iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6408

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

3D Password Authentication System

Chandan A M[1], Dr. A S Poornima[2]
[1]*Student,* [2]*Assistant Professor, Department of CSE, Siddaganga Institute of Technology, Tumkur, India*

Abstract: ***Authentication is a process of validating who are you, to whom you claimed to be or a process of identifying an individual, usually based on a username and password. It is one of the most important security service provided to 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 & secure but having some drawback. Many authentication algorithms are available some are effective & secure but having some drawback. The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. In other words. The 3D Password scheme is a new authentication scheme that combine RECOGNITION + RECALL in one authentication system. 3D passwords are flexible and they provide unlimited passwords possibility. They are easy to Memorize and can be remembered in the form of short story.***

I. INTRODUCTION

The authentication system which we are using is mainly very light or very strict. Since many years it has become an interesting approach. With the development in means of technology, it has become very easy for others to hack someone's password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the same number coming is rare. We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. But there are many weaknesses in current authentication systems.

A. Ideally There Are Two Types Of Authentication Schemes Are Available According To Nature Of Scheme & Techniques Used, Those Are

1) *Recall based:* In this authentication technology. user need to recall or remember his/her password which is created before [1]. Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. This technique is commonly used all over the world where security needed.
2) Recognition based: In this user need to identify, recognize password created before.

Recognition based authentication can be used in graphical password. Generally, this technique is not use much more as Recall based is used.

When a person uses textual passwords, he likely chooses meaningful words from dictionary or their nick names, girlfriends etc which can be cracked easily. And if a password is hard to guess then it is hard to remember also. 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. Graphical passwords can also be used. Their strength comes from the fact that users can recall and recognize pictures more than words. Token based systems can also be used as way of authentication in banking systems and for entrance in laboratories. But smart cards or tokens are susceptible to loss or theft. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. Many years back Klein performed tests and he could crack almost
15 passwords per day. As the technology has changed many fast processors and tools are available on internet it has become very easy. So in this project, we have introduced 3-d password scheme.

The proposed system is a multi-factor authentication scheme. It can combine all existing authentication schemes into a single 3D virtual environment .This 3D virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user's 3D password [1]. The 3D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3D 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 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 biometric information. Therefore it is the user's choice and decision to construct the desired and preferred 3D password.

II. LITERATURE SURVEY

The existing authentication techniques includes textual passwords, token based passwords, biometrics and recognition based passwords.

A. Textual Passwords

The most commonly used password now a days is textual password, these are the passwords that appear in the form of the text, the meaning full words taken from the dictionary, user names etc forms the text.

On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack, which make textual passwords easy to break, can be copied easily by the hacker and vulnerable to dictionary or brute force attacks.[3]-[2]

B. Token Based Passwords

These are the passwords that appear in the form of token such as combination of numbers, jumbled letters , symbols etc. ATMs, laboratories entrances uses token based passwords as a mean of authentication.

On the other hand, smart cards or tokens are vulnerable to loss or theft and the user has to carry the token whenever the access is required and there is also a chance that users can forget or may loose his token.[3]-[2]

The drawbacks of the textual password and token based passwords leads to new authentication called graphical passwords.

C. Graphical Passwords

These are the passwords that comes from the fact that users can recall and recognize pictures more than words.

Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate users graphical password by camera. [3]-[2]. The drawbacks of the textual password, token-based passwords and graphical passwords leads to new authentication called Biometrics.

D. Biometrics

Biometrics means what you are. These are the passwords that appear in the form of thumb impressions, natural signatures etc. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity.

On the other hand, hackers may use some chemicals and they can easily hack the thumb impression of the user, also some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning), as the age goes on, the biometrics may slightly vary.[3]-[2]

III. PROPOSED SYSTEM

The proposed system is a multi-factor authentication scheme which combines the advantages of other authentication schemes. Users can choose whether the 3D password will be only recall, biometrics, recognition, or token based, or a combination of two schemes or more. This choice of selection is necessary because users are different and they have different requirements. So, for surety of high user acceptability, the user's freedom of selection is essential.[4]

A. The Following Are The Objectives In Proposed Scheme

1) The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.

2) The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.

3) The new scheme provides secrets that can be easily revoked or changed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

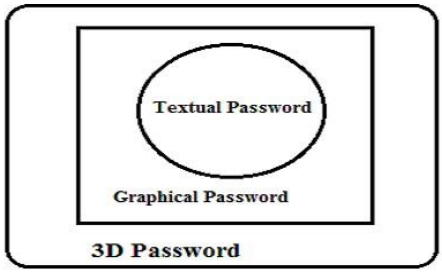


Fig.1 3D Password as Multifactor Authentication

IV. DESIGN AND IMPLEMENTATION

1) *Registration Phase:* User registers into the 3d environment by doing textual authentication. Once he logs in he interacts with the 3d environment , he then selects the images which he want. His interaction is stored in the database. User provides the textual passwords, enters into the 3d virtual environment. The interactions of the user with these objects in the 3d environment are stored by the database as users 3d password as shown in Fig 3.

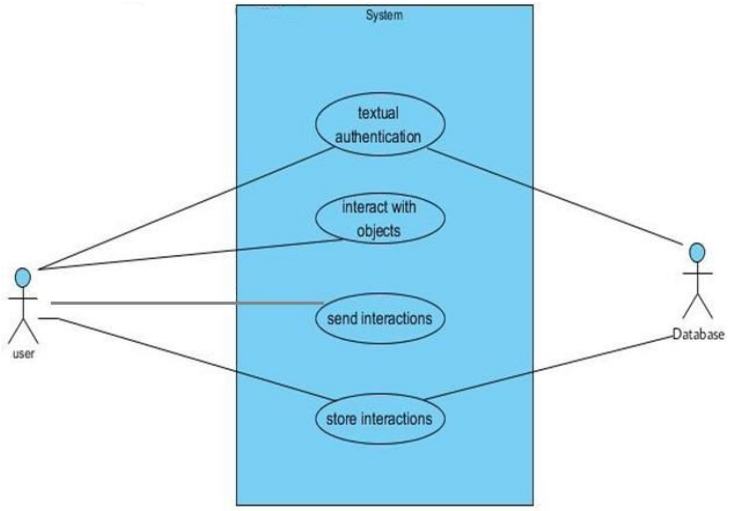


Fig 3. Use Case Diagram Registration Phase

2) *Login Phase*: If the user has already registered, he selects login phase. Once he logs in he does the same which he had done during registration phase If the user selects the same image which he had selected during registration, the password matches else the system shows invalid password as shown in Fig 4.

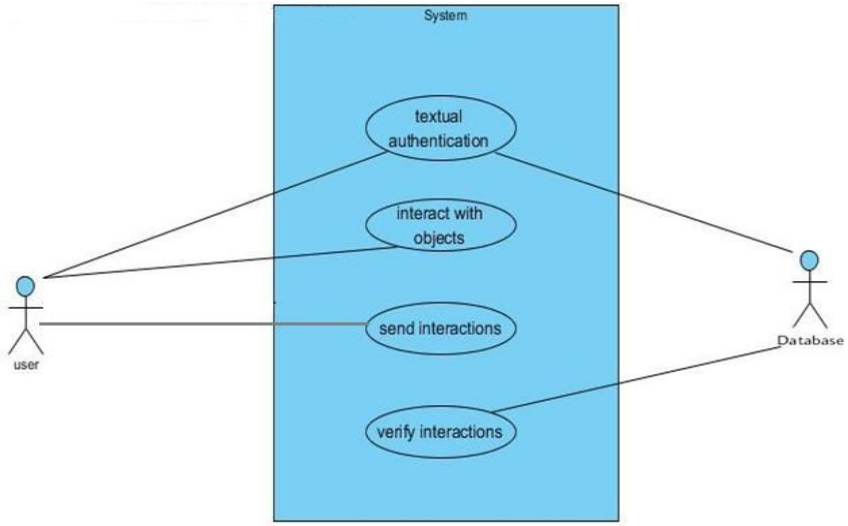


Fig 4. Use Case Diagram Login Phase

V. RESULTS

In this phase the new user need to register first by giving both Textual password and 3D password. To register, Name, Email-id and Password fields are mandatory. It Generates the unique Id to the particular users which used in the time of login. After clicking the NEXT button it will move on to the phase where we need to SET the 3D password other words it will move on to the phase where we get the 3D virtual environment to set the password as shown in Fig 5.

VI. CONCLUSION AND FUTURE WORK

In the existing system, Textual passwords and token-based passwords are the most common user authentication designs. Many other designs are also there like graphical password, biometric authentication design etc. which are used in different fields. The main goal of this project is to have a design which has a huge password space and which is combination of any existing, or upcoming, authentication designs into one design.

While using 3D password, have the choice to construct their 3D password according to their needs and their preferences. A 3D password's probable password space can be reflected by the design of the three-dimensional virtual atmosphere, which is designed by the system administrator. The three- dimensional virtual atmosphere can contain any entities that the administrator feels that the users are familiar with.

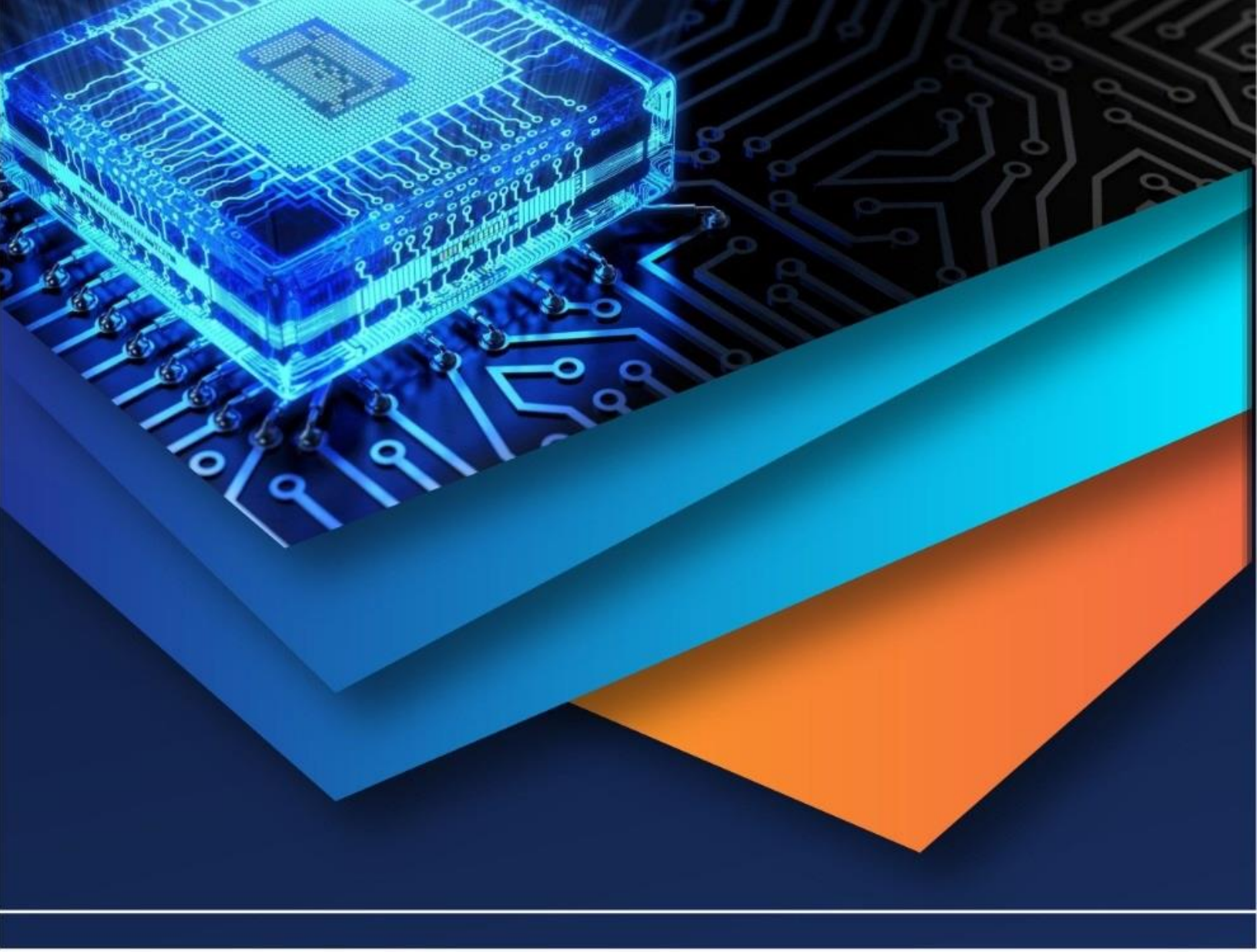
The 3D password is just introduced means it is in its childhood. A study on a large number of people is required. We are looking at designing different three-dimensional virtual atmospheres that contain entities of all possible authentication designs and also to develop the same in the form of an Android app.

A. The 3D password's main application domains are:

1) Protecting critical systems and resources
2) Critical Servers
3) Nuclear Reactors & military Facilities
4) Airplanes and missile Guiding
5) A small virtual environment can be used in the following systems like ATM, Laptops and PCs.

REFERENCES

[1] S Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
[2] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, 3D password, International Journal of Computer Applications (IJCA), 2012
[3] V.Sindhuja, S.Shiyamaladevi, S.Vinitha-"A Review of 3D Protected Password" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, pp3995-4001, 2016.
[4] Ms. Swati Bilapatte, Prof. Sumit Bhattacharjee "3D Password: A novel approach for more secure authentication" International Journal of Computer Science & Engineering Technology, ISSN: 2229 -3345, pp150-156, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY