3D Password - A Way of Secure Authentication

Jeetu Sonar[1] Gaurav Joshi[2]
[1,2]Department of MCA
[1,2]Vivekanand Education Society Institute of Technology, Affiliated to Mumbai University, Mumbai

Abstract— Present days, confirmation framework has numerous issues, for example, literary passwords can be effectively distinguished either by utilizing savage power system or by picking important words from lexicons. To accomplish this constraint numerous graphical secret key are accessible which consume less memory room when contrasted with printed watchword. Additionally, biometric framework is utilized which may mechanize the ID or confirmation of a person by recognizing human qualities. Multi component verification plan is called 3-D secret key which speaks to the 3-D virtual environment of the different virtual items. Association with articles happens by the client through this environment. In 3-D virtual environment there is an arrangement and mix of client cooperation which is characterized as 3-D secret key. 3-D watchword key space is characterized by the outline of 3-D virtual environment and kind of articles chose.

Key words: Authentication, OTP, Bio-metrics, Multi-password, Multi-factor, Virtual Environment, 3D password

I. INTRODUCTION

Authentication is a technique of identifying the authenticity of the user which means that it checks whether the user connected is genuine user or not. So we can say that authentication is one of the most important security service for a system to keep it secured. There are various authentication techniques, algorithms that are been used to provide security to the system so as to provide right access, to the right person, to access the right data. Which means that only authorized users have the rights to access the system and the data. There are various authentication techniques that have been developed, with some of its drawbacks, which were overcome by other authentication systems. Basically there are four types of authentication systems.

A. 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.: ATM Card.

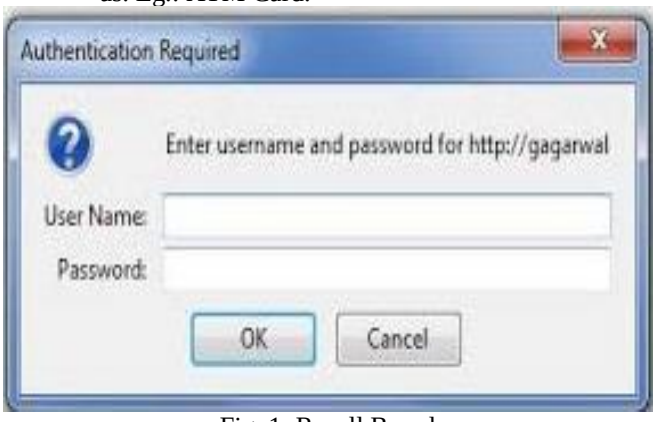

Fig. 1: Recall Based

B. Recognition Based

1) Bio-metrics: It means what we are. Eg: Thumb Impression.
2) Recognition Based: It means the objects that we recognize. Eg: Iris Recognition.

Fig. 2: Recognition Based Authentication.

II. PROPOSED SYSTEM

The proposed 3d password authentication system is the mixture of various other authentication techniques combined together to develop a highly secured authentication technique. 3d password is nothing but the combination of recall based and recognition based authentication techniques. Thus, providing multi-password and multi-factor authentication techniques.

In 3d password for authentication we have not made use of bio-metrics as it has some major drawbacks and also including bio-metrics in 3d password would lead in to increasing the cost and hardware parts of the system. so 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.

A. Objective of Proposed System

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.
5) The system should be the mixture of recall based and recognition based authentication techniques.

III. 3D PASSWORD

A. Architectural Study of 3d password

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 3d password. As 3d password is a multi-factor and multi-password authentication tool many

techniques like textual password, graphical password, recognition, bio-metrics [5], 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.

B. Generation of 3d Password

1) User has to authenticate themselves with a simple textual password.
2) After the authentication is verified and is successful, user is directed to a 3d virtual environment.
3) Here the user has to enter the x1, y1, z1 coordinates with the onscreen keyboard that is displayed to him on the screen.
4) After successful authentication in virtual room now, the user moves into next level where he can see various kinds of arts and has to perform some action like, pressing the button, etc.
5) All these actions that user has performed are recorded sequentially in a text file in encrypted format.
6) Thus user has created his 3d password.

Fig. 3: 3D Password

C. Working of 3d password

The actions that user has performed for generating his 3d password are recorded with the help of 3d Quick hull algorithm. This 3d Quick hull algorithm is based upon the convex hull algorithm that tracks the user selection points. Now when the user wants to use the system next time then the user will be asked for the 3d password which he has generated. So the user has to perform the same steps, select all the objects in the same sequence 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.

IV. Mathematical Concepts for 3D Password

A. Time Complexity

For calculating the time complexity of 3d password technique let us consider A as the virtual 3d environment plotting and B algorithmic processing. So, then time complexity=A^m+B^n where m is time required for communication with system and n is time required to process the algorithm.

B. Space Complexity

As we're using 3d virtual environment for generating 3d password each point in the environment will be having 3 co-ordinates X, Y, Z. Thus the space complexity of this proposed system is n^3.

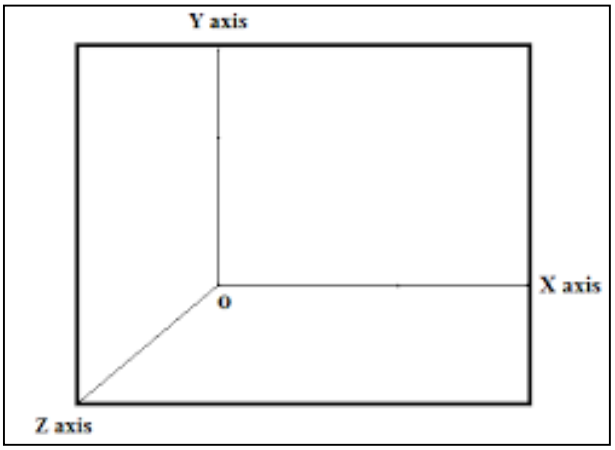

Fig. 4: Mathematical Expression [5]

V. Conclusion and Future Work

The currently available technique of 3d password uses textual and graphical passwords. There are various another authentication technique 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 combination of recall and recognition based authentication techniques it is a multi-password, multi-factor authentication technique. Including bio-metrics in current system leads to increase in the cost [6]. So there is still more research to be done of how bio-metrics can be included in current system by not affecting the cost very much [6]. Also a brief research can be done on how 3d password can be utilized in mobile smartphones.

Fig. 5: Virtual Room

References

[1] Smita Verma, Roopal Dubey, "3D PASSWORD AUTHENTICATION".
[2] Mrs. Vidya Mhaske-Dhamdhere, Lecturer. Bhakti Pawar, Pallavi Ghodke, Pratibha Yadav,Student, "3-D Graphical Password Used For Authentication".
[3] Tejal Kognule, Yugandhara Thumbre, Snehal Kognule, "3D PASSWORD".

[4] A.B.Gadicha , V.B.Gadicha , ―Virtual Realization using 3D Password".
[5] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, "Secure Authentication with 3D Password".
[6] Anil K. Jain, Ajay Kumar, "Biometrics of Next Generation: An Overview".
[7] http://www.slideshare.net/subhashreeforever/3-d-internet-24624309
[8] http://www.slideshare.net/asertseminar/3d-password-33114510
[9] http://codetechie.blogspot.in/2013/05/3d-password.html
[10] http://www.slideshare.net/Gowsalyasri/3d-password-ppt
[11] http://www.watchguard.com/training/fireware/82/authent2.htm.

