Security using 3D Password

Dhatri Raval
Lecturer
CMPICA
CHARUSAT, Changa

Abhilash Shukla
Assistant Professor
CMPICA
CHARUSAT, Changa

ABSTRACT

Authentication of any system means providing a security to that system. There are number of authentication techniques like textual, biometrics etc. This type of textual password commonly follows an encryption algorithm to provide security. Each of these techniques has some limitations and drawbacks.

To overcome the drawbacks, a new authenticate technique is now available. This new authentication technique, known as 3D Password, is multi-factor and multi-factor authentication technique. The most important part of 3D Password is virtual environment containing the user interface which looks like a real time environment, but is not actually a real time environment [3]. 3D password is more secure technique of authentication in comparison to other techniques because it is difficult to break and simple to use [1].

The advantage of the 3D password is that combine the authentication of existing system and providing high security to user.[2]. This paper focuses on how to create 3D password and the design principles for 3D password.

General Terms
Security, Authentication

Keywords
3D Password, Virtual Environment

1. INTRODUCTION

There are four authentication techniques available:

a) Knowledge Base: Textual password is best example for knowledge base technique.

b) Token Base: Any ATM cards, swipe card are example of token base authentication technique .

c) Recognition Base: Any Graphical password or face identification is example of recognition base technique.

d) Biometrics Base: Thumb or finger impression is example of biometrics base authentication technique.

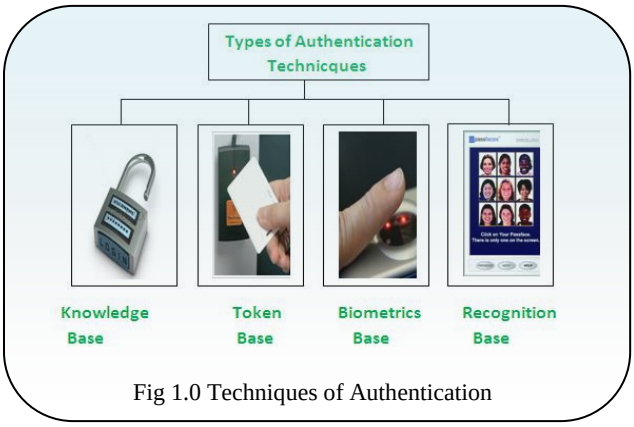

Fig 1.0 Techniques of Authentication

Basically all authentication techniques are working on two types of scheme.

a) Recall Base: now a day's security of system is major issue .Textual is example of recall based Scheme. To secure system the user provides a password to system. Strong Textual Password can secure a system at certain level. But it is difficult to memorize.

b) Recognition Base: In Recognition base scheme user is required to identify and recognize his/her password which was created by him/her. [3] Problem with graphical password is shoulder surfing attack. Biometrics base authentication technique is also part of recognition scheme. Biometrics authentication includes fingerprint, palm prints, face recognition, voice recognition, retina recantation etc. In biometrics technique record or replay attack as well as hill climbing attack is also possible. In Token base authentication there is possibility of fraud, loss, and theft.

2. 3D PASSWORD

2.1 What is 3d Password?

3D password is combination of recall based scheme and recognition based scheme. 3D Password is multi factor & multi- password authentication scheme.

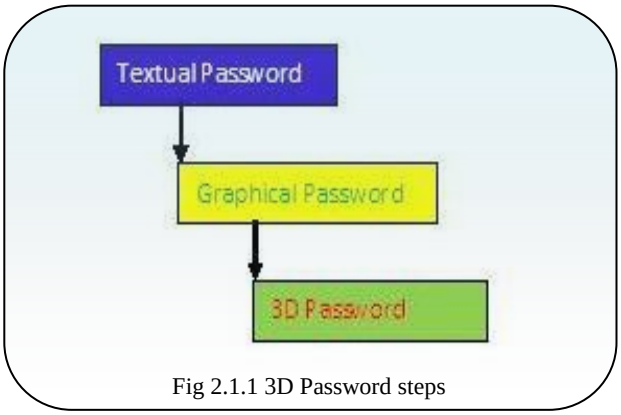

Fig 2.1.1 3D Password steps

Figure 2.1.1 shows 3D password is combination of multifactor password. 3D password provides a virtual environment for containing various virtual objects. Through this virtual environment, the user interacts with virtual object.

In simple terms, the 3D password is a series of sequential steps executed by the User in virtual 3D environment. Figure 2.1.2 represents the state diagram for 3D password authentication.

The user enters in to virtual environment and multi factor authentication process starts. It follows these guidelines.

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

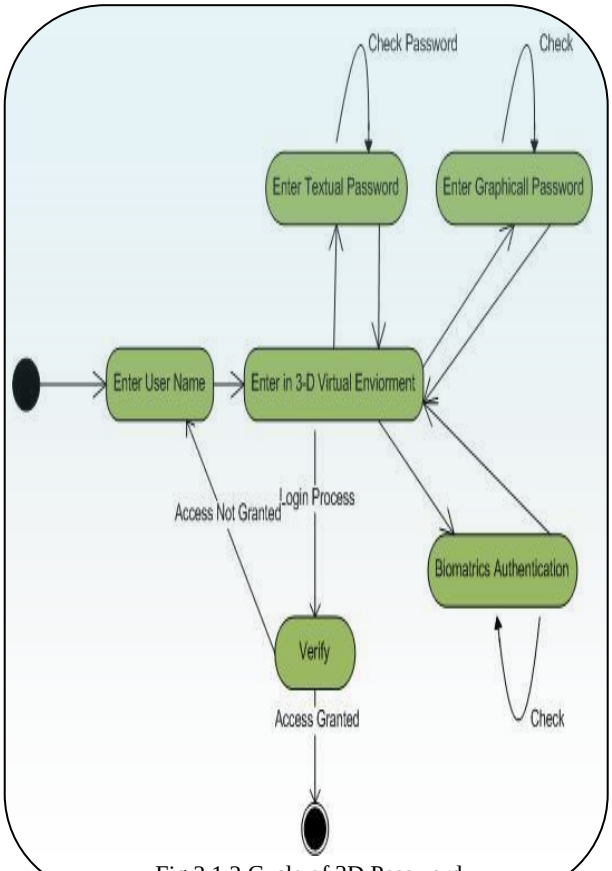

Fig 2.1.2 Cycle of 3D Password

2.2 Working scheme of 3D Password

In 3D Password user first enters with the simple textual password; if the username and password authentication is successful the user enters in to 3D environment. This password stored in simple text file in encrypted form of coordinates (x, y, z). Once user enters into 3D environment each action sequence is maintained in text file in encrypted form. For example selection of any point or object, opening door and etc activities in art gallery. Using this technique password is set for individual user. Convex hull and quick hull algorithm are used to store password.

When next time user enters in 3d environment he has to perform the same actions which are set then only he can enter into the system successfully.

3D password is a one of the authentication technique. It is implemented in 3D virtual environment. For that some mathematical concepts are required.

1) Time Complexity

Time complexity = Am + Bn

Here m is indicating time required to communicate with system, & n is time required to process each algorithm in 3D environment [4].

2) Space Complexity

In 3D password it stores 3 dimensions in database coordinate x, y, and z. Because in virtual environment it consider in dimension x,y,z.

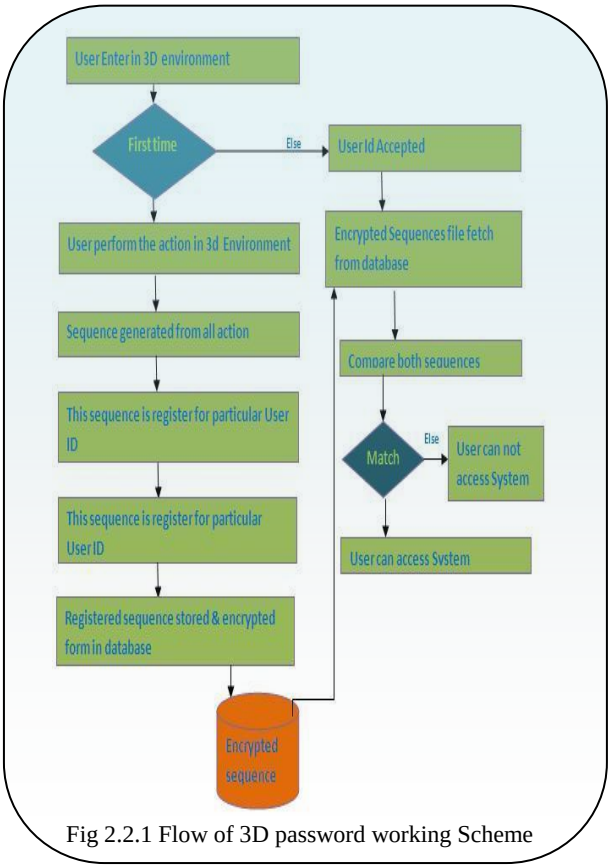

Fig 2.2.1 Flow of 3D password working Scheme

2.3 Advantages of 3D password

Compare to text & graphical password 3D password is more secure.

1. It provides user options to choose the type of authentication of his/her own choice.
    - •There are number of options available for users to choose sequence of own choice.
    - •In 3D password user can build a sequence which is easier for him to remember.
2. It eliminates a brute force attack.
    - •All data and critical information like passwords are stored in encrypted manner so it's difficult for brute force attack to crack it.
    - •In 3D password combination of recognition and recall base are using so it is difficult.
3. Provides high level security to the system which contains more important data.
    - •Its provide hide securities to data using multi factors and multiple technique to protect data.
4. Secure against a software like key logger.
    - •Software like key logger installed in a system it's difficult to secure your data these types software's are stored all text which are pass through the keyboard. In 3D password graphical password is also use for authentication.

2.4 Disadvantages of 3D password

1. Shoulder attack.
    - •Attackers observe the user from back shoulder than easily break their authentication.
2. More Time and memory.
    - •To use 3D password its require more time and memory chunk because 3D password need more space to store in database.
3. It's Expensive.
    - •3D Password is more expensive compare to other authentication technique.
4. Complexity.
    - •3D password is more complexity in coding.

3. CONCLUSION

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

4. REFERENCES

[1] http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_16.pdf

[2] 3D Password: Minimal Utilization of Space and Vast Security Coupled with Biometrics for Secure Authentication. http://www.ijater.com/Files/b8d368df-fb71-4b45-95c5-0a7a4b266a1c_IJATER_05_15.pdf

[3] 3D Password: A Novel Approach for More Secure Authentication. ttp://www.ijcset.com/docs/IJCSET14-05-02-080.pdf

[4] Alsulaiman, F.A.; El Saddik, A., "Three -for Secure" IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929 - 1938.Sept. 2008.