Security Authentication using 3D Password

Sunny Kumar
PG Student,
Department of Master of Computer Applications,
RV College of Engineering, Bengaluru, India.

Abstract

The number of digital users around the world is increasing day by day. For uniqueness and privacy, authentication is required. Providing authentication means providing security to the system from unauthorized and illegal access. The most common authentication technique is textual-based authentication where the user has unique identification and password. Users generally use passwords taken from the dictionary which are vulnerable and easier to crack. Other available authentication techniques are biometrics, smart cards, etc. Each of them is having its own drawbacks and limitations.

3D password is introduced to solve these problems. It is a multi-factor authentication technique that can combine all the available authentication techniques into a single 3D virtual environment. The virtual environment contains various real-life objects. The user has to interact with those virtual objects and the password is generated with the help of the sequence of the interactions. It is easier for the user to remember the sequence and it will be unique as different users' sequences of interaction will be different based on their interest.

Keywords: Authentication, 3D password, biometric, Virtual environment

Introduction

Authentication is the most basic and important service provided to various systems to provide security using various authentication schemes. A system should only be used the authorized users to protect the system. There are many authentication schemes available to provide security to the systems. There are basically two types of authentication schemes available. They are: Recall Based, Recognition based.

- **Recall Based:** Recall Based authentication technique is a technique where a user has to remember the credentials that he/she has created earlier during the registration or signup. It includes knowledge-based technique is the part of it. For example: Textual Passwords, graphical passwords etc. Textual passwords are the most used authentication technique worldwide.
- **Recognition Based:** Recognition based authentication technique is a technique where a user recognizes the password created before. It includes various authentication schemes such as: iris recognition, face recognition, finger prints etc.

There are various authentication schemes available but still they have drawbacks if they are used separately. Some of the drawbacks of them are: in case of textual passwords, users generally use similar kind of texts

like name, date of birth, or simple dictionary words. These passwords can be cracked easily using Brute force attack, where hacker or unauthorized personnel tries to crack the password using various dictionary words.

To overcome these issues a new authentication scheme is introduced called "3D Password" which is the combination of previously existing authentication techniques. 3D password is an authentication scheme which includes various combinations already available authentication schemes. This makes it multifactor authentication scheme. These already available authentication schemes are combined in a 3D virtual environment to create 3D password. The virtual environment contains various real time objects. The user interacts with the objects present in the virtual environment and according to the interaction patterns the 3D password is generated. As different user's behavior will be different and so that the interacting pattern differs. Therefore, different user's will be having different passwords and it has very few chances to be same.

Literature Review

Dhatri Raval, in her paper explains about the various already available password authentication schemes such as knowledge based, token based, recognition based, biometrics based.[1]

Parul, Neetu Verma, in their paper discuss about the drawbacks of the already available authentication schemes. They explained that people use textual passwords which are easy to remember and they can be cracked easily using Brute force attacks. [2]

Nayana S, Dr. Niranjanamurthy, Dr. Dharmendra Chahar, in their paper explains about the advantages and disadvantages of the 3D password. They explained that the 3D password is better than the other existing authentication systems but on the other hand it is expensive.[3]

Tejal M. Kognule, Monica G. Gole, Priyanka T. Dabade, Sagar B. Gawade, in their paper explains about the objects inside the 3D virtual environment. They found that the objects must be clearly visible and identical to each other. [4]

Mrs Ashwini B P, Ms Bhumika J, Ms Chinmayee T S, Mr. G M Akshay Bhat, Mr Naveen Kumar N, in their paper explain about the goals of the 3D password scheme. They explained that the 3D password must be the combination of both recall-based and recognition-based authentication techniques and these are not easy as to write on paper as they are coordinates. [5]

Ganesh Jairam Rajguru, in his paper he focuses on how the 3D password can be generated. And how they can be represented on a 2D screen.[6]

Parag Vade, Vaidehi Rahangdale, Saurabh Veer, in their paper focuses on the mathematical concepts related to 3D password scheme. They discuss on the time complexity, space complexity and the class problem related to the 3D password. [7]

Sahana R. Gadagkar, Aditya Pawaskar, Mrs Ranjeeta B. Pandhare, in their paper discuss about the design of the 3D environment. They also discussed about the length of the 3D password based on the design of the system. [8]

Anagha Kelkar, Komal Mukadam, in their paper discussed about the devices required to develop the 3 D password authentication systems. They mostly focussed on the input devices through which the user interacts the 3 D environment. [9]

P.K. Dhanya, M. Keerthiga, S Dinakar, in their paper discussed on the various attacks that are being done on the already available authentication schemes. They explained about Brute force attack, timing attacks, well studied attacks etc. [10]

There are many authentication schemes already available. They are knowledge based (textual password), token based (ATMs, credit cards), biometric based (thumb impression, iris recognition), graphical passwords, face recognitions. These all authentication schemes are used implemented separately on various systems for the security purposes. There are various attacks through which these authentication schemes can be broken which can lead to huge loss of information or data.

3D password is the combination of recall-based and recognition-based authentication systems. By having the combination of various authentication schemes, it becomes multi-factor and multi-password authentication schemes. 3D password's main component is 3D virtual environment. The 3D virtual environment is interactive and contain various real-life objects through which the user interacts. The 3D password is generated by noticing the sequence of the interactions and then stored in encrypted form.

Proposed System

3D password is the combination of both the authentication schemes together. This scheme combines both recall-based (for example: textual passwords) and recognition-based (for example: graphical passwords). This is how it becomes multi password and multi factor authentication scheme [Fig 1.1].

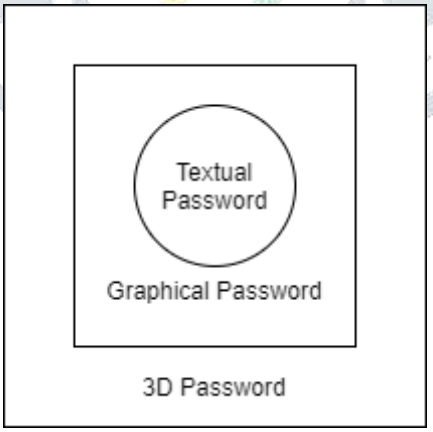

Fig 1.1: 3D Password as multi-factor and multi-password authentication scheme

3D password introduces a new virtual environment called 3D virtual environment. In this virtual environment the user navigates and thus the password is generated by noticing the navigation sequence of the users. Here biometric authentication schemes are not used mostly. Biometrics includes higher costs than other authentication schemes and is efficient for the shoulder surfing attacks. In other attacks biometrics are more vulnerable than other techniques.

In 3D password scheme the combination of various authentication schemes depends on the interest of the user. The user has choice to select the combination and the authentication scheme is developed on that choice.

Fig 1.2: Snapshot of Art Gallery

Fig 1.2 shows the snapshot of a 3D virtual environment. The virtual environment can be created based on any real-time environment like office, gallery etc. The 3D virtual environment are made interactive so the user can interact with the objects in the virtual environment and create his/her 3D password.

Architectural Diagram

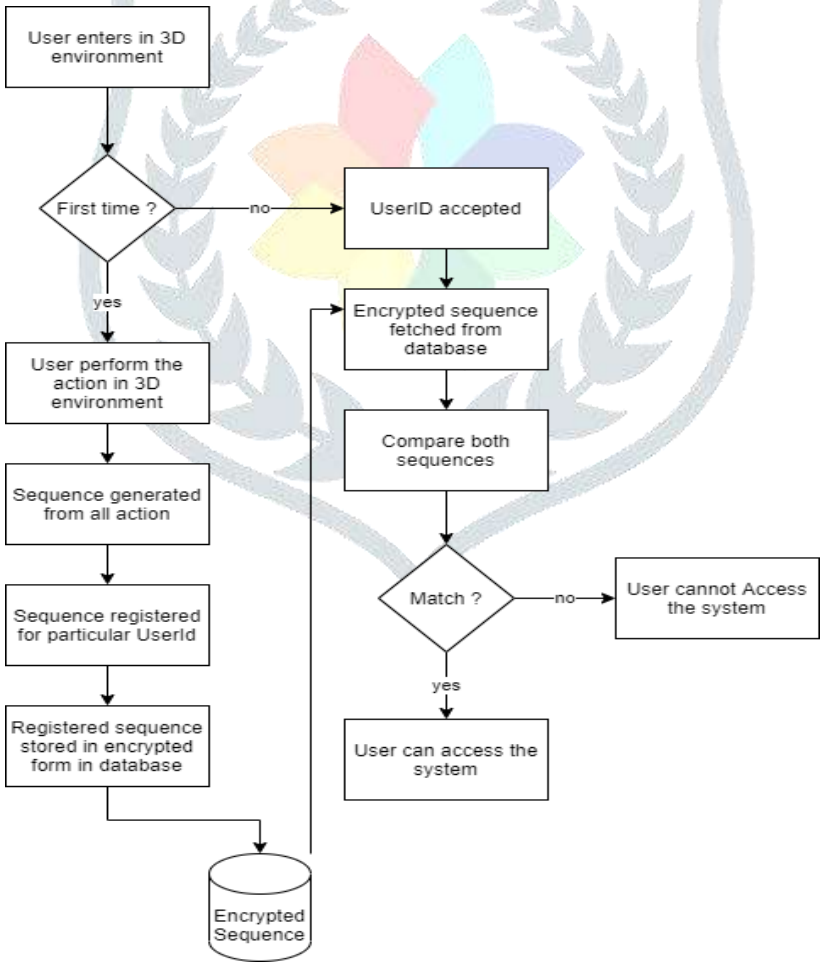

Fig 1.3: Architecture Diagram of 3D password

Figure 1.3 shows the architecture diagram of the 3D password. At the very first time the user enters into the virtual environment by providing the user details (Example: user_id). The system verifies the userId. If the userId is not registered which means the user is new and he/she has to create the 3D password. The user

will have to interact with the virtual objects inside the interactive 3D virtual environment. The sequence of the interactions is noted and then stored inside the database in encrypted format. If the user is already registered, the sequence of the user and the stored sequence will be matched with respect to the userId. If match successful, the user can access the system, otherwise not.

3D Virtual Environment

3D virtual environment is the basic building block of the 3D password authentication system. 3D virtual environment contains various real-life objects and will be presented inside a 2D screen. The environment can be developed containing any kind of virtual objects depending on the interest and demand of the users.

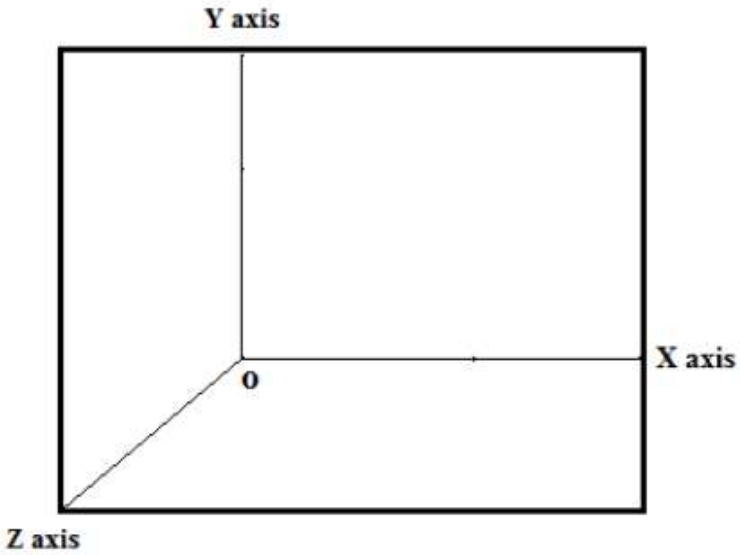

Fig 3.1: 3D environment in 2D screen

In this 3D virtual environment, for selecting the sequence of objects covex-hull algorithm can be used. It helps in storing the sequences in the 3 coordinates in the simple text file. The virtual environment must have uniquely and identifiable objects.

3D password authentication system can be implemented by 3D virtual environment. 3D password scheme can have mathematical problems. Some of them are:

- **Time Complexity:** Time complexity = Am + Bn

  Here, m is time required to communicate the virtual environment

  n is the time required to process each algorithm in the environment.

- **Space Complexity:** 3D password authentication system included 3D virtual environment. The user interacts with the virtual environment. Therefore, there will be 3 axes (x, y and z). The interaction coordinates will be each of 3 values (x, y and z). Therefore, for each interaction 3 coordinates are required to store. So, the space complexity will be n3.

Applications

3D password is more secure and more useful authentication scheme than other already available authentication schemes. 3D password can be applicable in wide range of areas. Some of them are:

- **Networking:** Networking includes many critical systems. Some of them are: client-server architecture etc. The data on these systems are very critical and must not be vulnerable to the unauthorized personnel. So, 3D password is a better solution to be used in these systems
- **Nuclear & Military Areas:** These are the area where the country needs the top-most security. They store the data which are very secret. 3D password can be the option to replace the older authentication schemes
- **Airplanes & Jet fighters:** There are many incidents in which these are misused for religion-political agendas. These airplanes must be secured. 3D password can be used to secure these.
- **Other areas:** 3D password can be used in various other areas like: ATM, cybercafes, Industries for data security etc.

Conclusion

Currently there are many authentication systems available. Some of them are based on the users' behaviour, while some of them are based on users' knowledge. All of them are used separately. Being used separately the systems becomes vulnerable to the attackers. The attackers can get to know the textual passwords through Brute force attacks. This may cause a huge loss to the users.

The 3D password is the multi-factor and multi-password authentication scheme which can combine all the already available authentication schemes. Its most basic component is the 3D virtual environment. The 3D virtual environment contains unique and distinct real-time objects on which the user interacts and generates the password. The password is generated by noticing the coordinates of the sequence of interactions in the text file. The text file then encrypts and after that gets stored in the database

Reference

[1] A.B.Gadicha, V.B.Gadicha-"Virtual Realization using 3D Password" International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, pp216-223, 2016.

[2] A.B.Gadicha, V.B.Gadicha-"Virtual Realization using 3D Password" International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, pp216-223, 2016.

[3] V.Sindhuja, S.Shiyamaladevi, S.Vinitha-"A Review of 3D Protected Password" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, pp3995-4001, 2016.

[4] Pooja M. Shelke, F. M. Shelke, Mr. B. G. Pund-"Advance Authentication Technique: 3D Password" International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, pp632-635, 2016.

[5] Vishal Kolhe, VipulGunjal, SayaliKalasakar, PranjalRathod-“ Secure Authentication with 3D Password” International Journal of Engineering Science and Innovative Technology, ISSN: 2319-5967, pp99-105, 2013.

[6] SmritiKhurana, Mili Patel, Prateek Kumar Singh-“ Study of 3D and 4D password Security” International Journal for Research in Computer Science, pp49-56, 2016.

[7] AnaghaKelkar, KomalMukadam-” 3D PASSWORD MODERN APPROACH TO SECURITY” International Journal of Computer Engineering and Applications, ISSN 2321-3469, pp31-38, 2015

[8] Shivani A. Patil, Shamli A. Hage-“Improving ATM Security Using 3D Password” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2278 – 8875, pp8308-8312, 2015.

[9] Mr. Rakesh Prakash Kumawat, Mr. SachinSampatBhosale, Mr. PrashantPrabhakar Ratnaparkhi-“3D Graphical Password Authentication System” International Journal for Research in Applied Science & Engineering Technology, ISSN: 2321-9653, pp319-325, 2015.

[10] NishaSalian, SayaliGodbole, ShalakaWagh-“Advanced Authentication Using 3D Passwords in Virtual World” International Journal of Engineering and Technical Research, ISSN: 2321-0869, pp120-125, 2015.

[11] DhatriRaval, Abhilash Shukla-“Security using 3D Password” International Journal of Computer Applications, pp36-38, 2015.

[12] Ms. Swati Bilapatte, Prof. Sumit Bhattacharjee-“3D Password: A novel approach for more secure authentication” International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, pp150-156, 2014.

[13] KalpanaRathi, Nidhi Sharma, Urmila Jangid-“The survey paper: 3d password” International Journal of Innovative Computer Science & Engineering, ISSN: 2393-8528, 2014.

[14] Mr.Jaywant N. Khedkar, Ms.Pragati P. Katalkar, Ms.Shalini V. Pathak, Mrs. Rohini V. Agawane - “ Integration of Sound Signature in 3D Password Authentication System” International Journal of Innovative Research in Computer and Communication
Engineering, ISSN: 2320 – 9801, pp447-452, 2013.

[15] Ashwini A. Khatpe, Sheetal T. Patil, Amruta D. More, Dipak V. Waghmare, Ajit S. Shitole-“3DLogin for More Secure Authentication” International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, 2992-3000, 2014