Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

Secure Authentication Mechanism for Users using Virtual Reality

S. Gayathri[1*], M. Arun Manicka Raja[2], T. Sumitha[3]

1* - Assistant Professor, Information Technology, Karpagam College of Engineering, Tamilnadu, India

2 - Assistant Professor, Computer Science and Engineering, RMK College of Engineering, Tamilnadu, India

3 - Assistant Professor, Computer Science and Engineering, RMK College of Engineering, Tamilnadu, India

Abstract:

Authentication plays a major role nowadays with the increase in digital technology and the mechanisms to break the technology. Entire world is moving towards the digital world where the data security has to be maintained. On this basis authentication system that exists now which are 2D based can be easily decoded or hacked. Hence a new mechanism using 3D concept has its scope for better authentication. Virtual Reality can be used for authenticating the user entry. This 3D based authentication provides user with utmost opportunity to increase usability by making the user to immerse in the virtual world. The user has to create a virtual password by wearing the HMD initially. The user alone will be able to identify the VR password after wearing the HMD and by providing the 3D password which was created earlier. Instead of using a password which consists of not creating a graphical pattern or typing in the password, a new Secure Authentication Mechanism (SAM) was introduced for effective and easy creation of passwords for authenticating the user using the VR technique.

Introduction:

Virtual Reality(VR) is a special environment which is created artificially with the help of computer Technology, Hardware and software which provides the user a feel of being present inside the environment. Instead of viewing a screen in front of them, user can be able to interact with 3D objects and they will be completely immersed inside the environment through two senses namely sight and sound. In addition with Virtual Reality, Augmented Reality(AR) provides a better environment with enhanced virtual objects in it. In Augmented Reality few real world objects will be present in addition to the background of the environment. Another technology called Mixed Reality(MR) where the objects can interact with the virtual objects. Instead of users seeing the 3D environment in this Virtual Reality they actually get immersed in the environment.

VR technology has been widely used in the field of Learning[14], Data visualization [13], Experimentation[8], Knowledge training[10], entertainment, aviation, medicine[9] and the military. With this emergence it is idler that the VR technology will take a good form in

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

providing secure authentication system. Various authentication schemes or algorithms are available for protecting a system [7][15][16]. Only authorized persons can have the right to use the system & its related data. Three categories of authentication system[11] [12][19] are there for mobile and computer: knowledge-based, token-based and biometric-based [5][17][18]. Token-based and Biometric-based are difficult because of the hardware setup. 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 mobile phones operating system. In this authentication using VR system, the user is immersed in an environment where the user alone will be able to interact in the environment. Objects are created virtually in this environment which is visible only for the user alone and no one else can be able to see it and user can interact through the devices connected with it. The user has to wear HMD and the hand devices for interacting with the objects. Objects will be moved and placed or multiple objects are to be connected sequentially following a pattern of selection for creating an authentication mechanism. So the possibilities of creating the object selection sequence are more and it is highly impossible to predict by external users or unauthorized persons.

In order to experience the Immersive Virtual Reality (IVR) the user has to wear the Head Mounted Displays(HMD) for effective experience. Users store their personal data on the devices and use them for social interactions; the need for seamless authentication in IVR becomes increasingly important.

Methodology:

Authentication system using knowledge base can be further classified as recall based and recognition based. The PIN, password that the user uses for authentication need to be remembered and it has to be recalled whenever needed. Recognition based authentication needs addition equipments may or may not be of high cost. In VR system the user needs HMD and other auxiliary devices for authentication. The user should wear the HMD so that the virtual environment will be visible only for that person. Many VR techniques have been proposed for rendering authentication.

Traditional Authentication:

This traditional authentication includes the normal password, PIN and pattern that are widely in use. These can be easily created and can be identified by the external user.

Augmented Knowledge Based Authentication

In this technique both Virtual Reality and Knowledge base has been augmented for authenticating. Devices that are necessary are HMD, Hand device for typing in the virtual keyboard. The user will be able to see a virtual keyboard or graphical representation for

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

providing the pattern through the HMD which is connected with the hand device and the user have to enter the password, PIN or pattern that was stored already for authentication.

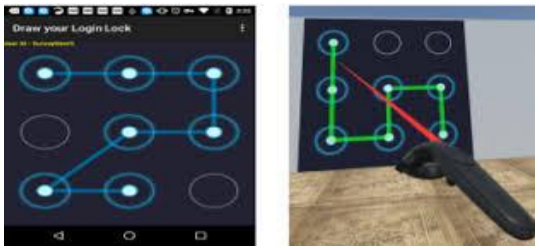
(a)  (b) 

Fig. 2.1 Knowledge Based Authentication (a) Hand device that is used for Password authentication (b) Sample of pattern authentication system

Image Recognition

In this technique the user has to wear the HMD and user will be able to see a set of images in the virtual environment. The user has to choose an image as password to get authenticated. But the problem here is any external user can guess the image with multiple tries.

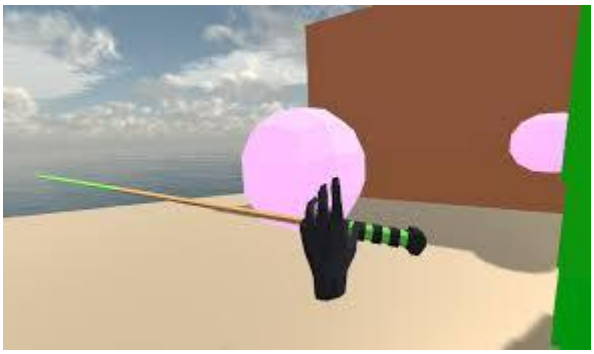


Fig. 2.2 User selecting image in virtual environment for authentication

Bio metric based authentication

Facial recognition or biometric based recognition has got its own value in the 90’s and was very popularly used authentication system since 2000. It captures the image of the user and tries to locate the facial features and that was proved as low efficient technique because an attacker can easily authenticated by putting a photo in front of the system's camera or video input, they could trigger the system artificially in authenticating an unauthorized user. With advancements made in this technique nowadays along with the face some kind of gestures are also been added for authenticating the users.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

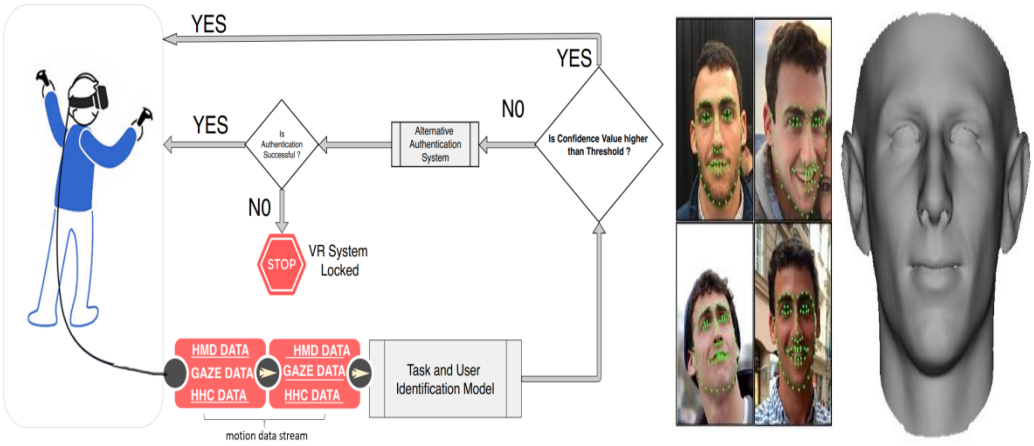


Fig. 2.3 Block diagram representing the authentication of user based on the biometric.

Object based recognition

In early days where ASCII terminals and command line interfaces were in use, usage of passwords has some value. Considering the current technology the devices connected with application are more in number and hence need a secure authentication mechanism. Thus as an alternate for providing random alphanumeric passwords which is non-obvious and nonmemorable string, the user will be provided with a set of pictures to start with and the user has to select some pictures of own leading to a meaningful and simple story for easy remembrance. So for authentication of any system the user has to choose a group of graphical icons which ranges from 10 to 20 according to the device support. When a particular icon or image was selected, other icons can be replaced in their place, expanding the number of possible combinations.

Fig. 2.4 Random object selection as password

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

Related Work:

With the availability of many authentication systems such as passwords, PIN, face, finger print etc., the user may feel comfortable. But the major drawbacks are as follows users may 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.

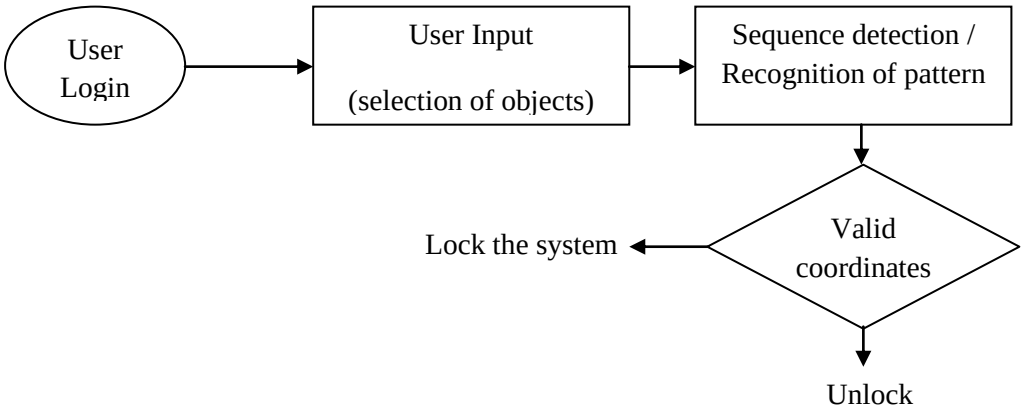
Hardware Requirement:

The major hardware that is needed to develop the authentication system includes HMD, Leap Motion and Oculus Rift DK2 which are cost effective and easy to work with the environment. Head Mountable devices provide the user the feel of being present in the environment, 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.

Working setup:

Initially user will wear the HMD and hand device for providing the input. This input is recognized by the user movements. These movements that link the objects are recognized and verified for the correctness that was previously stored in the device.

i. Login stage – User wears the HMD and provides the credentials for logging into the device
ii. User Input stage – Using the device user will provide the input which is a set of images from the environment.
iii. Recognition System – Device will remember the input and matches with the data already provided. It will verify for the coordinates of the objects from the environment that were recognized from the user input.
iv. Validation / Authentication – The system will let the user in or lock out the system after validating the input from the user. If the sequence and the coordinate does not match exactly then the user is denied to enter and access the environment.



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

Conclusion:

This system is able to provide a better authentication mechanism compared to many existing mechanism. Since the Head Mounted Display will be worn by the user, the possibility of identifying what is going on in the virtual environment by the external users is very less making it difficult to crack the authentication system. 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. By this way the security can be increased to a greater extent which may seem to be more difficult for setting up the environment and the interaction with the system initially.

References:

[1] Kapil M. Jain, Nirbhay A. Pherwani, "Virtual Reality Based User Authentication System", - International Journal of Science Technology & Engineering | Volume 4 | Issue 4 | October 2017 ISSN (online): 2349-784X

[2] 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.

[3] 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.

[4] S.Nikitha1 , Mr.L.Naresh Babu2 ,V.S.Pratyusha, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 142– 148, 2014.

[5] Rachna Dhamija, Adrian Perrig, Déjà Vu: A User Study Using Images for Authentication. In the 9th USINEX Security Symposium, August 2000, Denver, Colorado, pages 45-58.

[6] Darren Davis, Fabian Monrose, and Michael K. Reiter. On user choice in Graphical Password Schemes. In Proceedings of the 13th USENIX Security Symposium, San Diego, August, 2004.

[7] Madhumitha Ramamurthy, "Fraudster Mobile Apps Detector in Google Playstore", Journal of Computational and Theoretical Nanoscience, Vol 17, pp.1752-1757, 2020.

[8] Madhumitha Ramamurthy , Y. Harold Robinson , S. Vimal , A. Suresh, Auto encoder based dimensionality reduction and classification using convolutional neural networks for hyperspectral images, Microprocessors and Microsystems , Volume No. 79, 103280, 2020.

[9] Madhumitha Ramamurthy, Ilango Krishnamurthi, S.Vimal, Y.Harold Robinson, "Deep Learning based genome analysis and NGS – RNA LL identification with a novel hybrid model", Biosystems, Volume No. 197, 104211, 2020.

[10] Madhumitha Ramamurthy, Ilango Krishnamurthi, Sudhakar Ilango, Shanthi Palaniappan, 'Discrete Model based answer script evaluation using decision tree rule classifier', Cluster Computing, 22, 13499–13510 Nov(2019)

[11] G.Selva Marry, S. Manoj kumar "Self-verifiable Computational Visual Crptographic Protocol for Secure 2D Image Communication" International Journal of Measurement Science and Technology, Vol. 30, No. 12, 2019.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8622 - 8628
Received 16 February 2021; Accepted 08 March 2021.

[12] G. Selva Marry, S. Manoj kumar "Secure grayscale image communication using significant visual cryptography scheme in real time applications" SPRINGER International Journal of Multimedia Tools and Applications, Pages 1-20, 2019
[13] S. Manoj Kumar N.Rajkumar "SCT Based Adaptive Data Aggregation for Wireless Sensor Networks" International Journal SPRINGER - Journal of Wireless Personal Communication Volume 75, Issue 4 April 2014, Page 2121-2133
[14] S. Manoj Kumar N.Rajkumar W.Catherine "Dropping False Packet to Increase the Network Lifetime of Wireless Sensor Network using EFDD Protocol" International Journal SPRINGER - Journal of Wireless Personal Communication Volume 70, Issue 4 June 2013, Page 1697-1709.
[15]Ponmagal, R.S., Karthick, S., Dhiyanesh, B. et al. Optimized virtual network function provisioning technique for mobile edge cloud computing. J Ambient Intell Human Comput (2020).
[16]Ramamoorthy, S., Ravikumar, G., Saravana Balaji, B. et al. MCAMO: multi constraint aware multi-objective resource scheduling optimization technique for cloud infrastructure services. J Ambient Intell Human Comput (2020).
[17] Basha, A.J., Balaji, B.S., Poornima, S. et al. Support vector machine and simple recurrent network based automatic sleep stage classification of fuzzy kernel. J Ambient Intell Human Comput (2020)
[18] Balaji, B.S., Balakrishnan, S., Venkatachalam, K. et al. Automated query classification-based web service similarity technique using machine learning. J Ambient Intell Human Comput (2020)
[19]Viji, C., Rajkumar, N., Suganthi, S.T. et al. An improved approach for automatic spine canal segmentation using probabilistic boosting tree (PBT) with fuzzy support vector machine. J Ambient Intell Human Comput (2020).