Virtual Reality Based User Authentication System

Kapil M. Jain
UG Student
Department of Information Technology
Fr. Conceicao Rodrigues College of Engineering, Bandra

Nirbhay A. Pherwani
UG Student
Department of Information Technology
Vivekanand Education Society Inst. of Tech., Chembur

Abstract

In today's world authentication is the first parameter that is taken into account before creating a system and is also the first shell in providing security to your digitally stored profitable information. Providing Authentication to any system results in a more secure version of the same system. To provide this security many strides have been made in the field of security, over the years various attempts were made to provide a more secure solution to the already existing methods in areas of computers, tablets and mobile devices, like textual passwords, graphical passwords, etc. But security in Virtual Reality systems is an area which is underexplored. In this paper, we propose a security mechanism called the "VIRTUAL REALITY PASSWORD" which tries to overcome the drawbacks of existing authentication systems if used in VR and propounds a technique that can help users authenticate in a more secure and easy to remember manner.

Keywords: Virtual Reality, Virtual Reality Authentication, Authentication System, VR Password

I. INTRODUCTION

Virtual Reality (VR) is the use of computer technology to create a simulated environment. Unlike traditional user interfaces, VR places the user inside an experience. Instead of viewing a screen in front of them, users are immersed and able to interact with 3D worlds and objects. VR technology has been emerging with a plethora of applications in the field of education, Data visualization, Knowledge training, entertainment, aviation, medicine and the military. In future, the possibility of VR having its own Operating system with language and user interface doesn't seem a long shot. Advancement of VR systems as a standalone would open up the issue of illegal intrusion and attacks, and a critical one. Thus incorporating a secure authentication system in VR will prove beneficial for the further growth of VR in a secure way.

Authentication is one of the most important security service provided to the system by the different authentication schemes or algorithms. To protect any system authentication must be provided so that only authorized persons can have right to use or handle that system & data related to that system securely. When it comes to mobile and computer security the categories of authentication systems can be divided into three classes: knowledge-based, token-based and biometric-based [3]. External hardware requiring authentication schemes such as token-based and biometric-based are difficult and not cost-effective to implement. Textual password uses a PIN (Personal Identification Number) that uses digits ranging 0-9, which is easily memorisable but also easy to be broken. A largely used knowledge-based authentication system is Pattern Lock System that contains a (3x3) grid where the user constructs a pattern by connecting the points in the grid — commonly used in Android iOS operating systems.

The Systems are well tested for use in the 2D interface devices, however, there is little or no valid conceptual proof or literature for VR systems security. It thus makes it imperative to dive into investigating how the VR systems can be made secure can. The proposed system creates an amalgamation of virtual reality and authentication scheme. Most important part of VR password system is the inclusion of virtual environment. As the 3D virtual environment is an environment which is consisting of real-time object and scenarios which are algorithmically created and put together, it is not actually real time environment, but it is just user interface provided to make the user immersed in the system which looks like same as real environment. This environment is only visible to the person wearing the HMD and no one else outside, this provides the privacy which is the most important concept of security. We have implemented a password which consists of not creating a graphical pattern or typing in passwords but to move an object from one place to another place, repeating the actions with multiple objects in the VR environment in a particular sequence of objects together forms the Virtual Reality Password. The user wearing the HMD interacts with objects using the interaction hardware to create a sequence of specific movements of objects inside the virtual environment which will then be stored as the password. The sequences in which the objects are moved and change in position of each of the object together combine to form the virtual reality password. Any obvious actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as gesture recognition) in the virtual 3D environment can be considered as a part of the VR password [1] [2].

The user wearing the HMD interacts with objects using the interaction hardware to create a sequence of specific movements of objects inside the virtual environment which will then be stored as the password. The sequences in which the objects are moved and change in position of each of the object together combine to form the virtual reality password. The concept of this system in comparison to the currently existing system is more unique as there are infinite possibilities of placing the objects in the virtual

All rights reserved by *www.ijste.org*

world. Virtual Reality Passwords could be the next major authentication system which can be used in day to day VR applications and OS providing a new dimension to the existing methods of user authentication.

II. USING VIRTUAL REALITY FOR AUTHENTICATION

A. Drawbacks of the Current Authentication System

There are many authentication techniques available, such as textual password, Graphical password, etc. but each of this individually having some limitations & drawbacks. Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however users do not follow their requirements. Users face difficulty in remembering a long and random appearing password and because of that, they create small, simple, and insecure passwords that are easy to attack. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. With the development by means of technology, it has become very easy for others' to hack someone's password.

B. How can the proposed system be better than the current system?

In the proposed system, the authentication will be based on the virtual reality. VR password is based on the actions user performs in his day to day life in his daily environment. The password mechanism we have come up with makes use of the fact that rehearsal causes the memory to move from working memory into long-term memory, thus there might not be a need to remember the password if it's done on a daily basis. Creating an environment for the user suitable to their requirements and comfort makes it flexible, dynamic and secure to the user as he is more aware of the surroundings. VR password is based on the sequence of actions which are unique to each and every individual and there is an infinitesimally low chance of similar passwords if given the same environment.

C. Hardware and Software Used

The hardware used to develop the system includes Leap Motion and Oculus Rift DK2. These systems were found suitable for development and easy to integrate and work with. Leap Motion is a commercial hand tracking device which replicates the user's finger and hand movements from real world mapped to virtual world in the area defined by the device from. The Oculus Rift DK2 is a virtual reality headset developed and manufactured by Oculus providing development ease. To have better compatibility between these two pieces of hardware and provide the appropriate visual design, Unity, which is a cross-platform game engine, is selected as the main development tool while C# is chosen as the primary programming language.

III. ALGORITHM AND FLOWCHART

The Algorithm consists of 3 stages:-

- User Input Stage - This stage is where the user wears the HMD and logs in the system to perform the actions and interact with the objects.
- User Action Mapping - After the user enters its password the coordinates of initial and final position of the object and the sequence of their displacement together are mapped to the stored database coordinates.
- Authentication - if the coordinate and sequence mapping is successful then the user is granted access, else he has to re-perform the actions if access is denied.

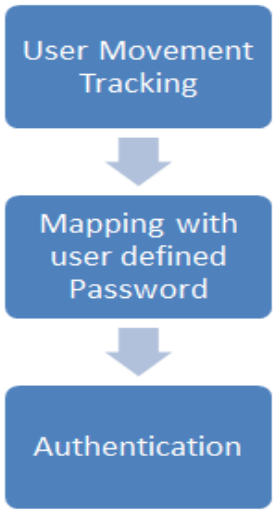


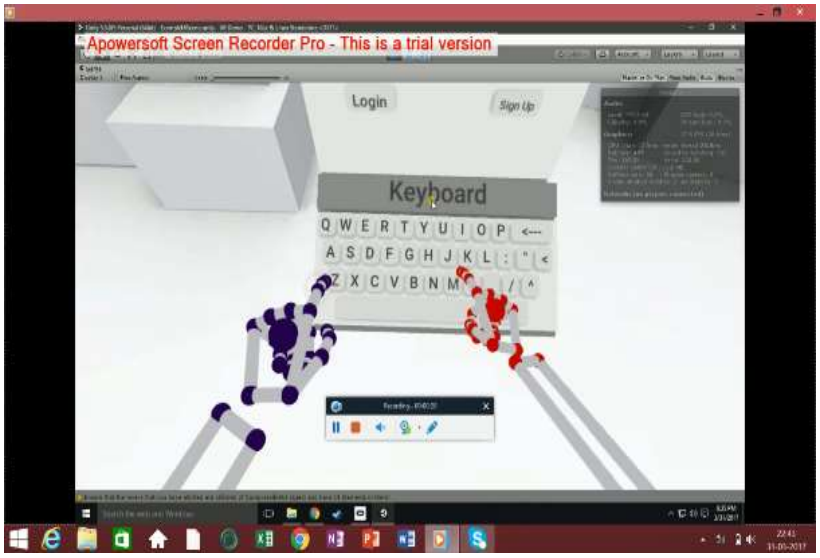
Fig. 1: Working Algorithm

All rights reserved by *www.ijste.org*

IV. WORKING

A. The Initial Step:

- The process starts by wearing the Oculus Rift HMD integrated with Leap Motion Hand Controller and the Unity3D software. This setup enables the user to move into the virtual world where the user feels a part of the environment.
- The user will start by entering his username and can either choose to login or signup. If the user is already registered then he/she can choose to login else he/she is first asked to sign up. If the user is new then he/she has to enter their username and signup.



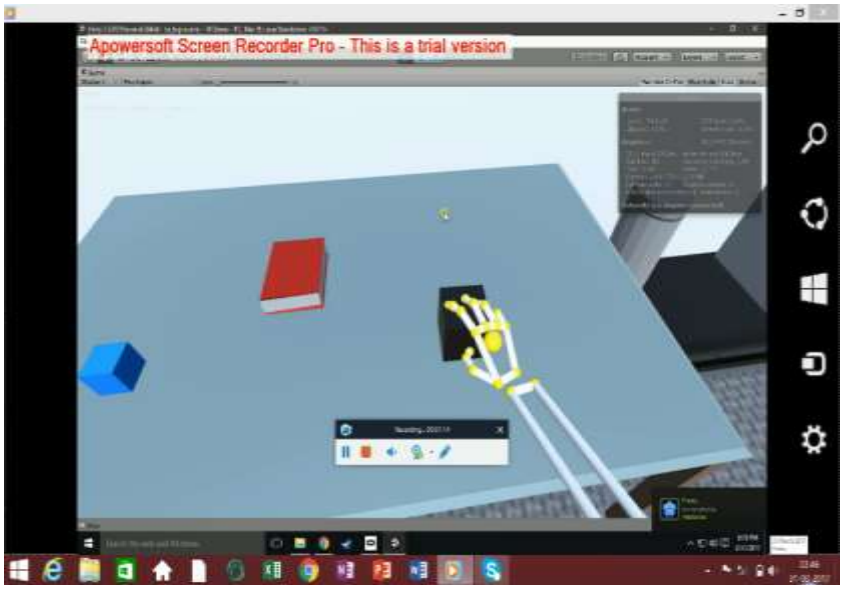
B. The User Interaction Step:

- When the user opts for signup he will be put into a virtual world when the user has to interact with the objects present in the virtual world to make his password. The user has to make a sequence pattern by displacing the objects from one position to another. This sequence pattern will be then set as his/her password.

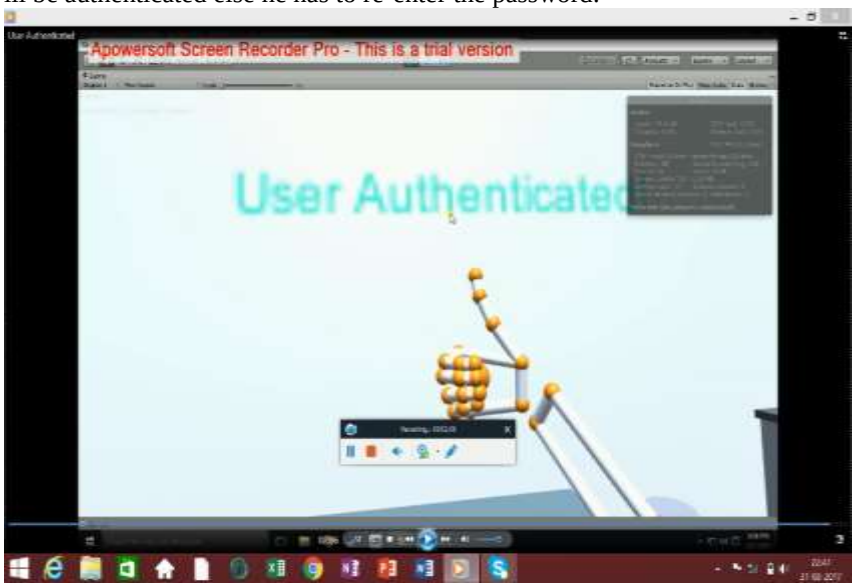
C. The Authentication Step:

- If the user has already signed up and wants to login then he can enter his/her name and opt for login. The user will then be put into the same virtual world where he/she had created the password and the user will have to enter his/her original sequence pattern of object displacement in order to authenticate himself/herself.

All rights reserved by *www.ijste.org*



– The sequence pattern and the object displacement position entered by the user will be then matched with the original password created by the user during the signup. If the sequence pattern and the displacement position matches with that entered by the user, then the user will be authenticated else he has to re-enter the password.



V. CONCLUSION

The proposed system developed will provide a new perspective when it comes to user authentication. The system can be more secure than currently existing user authentication systems. As the user would be wearing a Head Mounted Display, there is no way that any other person present around would know what the user would be doing in the virtual world, making it difficult to replicate the password. Also, the user will find the environment comforting and password remembrance easy. Even if someone wears the headset to perform the actions it would be almost impossible to perform the same action due to spawning and objects used for the password by the user. The constraints of the VR technology and Headsets may make authentication process time increase, but also gives a sense of increased security.

VI. FUTURE ENHANCEMENTS

The proposed model is an initial step to VR Passwords, the system can be further spread to mobile devices, gaming consoles because all of the newer technologies that are getting support to VR will require user authentication. Its application just doesn't curtail to pure VR systems but can also be used as a standalone security system. It can be used for Bank vaults security, Military level security for confidential data and also in VR operating systems as the first VR OS authentication system which will come up in near future

All rights reserved by *www.ijste.org*

REFERENCES

[1] Nisha Salian, SayaliGodbole, ShalakaWagh, Advanced Authentication Using 3D Passwords in Virtual World, International Journal of Engineering and Technical Research (IJETR), February 2015, Issue-2 Volume-3, ISSN: 2321-0869.
[2] Vishal Kolhe,Vipul Gunjal, SayaliKalasakar, PranjalRathod, Secure Authentication with 3D Password, International Journal of Engineering Science and Innovative Technology (IJESIT), March 2013, Issue-2 Volume-2.

All rights reserved by *www.ijste.org*