International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Security using 3D Password

Sourabh Kadam[1], Shubham Shinde[2]

[1]*Student, Department of Master of Computer Application, Finolex Academy of Management and Technology, Maharashtra, India*
[2]*Student, Department of Master of Computer Application, Finolex Academy of Management and Technology, Maharashtra, India*

Abstract - *Authentication of any system means providing security to that system. There are several authentication techniques like textual, biometric, etc. This technique has some limitations and drawbacks.*

To overcome them 3D-Password was introduced. In a 3D password, a virtual environment is present in which the user creates his unique password by interacting with objects in the 3D environment. It is a more secure technique as compared to other authentication techniques because it is very difficult for a hacker to break a 3D password.

Key Words: 3D-Password, Security, Authentication

1. INTRODUCTION

1.1 Authentication Techniques

There are four authentication techniques available:

1.1.1 Knowledge Based: A conventional method of Textual password is most commonly used for authentication.

1.1.2 Token Based: Bank systems and companies use smart cards for validating client or employee.

1.1.3 Recognition Based: A Graphical password or face identification is recognition based technique.

1.1.4 Biometric Based: Using a retina scanner or finger scanner is the best example of biometric authentication.

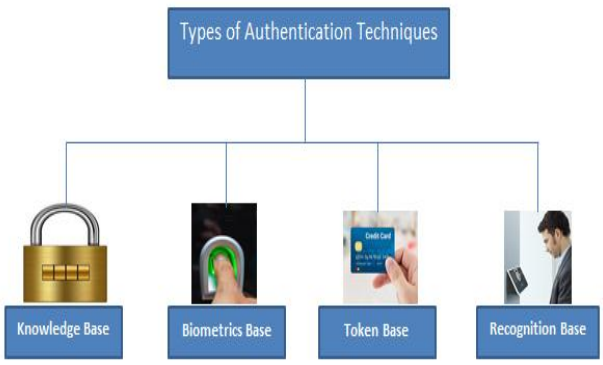

Fig -1: Techniques of Authentication

1.2 Authentication System

The authentication system works on two main schemes:

1.2.1 Recall Based:

In today's world security is a major concern part A Textual password is mostly used by many peoples which is a recall-based technique. It is very hard to remember a textual password and it can be guessed easily hence it is a less secure authentication technique.

1.2.2 Recognition Based:

In this authentication system, a user is recognized by his/her password that is created by him/her like a graphical password but the Problem with the graphical password is that it may be tracked. Another type of authentication is Biometric Authentication which includes several techniques such as fingerprint scan, palm scan, face recognition, voice recognition, and retina scan. In biometric authentication, there is a possibility of a reply attack. In token-based authentication, there is a chance of fraud or theft.

2. 3D Password

2.1 What is a 3D Password?

A 3D password is a combination of a recall-based and recognition based authentication system. 3D password is a combination of multi-factor and multi password authentication scheme.

In this user has to first provide a textual password it means user name and password. Once this step is authenticated then in the next step user enters a 3D virtual environment where a user creates a password by using various objects in 3d environments like switch on/off the button of TV or opening door. The sequence in which the user clicks on the object is recorded in an encrypted format. In this way, the password is generated for a particular user, next time when the user enters the correct sequence he generated before then he is allowed to enter in the system.

In simple terms, the 3D password is nothing but a series of sequential steps executed by the User in a virtual 3D environment. The above Figure 2 represents the state diagram for 3D password authentication. It has given a large number of virtual objects which makes more password combination and it is difficult for an attacker to guess the 3D password.

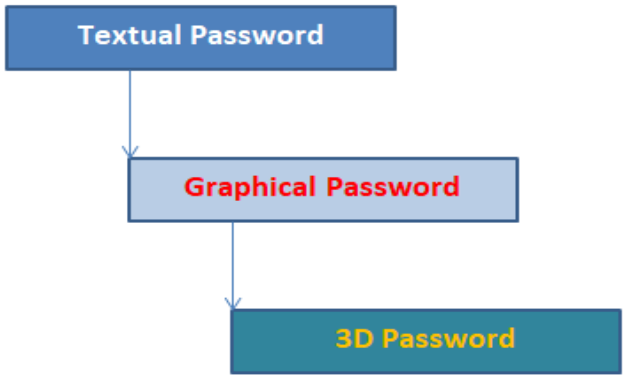

Fig -2: 3D Password Steps

.

The User enters in the virtual environment and the multifactor authentication process starts. It follows these guidelines

- Similar to Real Time System
- 3 dimension and virtual Environment
- Virtual Object Interaction

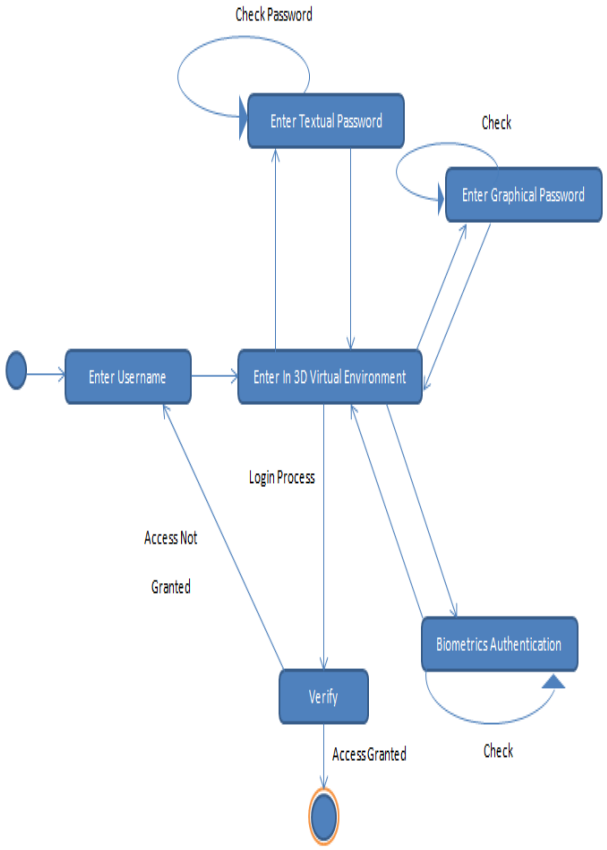

Fig -3: Cycle of 3D Password

2.2 Working Scheme of 3D Password

Consider a 3D virtual environment that is represented by the coordinates (x, y, z). The objects are distributed in a virtual environment where each object has its coordinates (x,y,z). Assume that users can navigate through a 3D virtual environment and can see the objects and interact with them. The input devices for interaction can be used as a keyboard, a mouse, a microphone, etc.

For example, consider a user who navigates through a 3D virtual environment that consists of a ground and house. Consider that in virtual ground user turns around and goes to the door located at (1, 2, 3) and opens it. The user types "SKY" into a computer that exists at position (4, 5, 10). After that user turn off the light located at (10, 12, 10) then closes the door, and then presses the login button.

The representation of these actions of user can be recorded as below:

(1, 2, 3) Action = Open the house door;

(4, 5, 10) Action = Typing, "S";

(4, 5, 10) Action = Typing, "K";

(4, 5, 10) Action = Typing, "Y";

(10, 12, 10) Action = Turning the light off;

(1, 2, 3) Action = Close the house door;

2.3 Mathematical Concepts in 3D Password

For 3D password implementation, some mathematical concepts are required.

2.3.1 Time Complexity:

Time Complexity = Am + Bn

In the above equation "m" indicates the time required to communicate with the system and "n" is the time required to process each algorithm in that 3D environment.

2.3.2 Space Complexity:

In a 3D password, it stores 3 dimensions in the database namely x, y, z as the 3D environment is represented by these 3 axes.

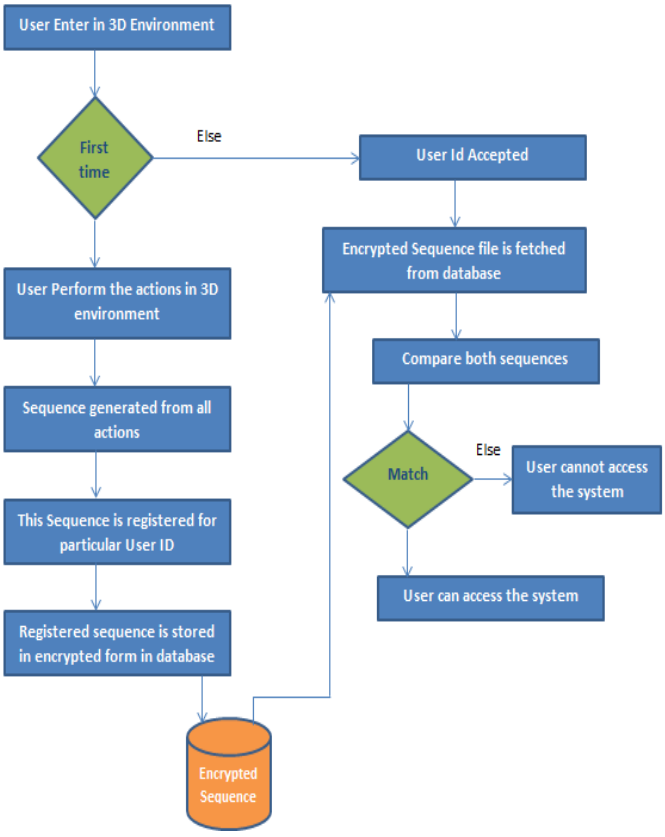

Fig -4: Flow of 3D Password working scheme

2.4 Attacks and Countermeasures

To realize and understand how far an authentication system is secure, we have to consider all possible attack methods. We have to provide a proper immune authentication system if the system is not strong enough to protect users privacy, then we have to find countermeasures that prevent attacks they are as given below

2.4.1 Brute Force Attack

The attacker has to try all possible a 3D passwords which are very difficult for the following reasons:

2.4.1.1 The time required for a legitimate user to login varies depending on the interactions and actions of the user in 3D environment. Therefore, a brute force attack is very difficult.

2.4.1.2 The 3D environment contains all biometric and token based recognition. The attacker has to find all possible biometric information and tokens which is very difficult and required high cost.

2.4.2 Shoulder Suffering Attack

An attacker may use a camera to record user activity in a 3D environment. In this case, the attacker may see the pattern of actions but he can't see information like textual password or biometric data from behind.

2.4.3 Timing Attack

In this attack, the attacker checks how much time is required for the user to perform the 3D password. Due to this attacker get a length of 3D password but it the attacker mere hints.

3. Applications of 3D Password

A 3D password requires more password space as compared to another so the main target of a 3D password is to protect critical systems and resources some possible critical applications are as follows.

3.1 Timing Attack

Many big organizations have critical servers that are protected by a textual password. In this scenario, a 3D password is a good replacement for a textual password.

3.1 Nuclear and Military facilities

Such systems should be protected on a high priority basis. The 3D password is most reliable as it requires a large password space. It can also contain biometric, recognition, and token-based authentications in a single system.

3.3 Airplanes and Jet fighters

Due to some political agendas or anything else such a system may be used to harm people. These systems can be protected by using a 3D password.

4. Advantages of 3D Password

4.1 Provides high-level security to the system which contains more important data by providing multi factors and multiple techniques for authentication.

4.2 It provides the user to choose the type of authentication system he wants as there are several options available in the 3D environment.

4.3 It eliminates the brute force attack as all data and critical information is stored in an encrypted format and 3D password in a combination of multiple systems hence it is difficult for an attacker to invade the security.

4.4 Security against software like key logger as this software can store all the text passing through your keyboard but 3D password also uses a graphical password for authentication.

5. Disadvantages of 3D Password

5.1 Shoulder attack in which the attacker observes the user from the back shoulder and then easily breaks the authentication.

5.2 In a 3D password there is **more complexity in coding.**

5.2 3D password is **more expensive** as compared to other authentication systems.

5.3 More space required to store a 3D password in the database.

6. CONCLUSIONS

3D Password mechanism is more secure and reliable as compared to other authentication systems. By using 3d Password we can make any system more secure and it will be beneficial for applications used in the corporate world, government sector, and personal use.

REFERENCES

[1] https://www.youtube.com/watch?v=7sP7TawXAUg
[2] https://www.slideshare.net/manisha0902/3d-password-ppt-43870131
[3] http://research.ijcaonline.org/icacact/number1/icacact1002.pdf
[4] http://research.ijcaonline.org/volume120/number7/pxc3904024.pdf
[5] 3D Password: A Novel Approach for More Secure Authentication. http://www.ijcset.com/docs/IJCSET14-0502-080.pdf
[6] http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_16.pdf
[7] Kumar, Devender & Singh, Vikram. (2017). Enhanced Multifactor Authentication Scheme. International Journal of Engineering Trends and Technology. 52. 109-114. 10.14445/22315381/IJETT-V52P217.