International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1129-1132 www.ijaem.net ISSN: 2395-5252

3d Password Security

Dhanshri Bajaj, Poonam Antre, Prachodaya Bagade, Sahil Raut, Prof Ms.Yogita Fatangare

Department Of Information Technology
PES Modern College Of Engineering, Sppu.

Date of Submission: 15-05-2023 Date of Acceptance: 30-05-2023

ABSTRACT
The proposed system is a new scheme of multifactor authentication system. This scheme is based on a virtual three-dimensional environment which is based on existing 3 authentication factors ie Textual, Graphical, Biometric. This new system is implemented to overcome the drawbacks of existing authentication systems and act as an added security layer to the protected data. The user logs into the 3d virtual environment where there will be various intractable objects based on the 3 authentication factors. Users interacts with these objects which will generate a sequence of his own choice resulting in constructing a 3D password which can be used to secure many applications and other systems.
This password will be more secured difficult to crack as sequence will be only know to authorized user but also easy for to recall.

I. INTRODUCTION

Authentication is the process of validating who you are to whom you claimed to be. In general, there are four human authentication techniques: 1. What you know (knowledge based). 2. What you have (token based). 3. What you are (biometrics). 4. What you recognize (recognition based).

In today's digital age, the security of online information and systems is of utmost importance.Users nowadays are provided with major password stereotypes which are textual passwords, biometric scanning, tokens or cards (such as an ATM) etc.

Traditional authentication methods, such as passwords and PINs, are often inadequate and vulnerable to attacks such as phishing, brute force attacks, and social engineering. As such, there is a growing need for more robust and user-friendly authentication solutions.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) This research project proposes and evaluates a new approach to authentication, known as the 3D password security system.

Therefore we present our idea, the 3D passwords which are more customizable and very innovative way of securing your data. The 3d password Security system is a multifactor authentication system which is based on the three authentication factors given by 1) Textual 2) Graphical 3) Biometrics. It is the combination of the existing system which allows it to be more powerfull and harder to crack. 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 based authentication.

The 3D paswords will have a large number of possible actions and interactions towards every object inside the 3D virtual Environment.

II. LITERATURE SURVEY

[1.] 3D Password: A Survey of Authentication Techniques by Tejal Kognule, Yugandhara Thumbre, Snehal Kognule(2012): This paper propose and evaluate our contribution which is a new scheme of authentication. This scheme is based on a virtual three-dimensional environment design & develop more user friendly & easier authentication scheme . Now the passwords are based on the fact of Human memory.

[2.] 3D Password – More Secure Authentication Scheme by Tejal M. Kognule, Monica G. Gole, Priyanka T. Dabade, Sagar B. Gawde (2014): This paper provides a survey of 3D password authentication techniques, including graphical password schemes, biometric techniques, and smart card-based authentication.

[3.] Study on Three Dimensional (3D) Password Authentication system by Nayana S, Dr. Niranjanamurthy M, Dr. Dharmendra Chahar (2016):

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1129-1132 www.ijaem.net ISSN: 2395-5252

This paper proposes a system to build authentication system using different authentication factor. The main intention is to give user the freedom to select whether the 3D password will be simply Recall, Recognition, Graphical, Biometric, or combination of any two techniques or more

[4.] 3D PASSWORD AUTHENTICATION by Mrs. Ashwini B P, Ms. Bhumika J, Ms. Chinmaye T S, Mr. G M Akshay Bhat, Mr. Naveen Kumar N (2019): This paper proposes system is to build a multi-feature, multi-password safe authentication scheme which combines all the several authentication techniques into a solitary 3 Dimensional virtual environment that results into a larger password space which is more secure. . The system uses a 3D grid of cells to generate a password, making it resistant to various attacks.

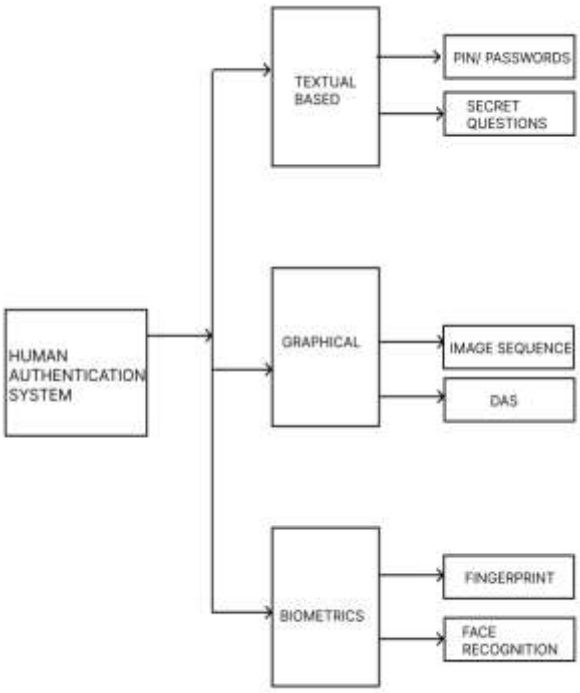

Fig.1. THE HUMAN AUTHENTICATION SYSTEMS

III. EXISTING SYSTEM

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. 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. Smart cards or tokens can be stolen. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The 3D password is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. User have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more.

DRAWBACKS IN EXISTING SYSTEM

Textual Passwords: Textual passwords should be easy to remember at the same time hard to guess. But if a textual password is hard to guess then it will also be hard to remember.

Graphical Passwords: They are based on idea that users can recall and recognize pictures better than words. Some graphical schemes require a long time to perform. They are vulnerable to shoulder surfing attacks.

Biometrics: Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition,iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometrical

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1129-1132 www.ijaem.net ISSN: 2395-5252

recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

IV. METHODOLOGY

The 3D password is a multi factor 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. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

For example, the user can enter the virtual environment and type something on a computer that exists in (x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user's 3D password.

Virtual objects can be any object that we encounter in real life. 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 speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password.

We can have the following objects:
1) A computer with which the user can type;
2) A fingerprint reader that requires the user's fingerprint
3) A biometric recognition device;
4) A light that can be switched on/off;
5) A television or radio where channels can be selected;
6) A book that can be moved from one place to another;
7) Any graphical password scheme;
8) Any real life object;
9) Any upcoming authentication scheme.

The action toward an object (assume a fingerprint recognition device) that exists in location (x1, y1 , z1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x2 , y2 , z2), where x1 = x2 , y1 = y2 , and z1 = z2 . Therefore, to perform the legitimate 3D password, the user must follow the same scenario performed by the legitimate user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

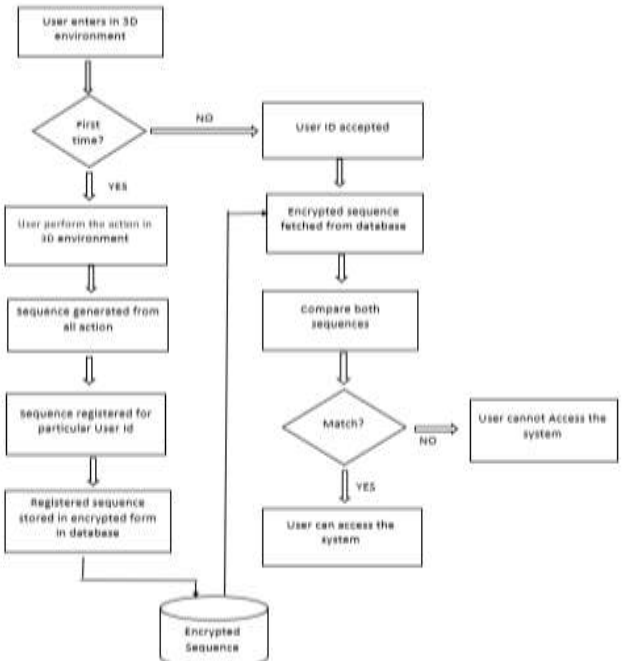

Fig. 2. ARCHITECTURE DIAGRAM

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1129-1132 www.ijaem.net ISSN: 2395-5252

V. 3D PASSWORD APPLICATION

The 3D password can have a password space that is very large
compared to other authentication schemes, so the 3D password's main application domains are protecting critical systems and resources.

1. Critical server many large organizations have critical servers that are usually protected by a textual password. A 3D password authentication proposes a sound replacement for a textual password.
2. Nuclear and military facilities such facilities should be
protected by the most Powerful authentication systems. The 3D password has a very large probable password space, and since it can contain token, biometrics, recognition and knowledge Based Authentications in a single authentication system, it is a sound choice for high level security locations.
3. Airplanes and jet fighters Because of the possible threat of
misusing airplanes and jet fighters for religion, political agendas, usage of such airplanes should be protected by a powerful authentication system.In addition, 3D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system needs. A small virtual environment can be used in the following systems like

1) ATM
2) Personal Digital Assistance
3) Desktop Computers & laptop logins
4) Web Authentication
5) Security Analysis

VI. CONCLUSION :

In conclusion, the 3D password security system represents an innovative and promising approach to authentication and security. Through rigorous evaluation and analysis, our research has demonstrated the system's feasibility and effectiveness in terms of security and usability. The system offers a secure and user-friendly means of authentication, leveraging a personalized 3D virtual environment and biometric authentication to provide a high level of security. The potential for integration with other authentication methods and real-world applications makes the 3D password security system a compelling area for future research and development. Ultimately, our project offers a valuable contribution to the field of information security, paving the way for further advancements in this critical area.

REFERENCES:

[1]. Department of Computer Science and Engineering, Siddaganaga Institute of Technology (IJSDR) ISSN: 2455-2631 Special Issue - 2019.
[2]. [2] International Journal of Advanced Research in computer and communication Engineering (IJARCCE) ISSN No:-2319-5940 Volume 5, Issue 2, Oct-2016.
[3]. International Conference on advances in communication and computing technologies (ICACACT) in 2012.
[4]. International Journal of Engineering research and technology (IJERT) ISSN: 7278-0181: Volume 3, Issue 2 in Feb 2014.