ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 9, September 2016

# A Survey on 3D Password

Prof. Dr.G.M.Bhandari[1], Naikwadi Shradha[2], Deshpande Gandhali[3], Tapkire Priya[4], Nawale Sanchita [5]

Asst. Professor, Dept. of Computer, BSIOTER, Savitribai Phule Pune University, Pune, India[1]

Student, Dept. of Computer, BSIOTER, Savitribai Phule Pune University, Pune, India[2,3,4,5]

**ABSTRACT**: The 3D passwords is very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. In our case, let's say a virtual garage. The 3D password is a multifactor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized.

**KEYWORDS**: Virtual environment, 3D password, authentication , MD5.

## I. INTRODUCTION

Users now a days are provided with major password stereotypes such as textual passwords, biometric scanning, tokens etc. Current authentication systems suffer from many weaknesses. We present our idea, the 3D passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionary or their pet names, girlfriends etc. Ten years back Klein performed such tests and he could crack 10-15 passwords per day. On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack. Which make textual passwords easy to break and vulnerable to dictionary or brute force attacks.

Graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate users graphical password by camera. Token based systems such as ATMs are widely applied in banking systems and in laboratories entrances as a mean of authentication. However, Smart cards or tokens are vulnerable to loss or theft. Moreover, the user has to carry the token whenever access required.

Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning).In this paper, we present and evaluate our contribution, i.e., the 3D password.

## II. RELATED WORK

In the 3D virtual environment, each 3D virtual object has its own response to the actions performed by the user. The different actions and their combined sequences form the user's 3D password. The following scenario can be used to illustrate this concept. In a 3D virtual environment, a user might place virtual objects such as garden tools scattered in a virtual garage in a particular order so as to represent his/her password, or may engage in a form of role playing in the virtual world and thereby using such repeatable actions to represent the password actions that allows login into a mobile device. The 3D password scheme has many advantages as summarized in. A 3D password is easy to remember because the user can regard the password as a 'little' story.

Additionally, the diverse 3D objects and the large number of possible interactions towards them can provide large theoretical password space, which increases the difficulty of cracking.

## III. PROPOSED ALGORITHM

The proposed system can be implemented with three stages. The initial stage is the predominant one, which requires intense use with the objects in the environment. The 3Dvirtual environment must be responsive enough to set the password. The real life situations will be having high responsive rate as it is using every day and it won't be a for gettable one. The three stages of this algorithm are Password creation stage, Password storage case and password verification stage. The explanation is given below

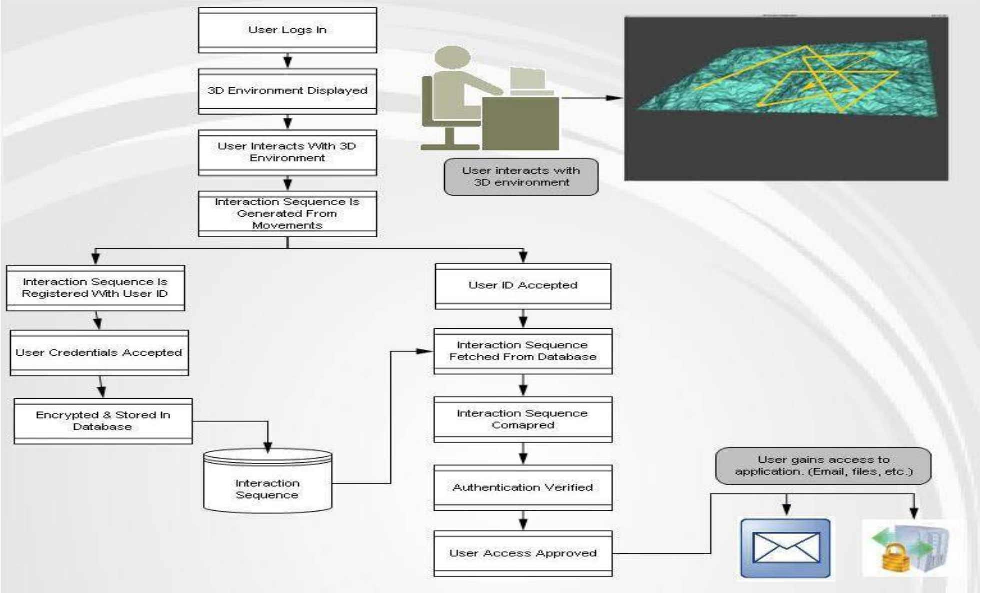
User Logs In
3D Environment Displayed
User Interacts With 3D Environment
Interaction Sequence Is Generated From Movements
User interacts with 3D environment
Interaction Sequence Is Registered With User ID
User Credentials Accepted
Encrypted & Stored In Database
Interaction Sequence
User ID Accepted
Interaction Sequence Fetched From Database
Interaction Sequence Comapred
Authentication Verified
User Access Approved
User gains access to application. (Email, files, etc.)

Fig: System Architecture

### A. PASSWORD CREATION STAGE

1. The user is asked to select the virtual environment, which is familiar to the user. It is selected from the virtual environment gallery of server.

2. The user has to perform sequence actions and interactions with the selected objects in the virtual environment. These details regarding selected object will be recorded. A new linked list is created in which each node will contain data for one object.

DOI: 10.15680/IJIRCCE.2016. 0409154

3. This sequence of value is used as the graphical password for the user.

### *B. PASSWORD STORAGE STAGE*

1. MD5 algorithm is used for the authentication purpose. The linked list is stored in a buffer where padding and appending is done to make its length 128 bits.

2. 128-bit sequence is generated by MD5 algorithm.

3. User selects an object in the virtual environment, where password can be stored.

4. As user click on store the password, the 128-bitsequence generated by MD5 is watermarked with the object selected by the user.

### *C. PASSWORD VERIFICATION STAGE*

1. The user should select the same virtual environment that has been chosen at the registration time.

2. User selects an object in the virtual environment, where password was stored and extracting from the object.

3. The user needs to repeat the same sequence of user's actions and interactions towards the selected object in the virtual environment 3D for making the password.

4. This new linked list link list is appended and padded to send as an input for MD5 algorithm.

5. The new MD5 128 bit string is compared to the 128 bit MD5 value is extracted from the object as shown

## IV. SIMULATION RESULTS

The 3D password presents a virtual environment containing various virtual objects. The user walks through the environment and interacts with the objects. It is the sequence of user interactions that occur in the 3D environment. The sequence of actions and interactions towards the objects inside the 3d environment constructs the user's 3d password. And no one can hack this password. This is the main advantage of our system.

## V. CONCLUSION ANDFUTUREWORK

Our main focus is to give priority or security to critical data section in any field. For implementing such a system storage space requirement is very large. In future programmers or algorithm designers must ensure fast way to extract password and limit storage requirement.The authentication can be improved with 3d password, because the unauthorized person may not interact with same object at a particular location as the legitimate user. It is difficult to crack, because it has no fixed number of steps and a particular procedure. Added with biometrics and token verification this schema becomes almost unbreakable**.**

## REFERENCES

[1] Praseeda K Gopinadhan, Renjith P R Biju ,Abraham Naremparambil "A New User Authentication Strategy Based on 3D Virtual Environment" International Journal of Computer Science and Information Technology & Security 2012.
[2] Zhen Yu, Ilesanmi Olade," An Exploration of 3D Graphical Passwords"IEEE 2016
[3] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, , IEEE "Three-Dimensional Password for More Secure Authentication" IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT,
[4] Tejal Kognule, Yugandhara Thumbre "3D Password"International Conference on Advances in Communication and

Computing Technologies2012

[5] Shipra Kumari1, Hari Om2”Remote Login Password authentication Scheme based on Cuboid Using Biometric “2014 International Conference on Information Technology

[6] M. K. Khan, S. Kumari, M.K. Gupta, F. T. Bin Muhaya,“Cryptanalysis of Truong et al.’s Fingerprint Biometric Remote Authentication Scheme Using Mobile Device”,Advances in Brain Inspired Cognitive .

[7] Novel 3D graphical password schema-Fawaz A Alsulaiman and Abdulmotaleb El Saddik

[8] Mun-Kyu Lee”Enhancing Security with 3D Display” global conference on electronics.

[9] Dhatri Raval”Security using 3D Password” International Journal of Computer Applications (0975 – 8887) Volume 120 – No.7, June 2015.

[10] 3D Password: Minimal Utilization of Space and Vast Security Coupled with Biometrics for Secure Authentication. http://www.ijater.com/Files/b8d368df.