

Virtuoso Infotech Pvt. Ltd.



3D Password



What is a 3D Password

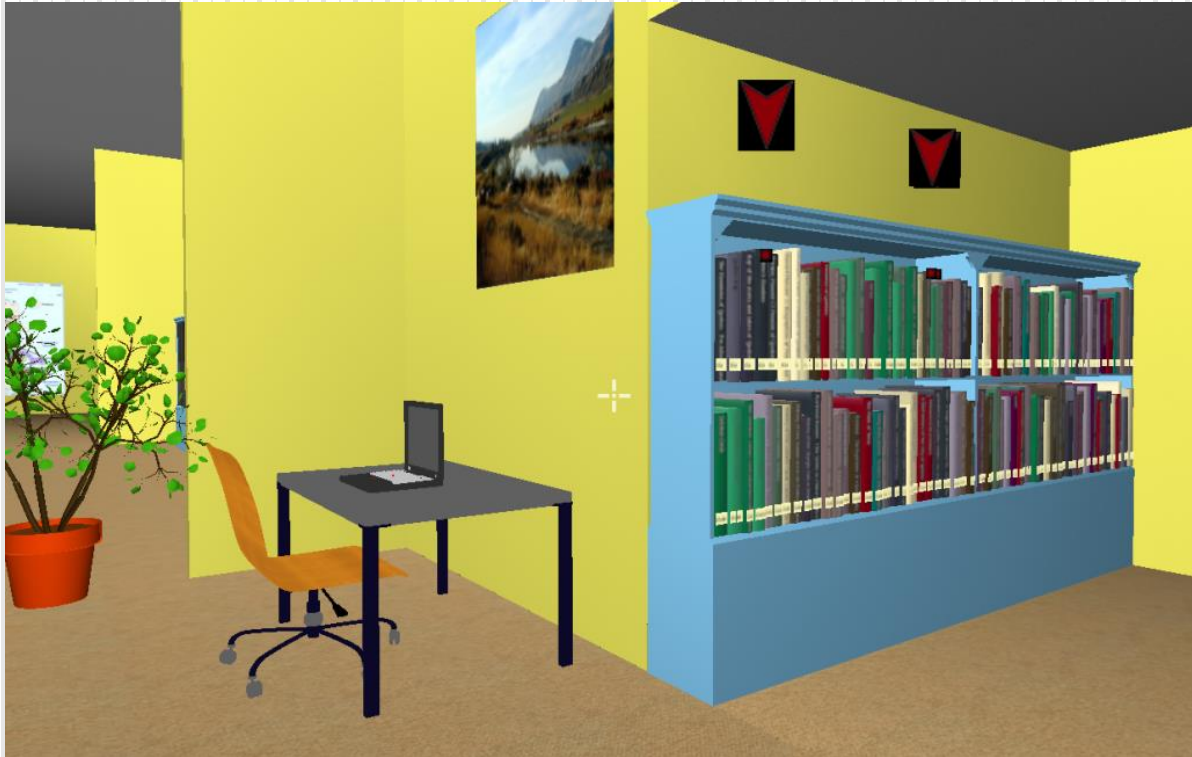
- A multi-factor authentication scheme. (KNOWLEDGE BASE + TOKEN BASE + BIOMETRICS)
- The user login by navigating through a 3D environment.
- The collected user actions and interactions in the 3D virtual environment construct the 3D password.

Virtual Environment

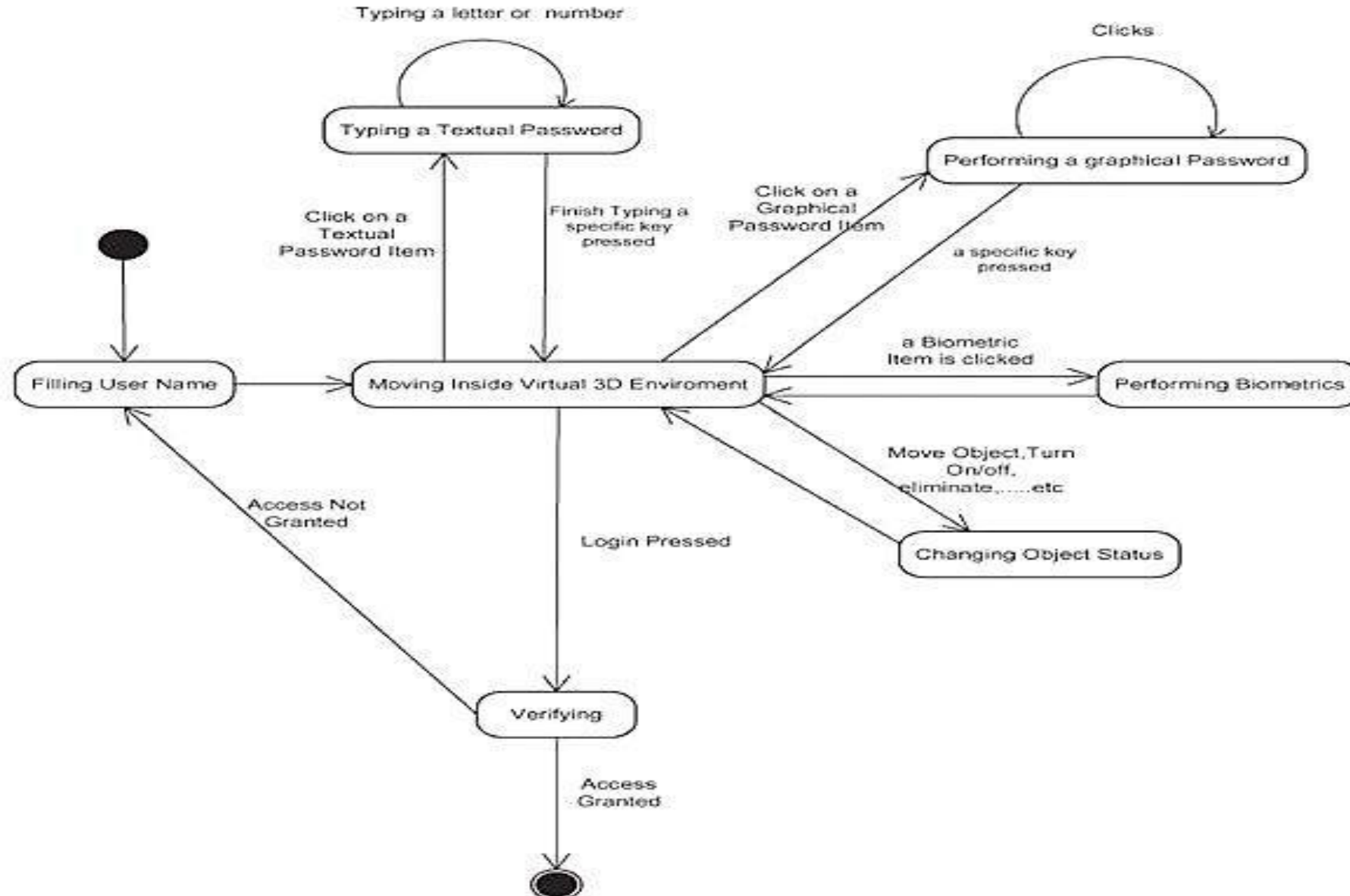
- A Computer based simulated environment.
- The environment consist of many objects and items.
- The collected user actions and interactions in the 3D virtual environment construct the 3D password.
- The user interaction with the objects creates the user's 3D Password.



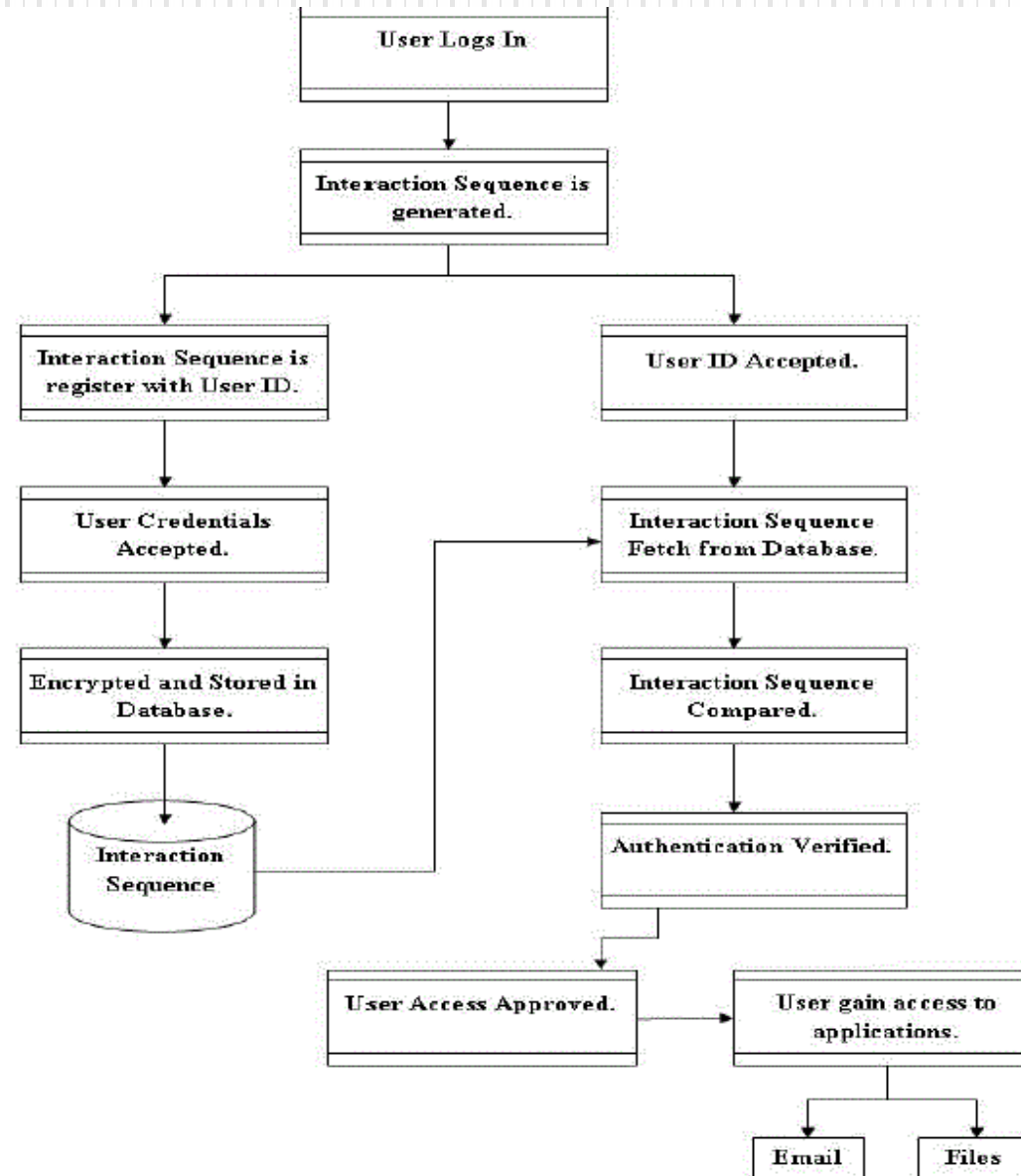
Virtual Objects



Architecture of 3D Password



Working of 3D Password



- Consider an example, the user can enter into virtual environment and type something on a computer that exists in “(x1, y1, z1)” position, then go to a room that has a fingerprint recognition device that exists in position say “(x2, y2, z2)” and provide his/her fingerprint. Then, the user can visit the virtual garage, open the car door and turn on specific channel in the radio.
- The sequence and combination of the previous actions towards the specific objects constructs the users 3 Dimensional password. Any object can be a virtual object that we encounter in our day to day life.

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

1) Time Complexity:

Time complexity = $A_m + B_n$ Here m is indicating time required to communicate with the system and n is the time required to process each algorithm in 3D virtual environment.

2) Space Complexity:

A 3D password is stored in the database as co-ordinates x , y and z . Because in a virtual environment it is considered in 3 dimensions as x , y and z .

Attacks and Counter Measures

- Brute Force Attacks.
- Well Studied Attacks.
- Shoulder Surfing Attacks.
- Timing Attacks.
- Key Logger Attacks.

Advantages

- Provides high security.
- Flexible, as it provides multifactor authentication.
- Provides infinite number of password possibilities.
- Can be memorized as a form of short stories.
- Easy to implement.
- Easy to change password anytime.
- Easy to implement.

Disadvantages

- Difficult for blind people to use the system.
- A lot of program coding is required.
- Expensive.
- Time and Memory requirement is large.

Applications

- Critical Servers.
- Nuclear reactors and military facilities.
- Airplanes, jet fighters and missile guiding.
- Networking.
- A small virtual environment can be used in
 - a. ATM
 - b. Personal Devices.
 - c. Web Authentication.
 - d. Security Analysis.

Conclusion

- The authentication can be improved with 3D password, because the unauthorized person may not interact with same object as the legitimate user.
- It is difficult to crack because it has no fixed number of steps and a particular procedure.
- Added with biometric and token verification this scheme becomes almost unbreakable.

Password Facts

- Nearly 30% of the users reuse the same password on multiple accounts.
- There is a 50% chance that a password contains at least one vowel
- People are 3 times more likely to use their pet's name as password rather than that of a family member
- Saving passwords in the web browser isn't a very smart move as the browser stores this sensitive information locally on your device in plain text. There is no master password involved, as is the case with password managers. So, if someone has physical access to your device, the person can easily have a quick look at all your passwords.
- First Thursday of month of May is World Password Day

Thank You!

Virtuoso InfoTech Pvt. Ltd.
4th Floor, Victory Landmark, Opp. D-
Mart, Behind Dominos Pizza,
Baner, Pune.

+91 80870 81318
support@virtuosoitech.com



www.virtuosoitech.com

