International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Enhancing 3 Level Security using 3D Password

Divya PremChandran[1], Sailee Sunil Rajeshirke[2]

[1]Assistant Professor Department of MCA, Bharti Vidyapeeths Institute of Management Information Technology, C.B.D. Belapur, Navi Mumbai, India

[2]Department of MCA, Bharti Vidyapeeths Institute of Management Information Technology, C.B.D. Belapur, Navi Mumbai, India

Abstract: ***Authentication is a technique of providing a system to service in a more secure way. Password authentication can be done in various techniques like OTP, Bio-metrics, Textual Password, Graphical Password, and algorithms. But there are some or the other limitations in every techniques. To overcome those limitations a new improved technique named 3D Password is been developed. Our technique uses textual password, graphical password, bio-metrics, recognition, etc. So 3 Level security provides multi factor facility in authentication technique. 3 Level security exclusively uses a 3-Dimensional virtual environment which contains scenarios of real time objects which are not real objects, but looks like the real ones, an biometric device for finger print scanner,and a textual password. Virtual environment is a user interface which looks like the real life environment. 3Level security is more secure and unbreakable authentication method. In this research paper we have focused upon how this 3 Level security technique can be made more user friendly and more secured. We're also explaining what exactly is 3D password?, Why is 3D password said to be as most secured authentication tech-nique?, working of 3d password technique, some of its related mathematical concepts briefly section wise in this research paper. Authentication is a technique of providing a system to service in a more secure way. Password authentication can be done in various techniques like OTP, Bio-metrics, Textual Password, Graphical Password, and algorithms. But there are some or the other limitations in every techniques. To overcome those limitations a new improved technique named 3D Password is been developed. Our technique uses textual password, graphical password, bio-metrics, recognition, etc. So 3 Level security provides multi factor facility in authentication technique. 3 Level security exclusively uses a 3-Dimensional virtual environment which contains scenarios of real time objects which are not real objects, but looks like the real ones, an biometric device for finger print scanner,and a textual password. Virtual environment is a user interface which looks like the real life environment. 3Level security is more secure and unbreakable authentication method. In this research paper we have focused upon how this 3 Level security technique can be made more user friendly and more secured. We're also explaining what exactly is 3D password?, Why is 3D password said to be as most secured authentication technique?, working of 3d password technique, some of its related mathematical concepts briefly section wise in this research paper.***

Keywords: Authentication, OTP, Bio-metrics, Multi-password, Virtual Environment, 3d password,3 Level Security,Finger Print

1. Introduction

Authentication is a technique of identifying the authen-ticity of the user which means that it checks whether the user connected is genuine user or not. Authentication provides maximum larger protection checks that are provided to the system by special validation functions. In our system we have made the authentication process more strict and un breakable.In this security system we have made use of 3D password for its unbreakable security. In our Security we have madde the 3d password more tricky and unbreakable. Authentication provides restriction to illegal entries so that only legal users can get access to the system thus there are two types of authentication systems.

Recall Based:

1) Knowledge Based: It means the things that we know. Eg.: Textual Password.
2) Token Based: It means the things that we have with us. Eg.: Smart Card.

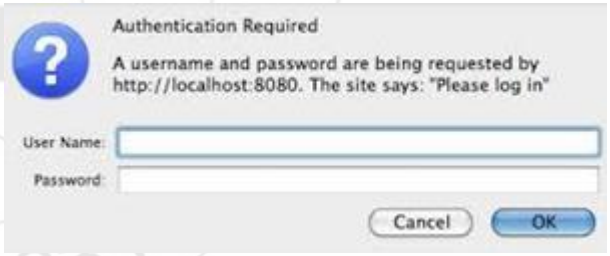

Figure 1: Recall Based Authentication

Recognition Based:

1) Bio-metrics: It uses the human body parts. Eg.: Finger print.
2) Recognition Based:It uses human oragans for recognition. Eg.: Face Recognition.

Figure 2: Recognition Based Authentication

2. Objective of the Study

The proposed 3 Level authentication system is the mix-ture of various other authentication techniques. 3d password is nothing but the combination of recall based and recognition based authentication techniques.

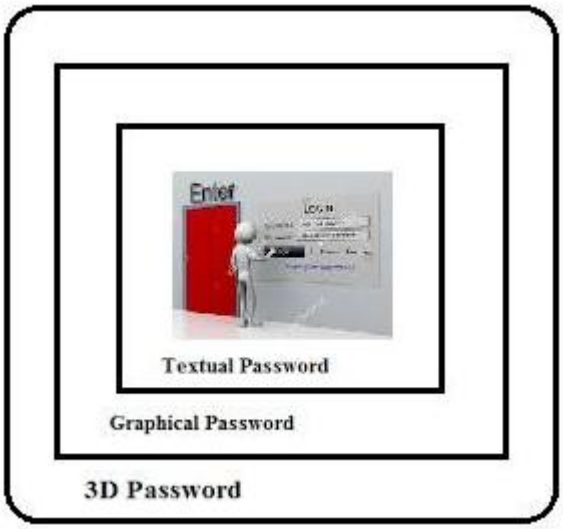

Figure 3: Multi-password and multi-factor authentication technique

In our authentication process we are using Bio-metrics because it is more precise and specific to the authincated person, there is a total information provided of who is logging in to the system, with the finger print scanner we have managed to store the information of the user by linking his/her adhaar card. The information is linked when the concerned person is an employee of the organisation. This will let us know all the details of the person logged in into the system. We have made use of virtual environment which is called as 3d virtual environment. This virtual environment allows user navigate by moving in the virtual environment to generate the 3d password.

The Objectives are:
1) To provide highly secured authentication technique.
2) The system should be more user friendly, easy to use.
3) The system should allow user to select more than one password.
4) The system should overcome the limitations of previously made authentication techniques.

3. Literature Review

As described in our introduction the types of authen-tication system are recall based and recognition based. Recognition involves identifying or recognizing the images seen previously, and not generate them from memory. On the other hand recall base is retrieval of those images or identification sources through external purely aided memory

.Pure memory recall is tougher than recognition technique. Recall based techniques involve knowledge based remem-bering textual passwords which are not written anywhere. Where as in the Recognition based technique the users are given a set of images from which they have to memorize one image and that image will become the password for that particular user. At the time of authentication the user will use his memorized image to unlock a particular system.

In the literature review of 3D password there happened to be a study conducted by Dhamija and Perrig. They had a approach of graphical authentication scheme which was using Hash Visualization technique. In their system, user had to select some images from a set of random pictures generated by a program. Later, user had to identify the previously selected images to be authenticated. This study resulted into 95% of all participants succeeded in the authen-tication using their technique, while only 75% succeeded using text-based passwords and OTP.

4. 3D Password

4.1. Architectural study of 3 Level security

In this section we will be explaining about how 3d password is created and what all different techniques are been used to make a highly authenticated 3 Level secu-rity. As 3d password is a multi-factor and multi-password authentication tool many techniques like textual password, graphical password, recognition, bio-metrics, etc. can be used to form a 3d password. Different techniques are been selected on the basis of type of user that are going to use the system.

4.2. Generation of 3 Level Password authentication

1) User has to authenticate himself/herself with a sim-ple textual password.
2) After the user is authenticated with the textual password, user is directed to the biometric finger print image scanner, where the users finger print is matched with the stored data in the system.
3) As the user scans his fingerprint in the scanner his information is cross checked and then the user if valid is granted to the 3rd level of security check that is the 3D password virtual environment.
4) After the above steps of successful authentication in virtual room further, the user moves into next level where he can see various kinds of graphical images and has to perform some action like, selecting a flower pot, or the frame, chair, etc. The objects in the room change their sequence as well as the over all environment also changes. The object which the user selects becomes his 3d password.
5) All the actions that user performs are recorded sequentially in a text file encrypted format.
6) Thus user creates his 3d password.

So, then time complexity=Am+Bn where m is time required for communication with system and n is time required to process the algorithm.

Space Complexity:- As we're using 3d virtual envi-ronment for generating 3d password each point in the environment will be having 3 co-ordinates X, Y, Z. Hence the space complexity for 3D Password is n3.

Figure 4: 3D Password demo

4.3. Working of 3 Level Security with 3D password

The actions that user has performed for generating his 3d password are recorded with the help of 3d Quick hull algo-rithm. This 3d Quick hull algorithm is build on the convex hull algorithm that tracks user selection X,Y,Z points. In future when the user wants to use the system the user will be asked for the 3d password which he has generated. So the user has to perform the same steps, select the objects in the room that he has performed while generating his 3d password. These steps are then compared with the file that was created during the generation of 3d password and if it matches then the user is given access to the system or else it is denied.

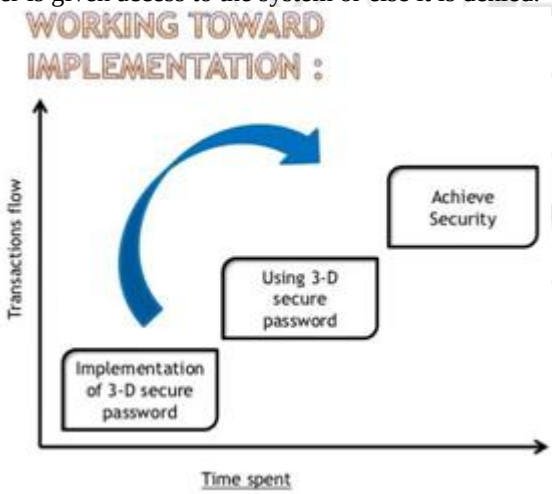

Figure 5: 3D Password working

5. Mathematical Concepts for 3D Password

Time Complexity:-To calculate the time complexity of 3d password let we assume A as virtual 3d en-vironment plotting and B as algorithmic processing.

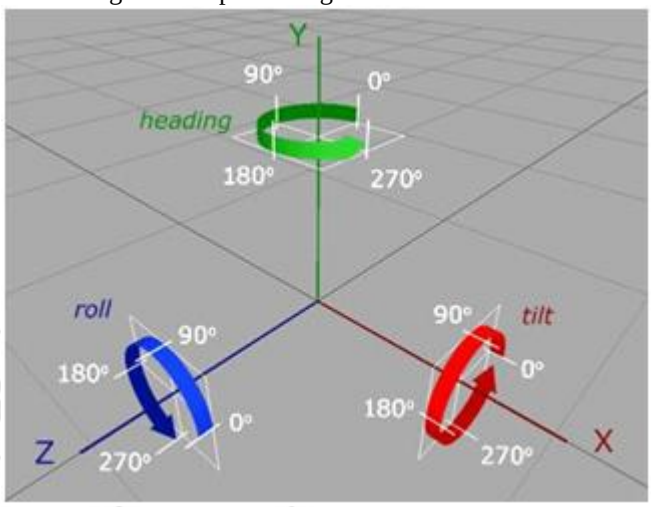

Figure 6: X,Y,Z co-ordinates for 3D Password

6. Conclusion

Currently password uses textual and graphical passwords technique. There are various another authentication tech-niques that can be implemented in this which are under study and will require more time. User can generate 3d password of his own choice with the help of the 3d virtual environment. As 3d password is a merger of recall and recognition based authentication techniques it is a multi-password, multi-factor authentication technique. Also a brief research can be done on how 3d password can be utilized in mobile smartphones.

Figure 7: Process of 3 Level security

References

[1] Smita Verma, Roopal Dubey, ”3D PASSWORD AUTHENTICA-TION”.
[2] Tejal Kognule, Yugandhara Thumbre, Snehal Kognule, ”3D PASS-WORD”.
[3] Mrs. Vidya Mhaske-Dhamdhere, Lecturer. Bhakti Pawar, Pallavi Ghodke, Pratibha Yadav,Student ”3-D Graphical Password Used For Authentication”.
[4] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, ”Secure Authentication with 3D Password”
[5] A.B.Gadicha , V.B.Gadicha , Virtual Realization using 3D Password
[6] http://www.slideshare.net/Gowsalyasri/3d-password-ppt
[7] http://www.watchguard.com/training/fireware/82/authent 2.htm
[8] http://www.slideshare.net/subhashreeforever/3-dinternet-24624309
[9] http://www.slideshare.net/asertseminar/3d-password-33114510
[10] http://codetechie.blogspot.in/2013/05/3d-password.html