International Journal of Research in Engineering, Science and Management
Volume-2, Issue-4, April-2019
www.ijresm.com | ISSN (Online): 2581-5792

3D Password for more Secure Authentication in Android Phones

K. Nandhini[1], R. Sankar[2]
[1]*Student, Department of Computer Applications, S. A. Engineering College, Chennai, India*
[2]*Professor, Department of Computer Applications, S. A. Engineering College, Chennai, India*

***Abstract*: Authentication can provide strong security. Authentication is important for any systems to use it and it can be strongly protected. Authenticating a system using tightly secured password using many authentication schemes. Users nowadays are provided with major stereotypes such as textual password, graphical password etc., but each individually have its own limitation and drawback. A new scheme can be introduced i. e, 3D password. It is a multi-factor authentication scheme where the user navigates and interacts with various objects. 3D password can combine most existing authentication scheme such as textual password, graphical password and various types of biometrics into a single 3d virtual environment. In this paper, it improves security for android phones using 3D password. It describes the concept about what is 3D password, how the working of 3D password done, concepts related to 3D password, applications of the scheme.**

***Keywords*: Authentication, graphical password, Multifactor, Textual password, 3D password, 3Dvirtual environment**

1. Introduction

Currently many problems occur due to lack of uncertainty. Using latest technology passwords can be easily hacked for unlawful purposes. Users often choose often face several difficulties while using the textual password. Many accessible passwords can be used in the form of graphical or textual password. Smart cards can be stolen by illicit users. Many authentication schemes can be introduced on the purpose of reducing the use of illegal users; however, users have their own thoughts on using the password in different schemes. Moreover, schemes of biometrics can be used. This paper fully represent8s the complete working of 3D password.

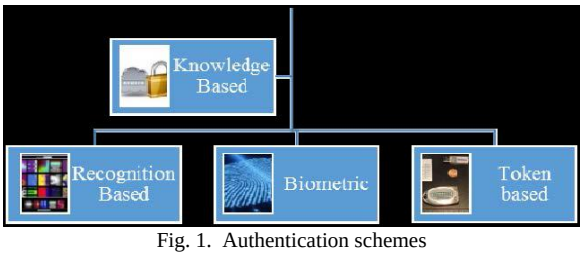

Fig. 1. Authentication schemes

Knowledge Based: means what you know. Textual passwords can be used in several ways.

- Token based: means what you have [1]. It includes all the cards including ATM card, Aadhar card etc.
- Biometrics: It can be used for all signs expressions such as fingerprints, face expressions etc.
- Recognition Based: means what you recognize. Includes, graphical password, iris recognition, face recognition etc. According to the nature of the scheme and method used preferably, two types of authentication schemes are available [2]-[4].
- *Recall Based*

In this authentication, user need to recall or memorize his/her password which is created before. It is a part of the knowledge based authentication e. g Textual password, graphical password etc, this technique is commonly used all over the world where security is required. Recall based performs all the existing schemes of the biometrics password, it can be either textual or graphical password. It is the most and efficient password system.

- *Recognition Based*

In this authentication technique user need to identify, recognize password that can be created before. This authentication technique can be used in graphical password. This technique can be used much more than recall based is used. These two techniques have some drawbacks and limitations individually or used single authentication at a time. To overcome these limitation and drawback of previously existing authentication scheme. A new authentication scheme introduced which is based on the combination of previously existing authentication scheme Called as the “3D password”. [5]-[7].

- Biometric Based: Biometric schemes such as fingerprints, Thumb impression, iris recognition, voice recognition etc. These authentication techniques are used in many areas, by using this simple method have revealed that token are susceptible to fraud, loss or theft.

2. Literature survey

3D Password is one of the most strong authentication system.3D password can be used as the often tightly secured Password. With this 3D password other unauthorized user cannot use this password in the illegal way. It often provides 3 levels of password which is often difficult for the illegal user to access the password.

3. Existing system

Generally current authentication system suffers from many weaknesses. Commonly textual password can be used which can be easily cracked by the application of various brute force attacks. currently accessible graphical password has a password breathing space which is slighter than or equal to the textual password space. smart cards and tokens can be stolen. Moreover, authentication can be cancelled. The 3d password is a multi-factor authentication scheme in a single 3D virtual environment to the user. The design of the 3D environment and the type of objects selected determine the 3D password key space. Users can have the choice to choose whether the 3D password will be recall, recognition, or token based or mixture of two schemes or more.

Disadvantages

- It is more expensive than other authentication technique.
- Large time and large memory space required.
- Shoulder surfing attack can attack this scheme.
- Difficult for blind people to use this technology.

4. Proposed system

This proposed system combining all the multi factor schemes that can be capable of securing the authentication in android. Users have their own idea of selecting their Passwords as token based, recognition based and biometrics [9]. This lack of restriction over the selection of passwords determine users are different from different ideas. Therefore, to authenticate the secure system users must be aware of the passwords that is adequacy and imperative. The following requirements are contented in the estimated scheme.

1. The new scheme secretly protects the system and very difficult for other illegal users to access it.
2. This scheme can be difficult to break the security as it is tightly secured.
3. The new scheme secrets cannot be written in paper.
4. It fails all the existing attack, so it is often difficult to break.

The 3D password contains all the schemes into a single scheme. This 3D virtual environment can interact with many objects or items. The user is obtained with the virtual 3D environment interacting many items or stuff. The actions and exchanges towards the 3D virtual environment constructs the 3D password. The 3D password combines all the existing authentication schemes and techniques that can be used. The 3D password can be used as the one of the most secured password. Nowadays in trending technology it is the most upgraded among the other password. The proposed system being the very successful and it is often very difficult for the illegal users to use it.

The choices of what authentication schemes to be used within the system as the requirements of the 3D password [8]. A user who is efficient of remembering can use the textual password and graphical password. Instead users who have poor recollecting power can use the smart cards and biometrics [10]. Besides user who wishes to keep biometric password can use such as face recognition, iris recognition etc.

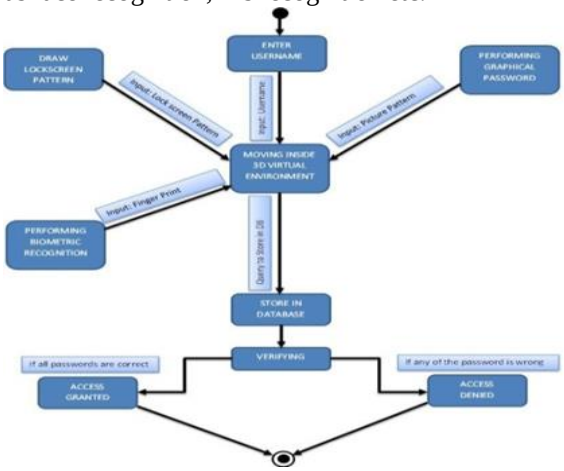

Fig. 2. State diagram of 3D password

Advantages

3d password is multi factor authentication scheme in a 3d virtual environment.

- It fails most of the brute force and dictionary attacks.
- Efficient to use as an end user.
- Flexible, as it provides multifactor authentication i. e token based, knowledge based, biometrics.
- Helps to keep lot of personal details.
- Can be memorized in form of short stories.

5. Working of 3D password

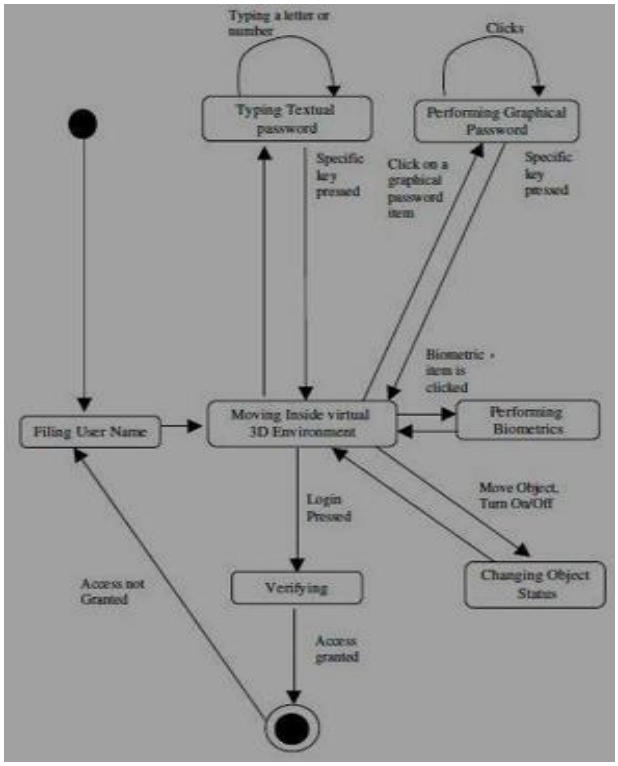

Fig. 3. Working of 3D password

The first step in creating the 3D password is that all the objects in the virtual environment can interacting each other [11]. The 3D virtual environment is visible usually as per the people sight. Objects used in virtual environment can interact with many objects (sized to scale). Possible actions and objects can interact it with the 3D environment. Object responses should be sensitive. The 3D virtual environment can interact with many object in the 3D virtual environment.

The 3D password has been implemented in many fields. Now it can be implemented in android using virtual environment.

6. Algorithm

A. *Time Complexity*

Time complexity = A m + B n, here m is indicating time required to communicate with system, & n is time required to process each algorithm in 3D environment. Time complexity provides better interacting with the objects and it can be capable of performing secured complexity. Time complexity is the efficient way of performing security.

B. *Space Complexity*

Method can contain 3D virtual environment, so that each point the coordinate axis in the working environment [12]. Space complexity can be used with the measure of memory spaces and algorithm used in the complex function.

C. *Virtualization*

Let us consider G*G*G to be the size of the total environment space. distributed with the unique (x,y,z) coordinates in the 3dimensional virtual environment. Here, system is implementing 3Dimensional password system to provide security to the android mobile.

7. Difficulties faced

A. *Shoulder Attack*

Attackers observe the user from back shoulder then easily break their authentication.

B. *More Time and Memory*

To use 3D password, it requires more time and memory chunk because 3D passwords needs more memory space to store in it.

C. *Expensive*

3D password is more expensive compare to other authentication technique.

D. *Complexity*

3D password is more complexity in coding.

8. Security analysis

A. *Timing Attack*

Here the attack is based on how much time is required by the legitimate user in completing successful login using 3D password scheme which gives the attacker mere hints and with this observation attacker can get a clue regarding authenticated user's 3Dpassword length.

Yet this attack is not very much effective as it gives mere clues to the attacker. Thus, it would perhaps be performed as a part of either brute force attack or well-studied attack. If 3D virtual environment is poorly designed, then timing attacks can be effective.

B. *Brute Force Attack*

In this kind of attack, the attackers have to try n number of possibilities of a 3D password [2]. As these attacks consider the passwords in automated fashion.

C. *Required Time to Login*

In 3D password, time required for successful login varies and depends on number of obvious actions and interactions, the size of a 3D virtual environment.

D. *Well Studied Attack*

In this attack the attacker tries to find the entire password scheme. In order to instigate such an attacker has to attain knowledge of the most probable This attack is quite difficult that the attacker has to well aware of all the existing schemes to be used. This is quite often difficult the attacker to remember all the previous process, so it cannot be easily unbreakable. It can also be tightly secured.

E. *Shoulder Surfing Attack*

Here, an attacker uses the camera to record the user 3Dimensional password or the hacker tries to watch the legitimate user creates 3D password. This kind of attack is the most effective than any other attacks on 3Dimensional passwords. Therefore, the 3Dimensional password must be performed in a secure place where shoulder surfing attack can't be performed.

- Shoulder surfing attack can attack this scheme.
- Difficult for blind people to use this technology.

9. Applications

The 3D password can be used in various applications such as

1. ATM
2. Personal Digital Assistance
3. Desktop computers and laptop
4. Web Authentication
5. Security Analysis etc.
6. Critical servers.
7. Nuclear reactors and military facilities.

10. Result

3D passwords are more efficient to use, being a tightly secured authentication, it provides very enormous areas to work under the 3D password. A future work is in the field of research.

11. Conclusion

The 3D password is a multifactor authentication scheme that can combine various authentication technique into a single 3D virtual environment. The user can navigate and interacts with various objects. The sequence of actions and interactions inside the 3D environment constructs the user's 3D password. The main goal of this paper is to provide security to the android using 3d password combining all the existing or upcoming authentication system. The 3D Password is the best method to provide security which can be used with the combination of all possible password together. It is more efficient than other authentication, hence it is a tightly secured authentication system. Moreover, it shows how the attacker will acquire knowledge of the most possible attacks. Shoulder surfing attacks are still possible and effective against 3D password, therefore a possible solution is a field of research.

12. Future scope

3D passwords are now currently used in military areas to provide high security. In future it will be used in banking transaction accessing our email accounts etc. The 3D password is still used in many areas as the research is going to the extent. In general, present system uses CAPTCHA that are freely available that can crack CAPTCHA within seconds, so the hacker uses the brute force attack.

Acknowledgement

I could like to thanks of gratitude to complete my journal on "3D Password for More Secure Authentication in Android Phones".

I convey my sincere gratitude to my Academic Supervisor Mr. R. Sankar, Assistant Professor of Computer Application. His guidance makes me to complete the journal. This was a good opportunity to do this paper my sincere thanks S.A Engineering College who gave me this opportunity to do this paper I came to know many good things I would also like to thank my parents, friends who helped me and encourage me to finalizing this paper.

References

[1] Swati Bilapatte, "3D password: A novel approach for more secure authentication," International Journal of Computer Science and engineering technology, 2014.
[2] Bharti, "Design 3D password with session based technique for security in smart phone," International Conference On Green Engineering and Technology, 2016.
[3] Shivani A. Patil, "Improving ATM Security using 3D password," in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2015.
[4] Sahana R. Gadagar, Aditya Pawaskar, Rangeeta B. Pandhare, "3D Password Authentication for Web Security," International Conference on Recent Innovations in Engineering and Management, 2016.
[5] Ashwini A. Khatpe, Sheele T. Patil, Amruta D. More, Dipak V. Waghmare, Ajit S. Shitole, "3D Login for more Secure Authentication," International Journal of Innovative Research in Computer and Communication Engineering, 2014.
[6] A. B. Gadicha, V. B. Gadicha, V. B. Gadicha, "Virtual Realization using 3D password," International Journal of electronics and computer science engineering.
[7] F. A. Alsulaiman and A. El Saddik, "Three-Dimensional Password for More Secure Authentication," in *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 9, pp. 1929-1938, Sept. 2008.
[8] Shubbam Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar, "New Era of authentication: 3-Password, International Journal of Science, Engineering and Technology Research, vol. 1, no. 5, November 2012.
[9] Sonker S. K, Ghungrad. S. B, "Minimum Space and Huge Security in 3D Password Scheme," in International Journal of Computer Application, vol. 29, no. 4, September 2011.
[10] I. Sobardo and J. C. Birget, "Shoulder surfing resident graphical password," Draft, 2005.
[11] F. A. Alsulaiman and A. El Saddik, "Three-Dimensional Password for More Secure Authentication," in *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 9, pp. 1929-1938, Sept. 2008.