.

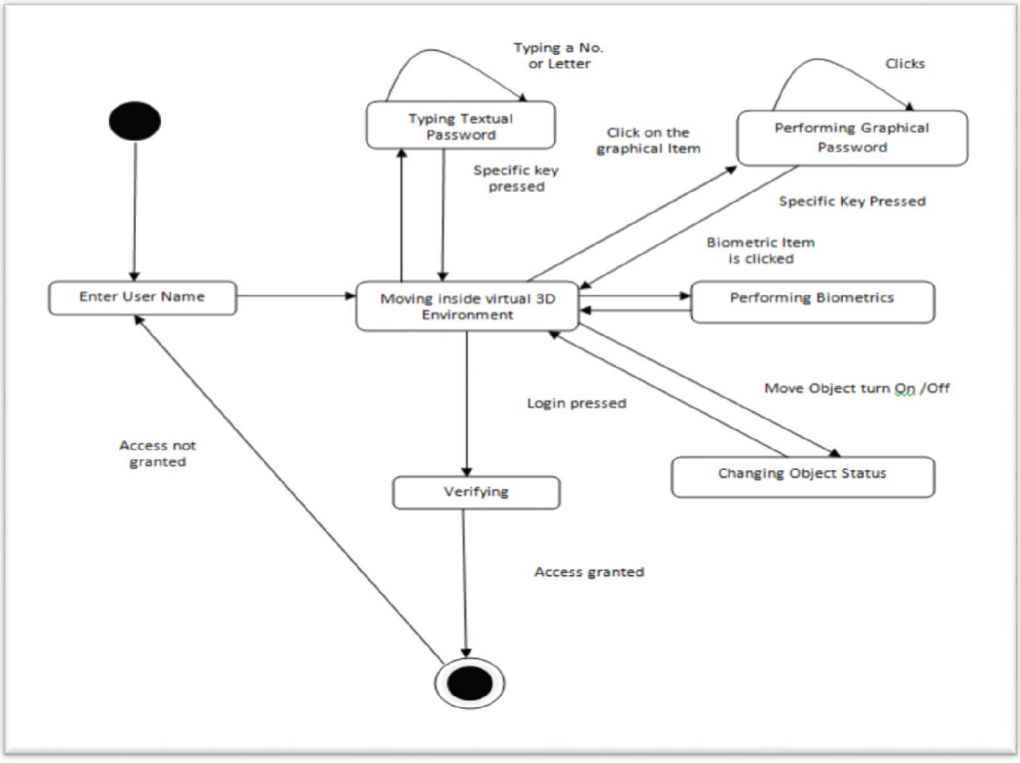
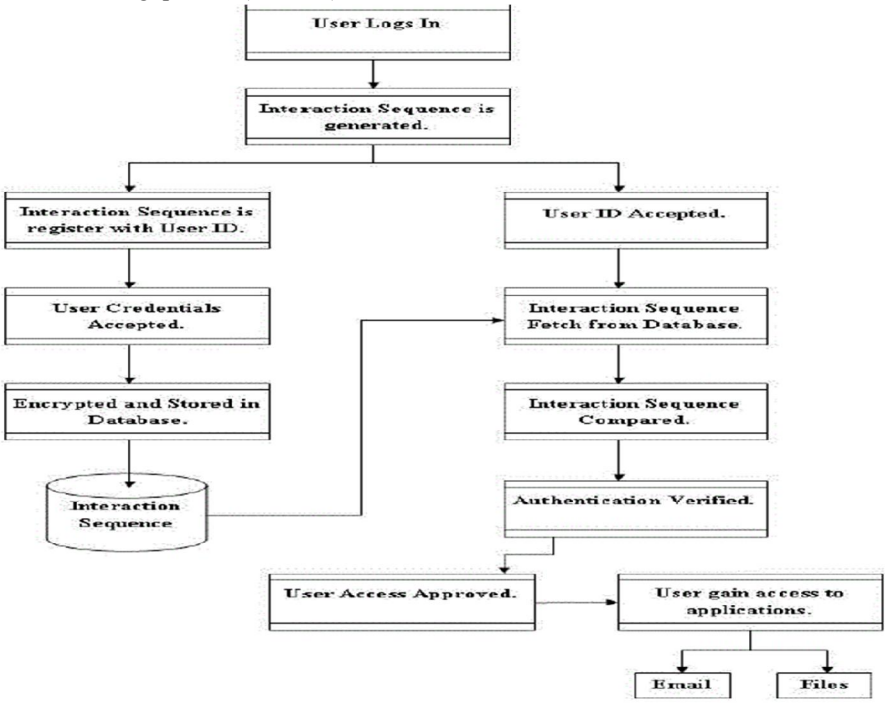


Figure: State diagram of 3D password

For example, consider a user who navigates through the three-dimensional virtual atmosphere that consists of a temple area. Let us assume that the user is in the virtual area and the user turns around to the bell placed in (9,16, 80) and rings it. Then the user touches God's feet. The user types 'KRISHNA' into a computer that be in the position of (10, 5, 25). The user then walks over and turns off the light placed in (15, 6, 20), and then goes to a whiteboard placed in (55, 3, 30) and draws just one dot in the (x, y) coordinate into the whiteboard at the point of (420,170). The user will press the login button. The initial representation of user actions in the 3D virtual atmosphere can be recorded as follows:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

(9, 16, 80) Action = Ring the Bell;
(9, 16, 80) Action = touch God feet;
(10, 5, 25) Action = Typing, 'K';
(10, 5, 25) Action = Typing, 'R';
(10, 5, 25) Action = Typing, 'I';
(10, 5, 25) Action = Typing, 'S';
(10, 5, 25) Action = Typing, 'H';
(10, 5, 25) Action = Typing, 'N';
(10, 5, 25) Action = Typing. 'A';
(15, 6, 20) Action = Turn Off the Light;
(55, 3, 30) Action = Drawing, point = (420,170);



4.1 Security Analysis

It is necessary to consider all possible attack methods to realize and understand how far an authentication scheme is secure. It is important to understand if the authentication scheme proposed is immune to such attacks or not. Besides, if the proposed authentication scheme is not immune, we then have to find the countermeasures that prevent such attacks. The countermeasures to such attacks are detailed in this section.

1. Brute Force Attack
2. Well-Studied Attack
3. Shoulder Surfing Attack
4. Timing Attack

4.2 Advantages

1. This 3D password Provides security.
2. It can't take by any other person.
3. 3D graphical password has no limit.
4. It may Change the Password easily.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, March 2022
Impact Factor: 6.252

5. The system can implement easily.
6. Password can keep in mind easily.
7. This password helps to keep a lot of personal details.

4.3 Disadvantages

1. 3D password Difficult for blind people to use this technology.
2. It Requires sophisticated computer technology.
3. It is Expensive.
4. Lots of program coding is required.

VI. FUTURE SCOPE

As the 3D password scheme uses a combination of Recognition + Recall + Token + Biometric, it mainly focuses on critical systems and resources. Critical Systems such as military facilities, critical servers, and highly classified areas can be protected by a 3D password system with large three-dimensional virtual atmospheres. Moreover, airplanes and jet fighters, ATM and operating system logins can also make use of 3D passwords to provide more secure authentication.

V. CONCLUSION

The 3D password is a multi-factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment. The design of the 3D virtual environment is the selection of objects inside the environment and the object's type reflects the resulted password space. Its password space is very large compared to any existing authentication scheme. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Its design is simple and easy to use 3D virtual environment is a factor that leads to higher user acceptability of the 3D password system.

REFERENCES

[1]. Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.
[2]. https://www.uniassignment.com/cassy -samples/information technology/secured authentication 3d-password-information technology essay.php
[3]. https://www.slideshare.net/mobile/Gowsayasn/3d-password.ppt
[4]. www.seminarsonly.com/Labels/3D password- technology.php