iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on the Use of 3D Password in Security

Paruthi Ilam Vazhuthi P[#1], Geetha M[*2], Parthiban S[#3]
[#]Department of ECE, V.R.S College of Engineering and Technology
[*]Department of EEE, V.R.S College of Engineering and Technology

Abstract— Passwords play an important role in various computing applications like ATM machines, internet services, windows login, and authentication in mobiles etc. There are many authentication techniques are available, Such as textual password, Graphical password, biometric password and token based password etc. But each of this individually having some advantages & disadvantages. To overcome the Drawbacks of existing authentication technique we propose a new improved authentication technique called as called as 3D password. The 3D password is a multifactor authentication scheme. The 3D passwords are more customizable and very interesting way of authentication. The 3D password can combine most existing authentication schemes such as knowledge based passwords, graphical passwords, and various types of graphics into 3D object virtual environment. The proposed authentication scheme is hard to break & easy to use. Finally, some suggestions are given for future research.
Keywords—passwords, authentication, 3D Password, multifactor authentication, 3D object virtual environment.

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.
Today, authentication is the principal method to provide system security by the different authentication algorithm and the most common and convenient method is password authentication. Authentication allows only authorized persons can have right to access or handle that system & data related to that system securely. The conventional password scheme is an oldest and most widely used algorithm in many applications such as ATM Banking client server architecture and laptop etc..There are many authentication algorithms are available but having some drawbacks.
The process of authorization is distinct from that of authentication. Whereas authentication is the process of verifying that "you are who you say you are", authorization is the process of verifying that "you are permitted to do what you are trying to do". Authorization thus presupposes authentication. For example, a client showing proper identification credentials to a bank teller is asking to be authenticated that he really is the one whose identification he is showing. A client whose authentication request is approved becomes authorized to access the accounts of that account holder, but no others.

II. AUTHENTICATION METHODS OVERVIEW

Generally, four types of authentication schemes are available such as:
A. Knowledge based
B. Biometric based
C. Token based

Knowledge based schemes are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [1].

Text based passwords are strings of letters (uppercase and lower case), symbols and digits, which are easy to use but such a password can be easily predictable by a unauthorized users. Most users tend to choose short or simple passwords which are easy to remember and has less security. Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack, shoulder surfing attack, spyware attack and social engineering attack etc.. Today users have many passwords for personal computers, social

networks, E-mail, and more.

Graphical password schemes have been proposed as a possible alternative to text -based schemes. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices [1].

Biometrics is also used as authentication procedure in which the recognition is based upon image processing. In this case to verify an image, it is first preprocessed to extract features from it and then the image based on these extracted features is matched with the database. There are many types of biometrics based authentication.

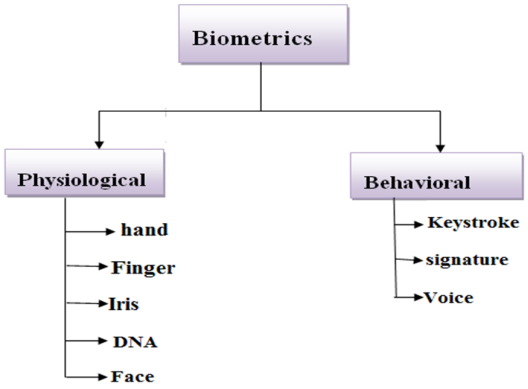


Fig.1 Biometric authentication methods

Fingerprints are imprints formed by friction ridges of the skin and thumbs. They are generally used for security based application because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9x1015.However, manual fingerprint verification is so tedious, time consuming and expensive that it is incapable of meeting today's increasing performance requirements [7].

III. 3D PASSWORD

A 3D password is a multifactor authentication scheme that combines recognition, recall, and token based and biometric based authentication in one authentication system. The 3D passwords are more customizable and very interesting way of authentication. 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 combination and sequence of user interactions that occur in the 3D environment. It becomes much more difficult for the attacker to guess the user's 3-D password.

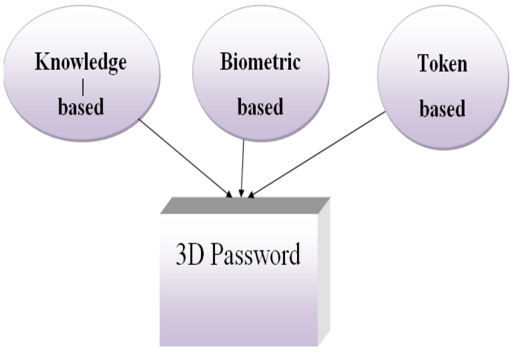


Fig.2 3D password

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The 3D password can combine most existing authentication schemes such as knowledge based passwords, graphical passwords, and various types of graphics into 3D object virtual environment. The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical password as part of their 3D object password. On the other hand users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password. Moreover user who prefers to keep any kind of biometric data private might not interact with object that requires position information. Therefore it is the user's choice and decision to construct the desired and preferred 3D object password [3].

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate , moving in 3D virtual environment to create a password which is based on both the schemes[2].the virtual objects in a 3D environment can be any object we encounter in real life:

A. A computer on which the user can type
B. A fingerprint reader that requires users fingerprint
C. A paper or white board on which user can type
D. An Automated teller(ATM) machine that requires a token
E. A light that can be switched on/off
F. A television or radio
G. A car that can be driven
H. A graphical password scheme

IV. 3D VIRTUAL ENVIRONMENT

3-D virtual environment affects the usability, effectiveness, and acceptability of a 3-D password system and reflects the administration needs and the security requirements.

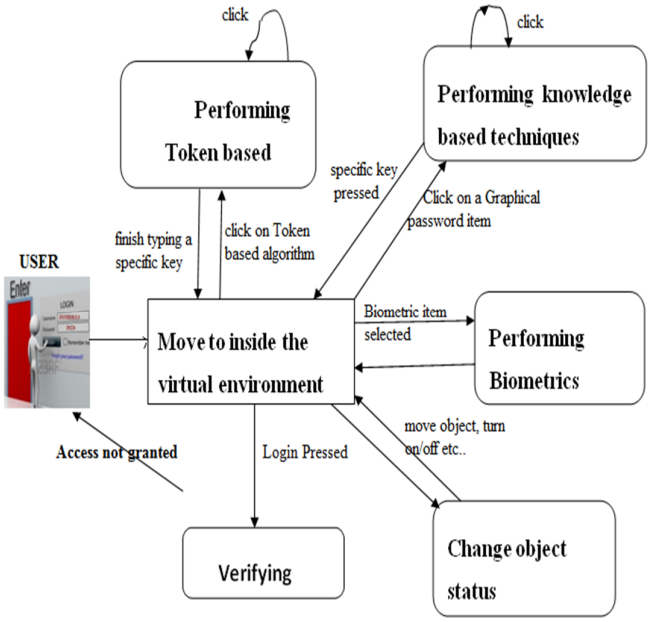


Fig.3 3D authentication procedure

A. Design Guidelines

The design of 3D virtual environments should follow these guidelines

1) *Real Life Similarity:* The prospective 3D object virtual environment should reflect what people are used to seeing in real life. Possible actions and interactions toward virtual objects should reflect real life situations. Object responses should be realistic. The target should have a 3D object virtual environment that users can interact.
2) *Three Dimensional Virtual Environment Size*: A large 3D virtual environment will increase the time required by the user to perform a 3D object password. A large 3D object virtual environment can contain a large number of virtual objects with high time complexity but the small 3D object virtual environment can contain a less number of virtual objects with low time complexity.

3) *Number of objects and types:* object types represent the response of the object and selecting the right object response types and the number of objects affects the probable password space of a 3D object password
4) *System Importance:* the number of objects and object type reflects the importance of the protected system

3D password is a authentication technique which can be implemented in 3D virtual environment. As every project having problem statement which is relation with mathematical concepts like feasibility study, complexities, set theory etc. This section of paper will explain almost all the mathematical concepts applied while creating 3D password schemes [2].

B. Parameters Calculations

1) Time complexity: Time complexity of the 3D password algorithm can be expressed as,

$$\textbf{Time complexity} = A^m + B^n$$

Where,

A= Virtual 3D Environment Plotting
B= Algorithmic processing
M=time required for communication
N= algorithm processing time

2) Space Complexity

Each point in the 3D environment will have 3 Co ordinate values. Any point from 3D virtual environment is represented in the form of (X, Y, Z).Where X, Y & Z are the coordinate values stored for particular point. We are storing three co-ordinate values of each point such as (x1, y1, z1). There for space complexity of proposed system is n^3.

V. PASSWORD ATTACKS

Some of the attacks to authentication scheme is listed below,

A. Brute Force attack:

In this type of attack, an attacker tries all possible combination of password apply to break the password. Brute force attacks are very time consuming. Brute force attack is depends on cost requirement and time required to login.

B. Key Loggers:

Key loggers attack is similar to the login spoofing attack. They are also called the Key Sniffers. The key logger is software program which monitor the user activity by recording each and every key pressed by the user.

C. Shoulder Surfing:

Shoulder Surfing is an alternative name of “spying” in which the attacker spies the user’s movements to get his/her password. In this type of attack, the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed.

D. Replay Attacks:

The replay attacks [10] are also known as the reflection attacks. It is a way to attack challenge response user authentication mechanism (Same type of protocols by each sender and receiver side for challenge and response). The method for this type of attack is that the attacker first enters his/her name in first login connection. To authenticate the user, the receiving device sends the challenge to the sender (in this case attacker). The attacker opens another login at the same time with its own valid user name and replies the receiving device as challenge of previous connection. The receiving side accepts the challenge and responds to it. The attacker then sends back that response through the account to be hacked and thus it gets authenticated. Then the attacker gets access to that account.

E. Timing attack:

Timing attack is based on how much time required completing successful sign-in using 3D password scheme. Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our 3D password scheme is designed more securely, these kinds of attacks are not easily possible on 3D Password & also not much effective as well.

F. Advantages

The advantages of the 3D passwords are listed below,

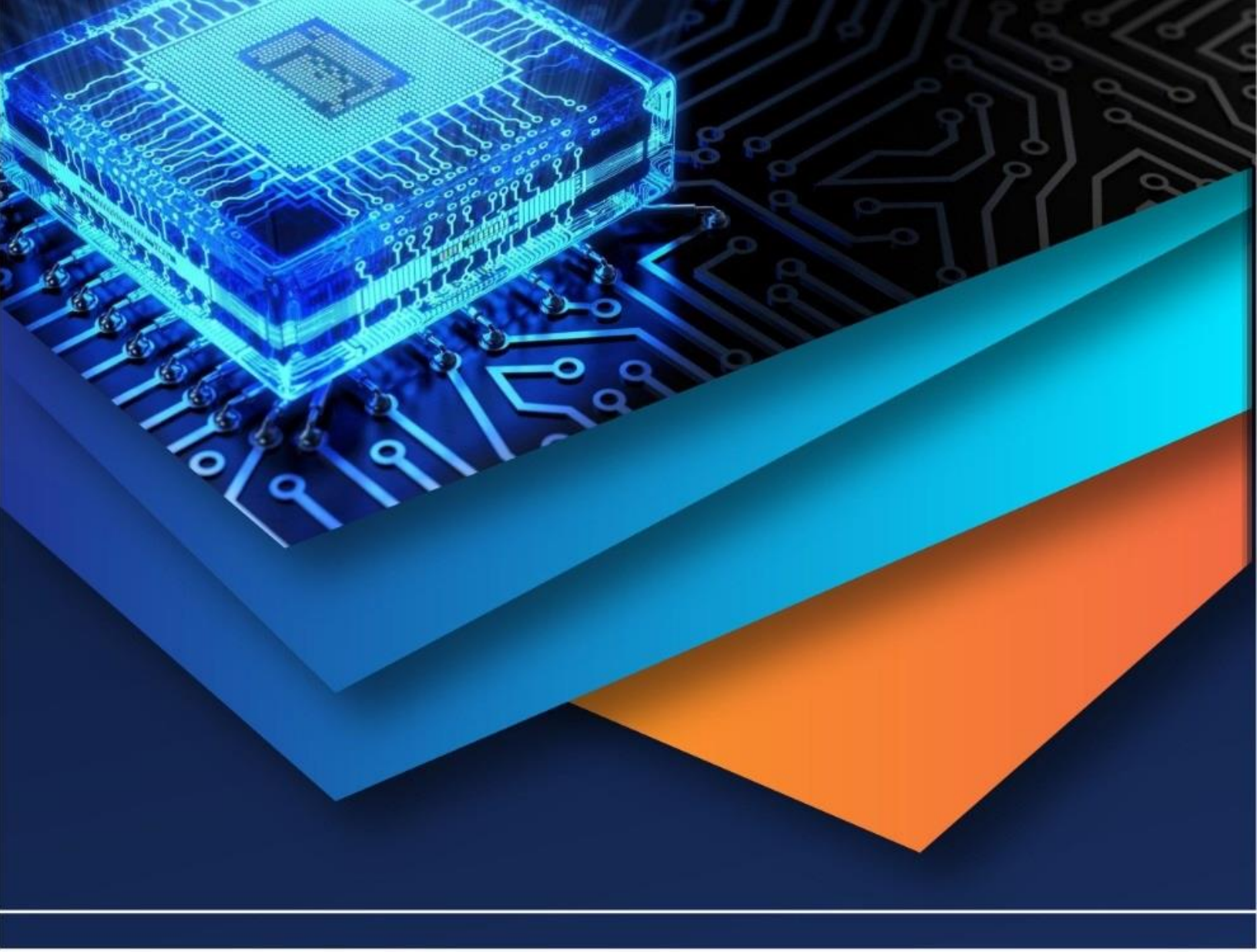
1) *Flexibility:* 3D Passwords allows Multifactor authentication biometric, textual passwords can be embedded in 3D password technology.
2) *Strength:* This scenario provides almost unlimited passwords possibility.
3) *Ease to Memorize:* can be remembered in the form of short story.
4) *Respect of Privacy:* Organizers can select authentication schemes that respect users privacy.

VI. CONCLUSION

The authentication can be improved with 3d password, because the un- authorized 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 no of steps and a particular procedure Added with biometrics and token verification this schema becomes almost unbreakable. Currently available schemes include textual password and graphical password .But both are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use [6]. The 3-D password is a multifactor & multi password authentication scheme that combines these various authentication schemes. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes. Due to which passwords space increases. It is the user‘s choice and decision to construct the desired and preferred 3-D password. The 3D password is still new & in its early stages [6].

REFERENCES

[1] Xiaoyuan Suo Ying Zhu G. Scott. Owen, “Graphical Passwords survey,
[2] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod” Secure Authentication with 3D Password “ International Journal of Engineering Science and Innovative Technology (IJESIT),vol.2,issue2, pp 99-105, march2013.
[3] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, ―3D password‖, International Journal of Computer Applications (IJCA), 2012.
[4] S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.
[5] Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999..
[6] Alsulaiman, F.A.; El Saddik, A., "Three for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
[7] Jay Merja, Sunny Shah “Simplified Secure Wireless Railway for Public Transport” 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, pp 77-82.
[8] Adams, M. A. Sasses, and P. Lunt. “Making passwords secure and usable”. In HCI 97: Proceedings of HCI on People and Computers, pp.1-19, London, UK, 1997.
[9] P. C. Van Oorschot, A. Salehi-Abari, and J. Thorpe. “Purely automated attacks on passpoints-style graphical passwords”. IEEE Trans. Info. Forensics and Security, 5(3):393-405, 2010.
[10] P. C. Van Oorschot and J. Thorpe. “On predictive models and user-drawn graphical passwords”. ACM Transactions on Information and System Security, 10 (4):1-33, 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY