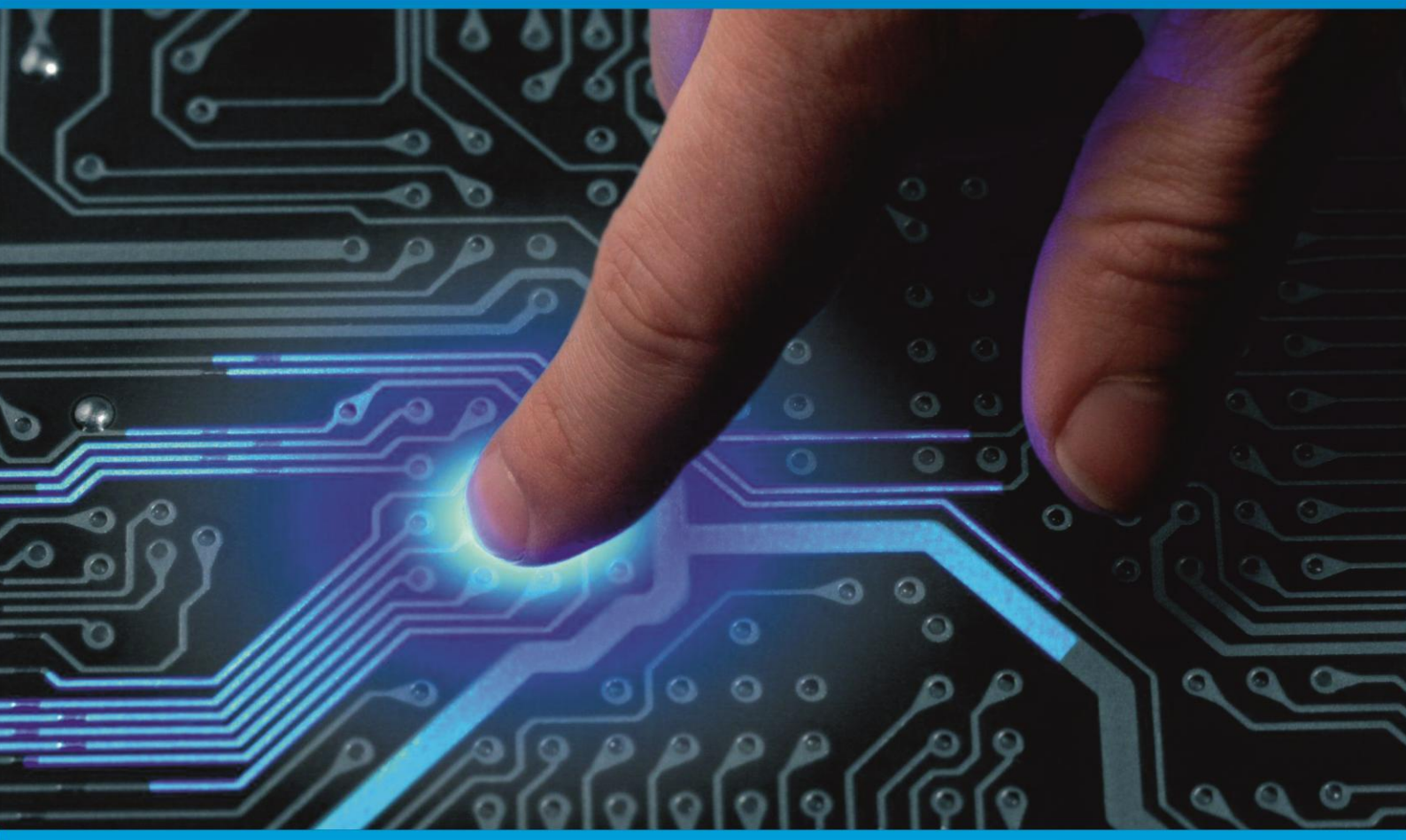
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 12, December 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812020 |

Design of 3-Dimensional (3D) Password: A Multi-factor Technique

Kartiki.Vanire[1] , Mrs. Rama Bansode[2]

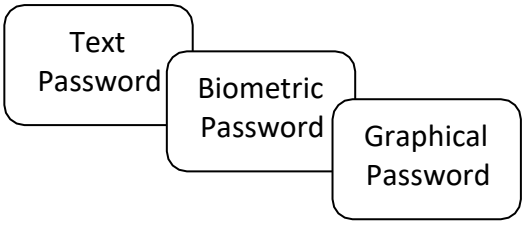
P.G. Student, Department Master of Computer Application, Modern College of Engineering, Shivaji Nagar, Pune, India[1]

Associate Professor, Department of Computer Application, Modern College of Engineering, Shivaji Nagar, Pune, India[2]

ABSTRACT: Authentication of any system means providing a security thereto system. There are much more authentication techniques like textual, biometrics. This type of textual password commonly follows an encryption algorithm to supply security. Each of these techniques has few limitations and drawbacks. To overcome the drawbacks, a replacement authenticate technique is now available. This technique isnothing but as 3D Password, which is multi-factor and multi-factor authentication technique. The most important a thing of 3D Password is virtual environment which contains the interface which looks like a real time present environment, but is not actually a real time environment. 3D password is safer technique of authentication as compared to other techniques because it's difficult to interrupt and straightforward to use. The benefit of the 3D password is that combine the authentication of existing system and provides high security to end-users. this paper focuses on the ways to create or form 3D password and therefore the design principles for 3D password.

I.INTRODUTION

There are four authentication techniques available:
a) Knowledge Base: Textual password is best example for knowledge domain technique.
b) Token Base: Any swipe card (ATM card)is example of token base authentication technique.
c) Recognition Base: Graphical password or face identification are examples of recognition base technique.
d) Biometrics Base: Thumb or finger impression is good example of biometrics base authentication technique.



Authentication of an individual's identity may be a very old but still a challenging problem. There are 3 common ways or methods which are used for authentication. First one is predicated on what a person's possession like keys, identity cards, identity number etc. Second way of authentication is predicated on what an individual knows or remembers knowledge like passwords, personal identification number etc. Third way of the features of a human being like biometrics. There are chances that the things which are under possessions could also be lost and knowledge could also be forgotten. But this is not the thing with biometrics. Limitations of those three methods are often overcome if we make use of all three methods during a single system. The main drive picture of biometrics based authentication getting more and more popularity as day passes. The purpose of employing a biometrics is to supply a mechanism to acknowledge an individual with the assistance of his/her own features and to remove the main use of much inconvenient ways of recognition which are supported ID card, password, physical keys etc. This proposed system could be a more factor based authentication scheme, and canhave combination of all existing authentication schemes into one 3D virtual environment. This 3D virtual environment has many objects or things with which the user can interact or communicate. Here used three layer methods which has texture, biometric and graphical password.

International Journal of Innovative Research in Computer and Communication Engineering

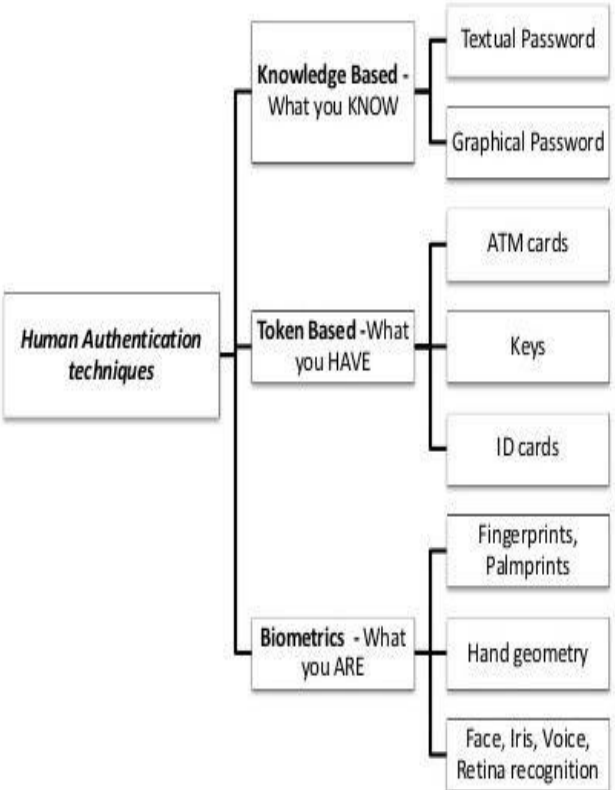
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812020 |

II.RELATED WORK

The theatrical increase of computer usage has given rise to several security concerns. One key security concern is authentication, which has process of validating the user.In general, human authentication techniques are often classified as:



Textual based: Recall based practices require the user to breed a secret again that the user twisted before. Identification based methods order the user to classify and be known of the secret or part of that the user carefully chosen before. One of the foremost common recall based schemes utilized in the mainframe world is textual passwords. One major disadvantage of the textual password is its too inconsistent within the choice of passwords that are easy to remember and at the same while are hard to guess.

Graphical based: this system is for those sort of users, who can recall and distinguish films better than words. Some of the graphical password strategies takes too much time for performing. Moreover most of the graphical password strategies has been identified as shoulder surfing attacks. Therefore, presently many graphical password techniques are still in their examine phase and could have more enhancement's and usefulness studies.

Token based: In the structure of banking authentication, it not only requires a knowledge based authentication systems like textual based and Graphical based systems but also token based system is required. In present, many reports have shown that tokens are vulnerable to loss, fraud or theft by using simple techniques. Any ATM cards, swipe card are samples of token based authentication systems.

Biometric based: Various Biometric schemes are proposed; Finger-Prints, Face-Recognition, Voice- Recognition, Retina-Recognition and Palm-Prints are all different biometric systems. But all are havingitsown limitations and disadvantages supported several factors like acceptability, uniqueness, and consistency. One of the main drawbacks of applying biometrics is its inappropriateness upon a user's personal characteristic. When system uses thumbnail expression of users for authentication purposes in real time this is the good example of biometric system. When the system register the new users, it'll initially take the thumbnail expression of latest user using thumb recognition device and store it in image format in system Database record. Next time when the user login into the system, user will need to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812020 |

give the thumbnail expression by using thumb detection device. Later the system validates that image and checks if it's same or not.

III.PROPOSED METHOD

In this section, here proposed as multilayer authentication scheme that mixes the benefits of three different authentication schemes. We attempt to justify the wants of current security issues for authentication on different platforms. The new scheme should provide secrets that are easy to recollect and really difficult for intruders to guess.

Layer1
At the first layer of authentication we used texture password as initially as recall method. This layer is predicated on knowledge level or we will say what the user knows. Passwords are used with computers since the earliest days of computing. Basically it's a LOGIN command that requested a user password. "After typing PASSWORD, the system turns starts working. To log in, at the client side is ensured by the utilization of text password, which text password has got to be entered by ensuring by applying of special characters. Therefore, security at Layer1 is ensured by use of text password which may be a usual approach with normal login scheme.

Layer2
At the second layer of authentication here used concept of biometric password as face recognition scheme. This is recognition based scheme because it require user to select and memorize a number of a given set of images of their face. At the time of authentication system must need to match face of user with multiple images of their face taken in several angles and distances.

Layer3
At the third layer of authentication here used concept of graphical password scheme for final access of the system. Graphical password is predicated on the concept that users can recall and recognize pictures quite words. Graphical password scheme were

IV.SECURITY ANALYSIS

To analyses and understand how far our authentication scheme is secure, we consider all possible attack techniques. We need to review whether our proposed authentication scheme is immune against such attacks or not. So, if the proposed authentication scheme isn't immune, we then need to find the countermeasures that prevent attacks which happens presently. In this section, we attempt to cover most possible attacks and whether the attack is valid or not. Moreover, we try to analyses system performance to assure for these attacks one by one as:
Brute force attack
In the first layer where texture based passwords taken for authentication have space to get all combinations of character and numerals. But it's difficult to try to this attack on graphical passwords .We believes it's harder for this attack to succeed for next two layer and their all efforts won't work on biometric and graphical passwords. Generally recall based password is safer then recognition based techniques when it involves brute force attack.

V.CONCLUSION

Basically introduced to decrease the human memory burden to recollect text-based password. During a virtual visual environment a specific pattern of images or clues can easily be recognized. In some cases of graphical passwords are susceptible only thanks to shoulder surfing attacks, where an attacker can observe or record the valid user graphical password by camera. We tried to use a virtual environment where multiple objects are there, which require to be organize during a particular manner can only authenticate the user. The coordinates of mixing objects are wont to create variety by calculating the typical distance between theses coordinates. If we've three objects in one environment as p1(x1, y1), p2(x2, y2) and p3(x3, y3) and their distances are d1, d2 and d3 then value are going to be average of d1, d2 and d3. Within the market most of the graphical password are within the research phase and need more enhancement and usefulness studies to develop them within the market

REFERENCES

1. Alsulaiman, FF.A. El Saddik, A., "Three- for Secure, "IEEE Transactions on Instrumentation and measurement", vol.57, no.9, pp 1929-1938.Sept. 2008

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812020 |

2. ZhiLii, Qibin Sun, Yong Lian, and D. D. Giusto, An association-based graphical password desigu immune to shoulder surfing attack',
3. International Conference on Multimedia and Expo (ICME), IEEE.2005
4. Nari Kannan; "How to catch some next big things and lose others" Online: http://blogs.ittoolbox.com/bi/entrepreneur/archives/000574.asp March 2004.
5. Sobrado, L and Birget, J. "Passwords of graphical", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 200

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details