ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
ICRITCSA
M S Ramaiah Institute of Technology, Bangalore
Vol. 5, Special Issue 2, October 2016

Study on Three Dimensional (3D) Password Authentication system

Nayana S[1], Dr. Niranjanamurthy M[2], Dr. Dharmendra Chahar[3]

Student, Department of Computer Applications, MSRIT, Bangalore, India[1]

Assistant Professor, Department of Computer Applications, MSRIT, Bangalore, India[2]

Asst Professor, Dept. of Computer Science, Smt. K.D.G.D. Mittal Mahila (P.G.) Mahavidyalaya, Churu, Rajasthan[3]

Abstract: Authentication is a procedure of validating who are you and whom you claim to be. Authentication secures the system from unauthorized people who have illegally accessed the right to handle the data present in the system. It also protects the system from potential threats. Though authentication is very strict procedure, with the developing new technologies it can be easily cracked and hacked to steal the user's identity. Current authentication techniques that are in use today are Texted based, Token based, Biometrics based, Recognition/Graphical based etc. but each of this strategies are having their own drawbacks and own limitations. To overcome the disadvantages of these existing authentication techniques a new authentication technique called 3d password is introduced. 3d password scheme is a new strategy recognition patterns, textual passwords, biometrics and graphical passwords. One of the important concepts of 3d password schema is 3d virtual environment which contains real time object scenarios. Also 3d password is more secure and hard to break. This paper focuses on what is 3D Password?, Working of 3D password technique and various applications involved in it.

Keywords: 3d Password, Critical servers, Networking, Authentication, Advantages, Virtual Environment

I. INTRODUCTION

3D password is an XML-based protocol designed to be an added security layer for online transactions. This strategy was initially developed by Arcot Systems, Inc and first deployed by Visa with the purpose of refining the security of Internet payments and is offered to clients under the name Verified by Visa.The 3D password is very user-friendly, and very interesting way of authentication process. Generally passwords are set on the bases of human memory. Usually simple passwords like pet names, places and phone numbers are set so as to quickly recall them. But in this 3d scheme human memory has to undertake the facts of recalling, recognition, token or biometrics based authentication in one single authentication system. When the 3d password is implemented and we log in to a protected site, the 3D password GUI opens up. Initially in 3d password system user can combine the earlier existing schemes for example, textual passwords, biometrics, graphical passwords, and even token based etc. in a single 3D virtual environment. The user is given the permission for choosing the type of authentication strategy which he is comfortable. A user who is good at memorizing the password might prefer to select textual or graphical password schema as a part of their 3d Password. Moreover, a user who often tends to forget textual passwords prefers to select biometrics or smart cards as part of their 3D Password. Hence, users are given full freedom to pick and select how the ideal and desired 3D Password will be constructed.

Once the user gets through the first authentication process next a 3d virtual environment which is mostly a virtual room will open on the display. This virtual area contains many virtual objects. The user initially navigates through this environment and interacts with the objects. The 3Dimensional password generated is usually the combination of all the sequence of user interactions that occur in the 3 Dimensional virtual environment.

For example, the user can enter the virtual environment and type a textual password .Then select a picture frame on a computer that exists in (x1 , y1 , z1) position, then click on the third window of the building in that picture frame that exists at position(x2,y2,z2), then enter a room that has a thumbprint recognition device that exists in a position (x3 , y3 , z3) and provide his/her impression.

The combination and the sequence of the former actions toward the specific objects construct the user's 3D password.

II. RELATED WORK

The theatrical increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating the user .In general, Human authentication techniques can be classified as:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

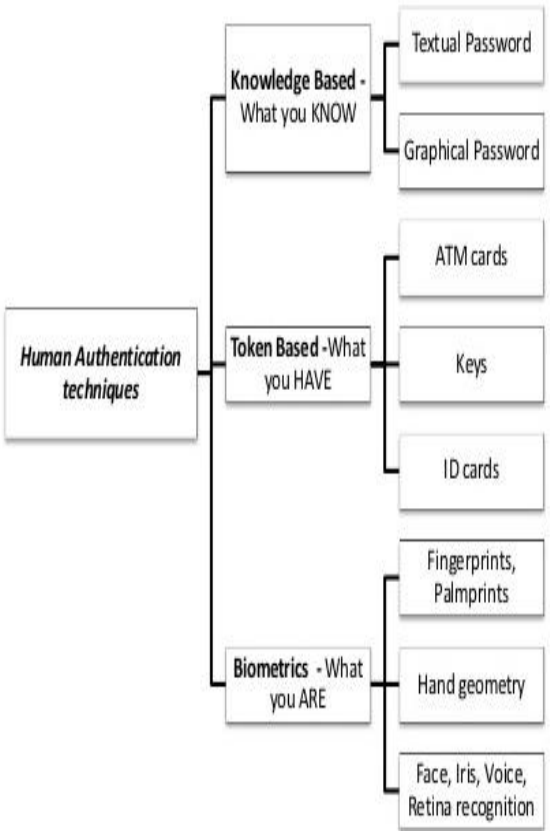

Fig 1. Human Authentication Techniques

1) Textual based: Recall based practices require the user to reproduce a secret again that the user twisted before. Identification based methods order the user to classify and be aware of the secret or part of that the user carefully chosen before. One of the most common recall based schemes used in the mainframe world is textual passwords. One major disadvantage of the textual password is its too inconsistent requirements in the selection of passwords that are easy to remember and at the same while are hard to guess[3].

2) Graphical based: This technique is for those type of users, who can recall and distinguish films better than words. Some of the graphical password strategies are time-consuming to be performed. Moreover most of the graphical password strategies are exposed to shoulder surfing attacks. Hence, presently most graphical password techniques are still in their examine phase and indulge more enhancement's and usability studies [3].

3) Token based: In banking authentication structures, it not only requires a knowledge based authentication systems like textual based and Graphical based systems but also token based system is required. However, many reports have shown that tokens are susceptible to loss, fraud or theft by using simple techniques [8]. Any ATM cards, swipe card are examples of token based authentication systems [11].

4) Biometric based: Various Biometric schemes have been proposed; Finger-Prints, Face-Recognition, Voice-Recognition, Retina-Recognition and Palm-Prints are all different biometric systems. But all schemes are has it' sown limitations and drawbacks based on several factors such as acceptability, uniqueness, and consistency. One of the main drawbacks of applying biometrics is its inappropriateness upon a user's personal characteristic [8]. Example of biometric system, if the system uses thumbnail expression of users for authentication purposes. When the system register the new users, it will initially take the thumbnail expression of new user using thumb recognition device and store it in image format in system Database record. Next time when the user log's into the system, user will give the thumbnail expression by using thumb detection device. Later the system validates that image and checks if it's same or not. If the thumbnail expression is validated to be correct then the system provides permission for next authentication scheme or if the thumbnail expression is validated to be incorrect then the system gives an error message [15].

To overcome the advantages and disadvantages of previously existing authentication systems. The new authentication system is introduced which is based on formerly existing schemes. It is combination of passwords called as "3 Dimensional Password". Which is a multifactor scheme uses combination of all the above discussed recall based, recognition based, graphical based and biometric based scheme & many other schemes. While creating 3d Password all these techniques are implemented in virtual 3 Dimensional environment. The user will interact with this virtual environment which contains various virtual objects. Different user will have different 3D environment, the environment will change as the user changes. The 3D password is constructed by observing the sequences of interactions of the user [2].

III.PROPOSED SYSTEM

A. Goal:

The key goal of the proposed system is to strategy 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 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.

B. Objective:

- The new scheme must offer more secure authentication when compared to existing authentication scheme.
- The new scheme must be built in such a way where it is easy to understand and very user-friendly

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

authentication technique, by providing the user freedom of choice to select the type of techniques to be involved in generating the password.

- The new scheme must provide secrets that are easy to recall or memorize and at the same time hard to guess for the hackers and crackers.
- The new scheme must provide secrets that are combinations of basically Recall, Recognition, Biometrics, and Token based authentication patterns or combination of any two or more systems together.
- The new scheme must provide permissions to only authenticated users to change or remove them [12].

C. Architectural study of 3D password

3D Password is multi-factor therefore several password schemes such as textual password, graphical password, biometrics, token or cards based passwords simultaneously can be used as a part of user 3D Password scheme. Different users have different needs so users are required to be given the independence of selection to choose which authentication schemes will be part of users 3D Password[12]. 3D password offers a 3D virtual environment which can be defined as the transformation of real life scenarios into virtual objects. For creating 3D passwords users moves inside the 3D virtual environment and interacts with the virtual objects present in the scenarios given. The interactions with the virtual objects inside 3D virtual environment vary as per the different user. The 3D virtual environment is a basic building block of the 3D password authentication system. In 3D password authentication system, the first step is to design a 3D virtual environment which reflects the security requirements and the administration needs. Designing a well- planned 3D virtual environment improves the acceptability, usability and effectiveness of a 3D password authentication system [15]. The figure is representing state diagram for creating a 3D Password application.

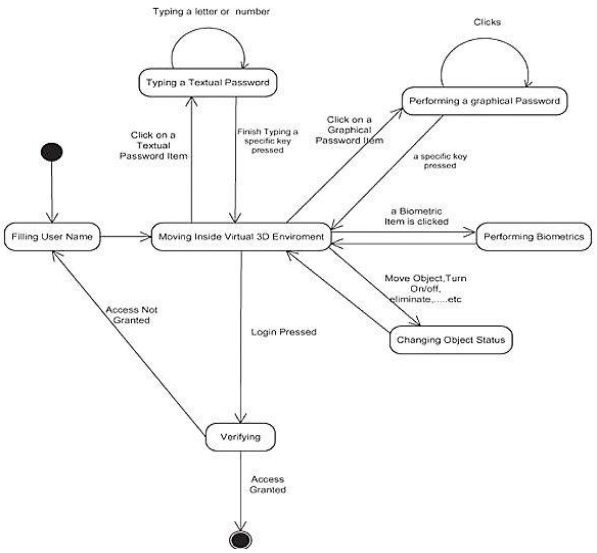

Fig 2. State diagram of 3d password

D. Working of 3D password

3D password key space is determined by the design of 3D virtual environment and type of object selected inside the 3d virtual environment. Now, let us consider G x G x G to be the size of 3D virtual environment space. The virtual objects are distributed with the unique (x,y,z) coordinates in the 3 Dimensional virtual environment[4]. Here we are implementing 3 Dimensional password system to provide the security to the email client system. User need to create the account to access mailing services. User has to fill up his or her profile details like user id, name, address etc. to create the account and has to provide password which will be a 3D password.

User moves in 3 Dimensional virtual environment after filling the profile details. Next the user will navigate inside 3D virtual environment and interact with the virtual objects using any input devices such as keyboard, mouse. In 3D virtual environment, user now enters into an art gallery. Art gallery consists of many paintings in it. User has to select various pointer pictures in that art gallery. This sequence in which the user has select or clicked on the objects that sequence of points will be stored in a text file in the encrypted form. In this manner the 3 Dimensional password is created or set for a specific user.

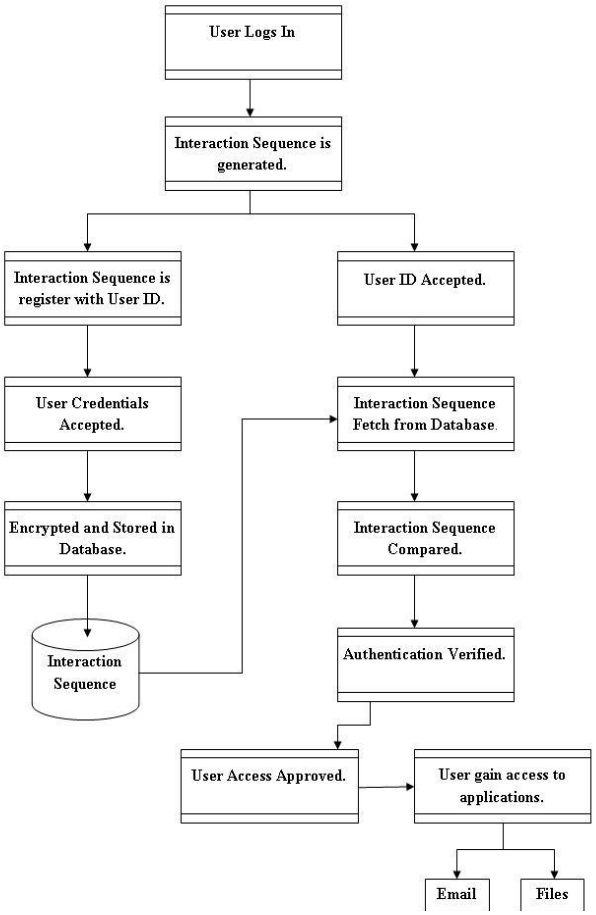

Fig 3. Flow diagram of 3d password authentication

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

In this technique we have used Centered Discretization method and Secure Hash Algorithm for the different selection of the points and to manage the database. Next time if the user wants to access his/her account, he has to reselect all the objects which he/has entered at the time of generating password with correct and proper sequence. This sequence is then compared with the coordinates that are stored in a text file before. Access is thus given to the authorized user if authentication is correct.

E. ADVANTAGES

1. 3D Password is multi-feature and multi-password authentication technique.
2. 3D password can't be hacked by any other person easily.
3. 3D password has no specific size limit and larger password key space.
4. 3D password is easy to be changed.
5. This password is better and more secure when compared to existing techniques.[8] [12]

F. DISADVANTAGES

1. 3d scheme is expensive when compared to others.
2. Requires computer expertise.
3. Visionless person find it hard to use this technique.
4. Lot of program coding is necessary.
5. Lot of time and memory consuming.
6. Shoulder-suffering attack is still active and can disturb this scheme. [8] [12]

IV. IMPLEMENTATION

In order to use 3D password first the user authenticates with simple textual password which means that the user provides username and password. The authentication is validated and if it is successful the user moves into 3 Dimensional virtual environment, thereafter a computer with a keyboard will be seen on the screen. On that screen user need to enter the textual password which is stored in a simple text file in the form of co-ordinates which are encrypted. After the authentication is successfully completed, the user can then automatically enter into an art gallery, where he/she has to select multiple objects or points in that gallery or he/she can perform some action like switching button on/off or perform any action associated with any object like opening a window, etc. The sequence in which the user has selected the objects in that sequence of points are stored in a text file in the encrypted form. In this way the passwords can be set for that particular user. For selecting points we have used 3 Dimensional Quick hull algorithm which is based on convex hull algorithm. And now this password can be used as an authentication when the user logs in next time. The user has to perform the actions in the same manner as that it is stored in the file for the authentication to be successful. If authentication is successful the access is given to authorized user. [7]

Consider an example, the user can enter into virtual environment and type something on a computer that exists in "(x1, y1, z1)" position, then go to a room that has a fingerprint recognition device that exists in position say "(x2, y2, z2)" and provide his/her fingerprint. Then, the user can visit the virtual garage, open the car door and turn on specific channel in the radio.

The sequence and combination of the previous actions towards the specific objects constructs the user's 3 Dimensional password. Any object can be a virtual object that we encounter in our day to day life. Any actions and interactions that are obvious and happens in real life can be done in the virtual environment towards virtual objects. However, any user input such as speaking in a particular location in the virtual 3D environment can be considered as a part of 3 Dimensional password.
We have the following objects:

1. An ATM machine that requires a smart card and PIN.
2. Any graphical password scheme.
3. A computer with which the user can type.
4. A chair that can be moved from one place to another.
5. A light that can be switched on/off.
6. A paper or a white board that a user can write on.
7. A car that can be driven.
8. A staple that can be punched.
9. Any real life object.
10. A television or radio where channels can be selected.
11. Any upcoming authentication scheme. [4]

A 3D password is a one of the authentication scheme. It is implemented in a 3D virtual environment. For that some of the mathematical concepts are required.

1) Time Complexity:

Time complexity = Am + Bn

Here m is indicating time required to communicate with the system and n is the time required to process each algorithm in 3D virtual environment.

2) Space Complexity:

A 3D password is stored in the database as co-ordinates x, y and z. Because in a virtual environment it is considered in 3 dimensions as x, y and z. [11]

V.3D VIRTUAL ENVIRONMENT

3D virtual environment is used as basic building block of this multi-factor authentication scheme.
The 3D virtual environment is created with the help of a 2D screen, see fig 1. It is a real time scenario seen by people in their day to day life which is virtually created in 3D virtual environment. This technique can be applied by using any real time object as an environment such as village but to be more precise and clear make use of small environment like room.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

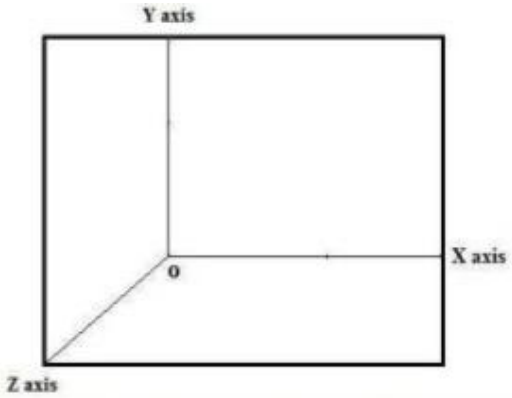

Fig 4. 3d environment under 2d screen

For selecting the sequence of points or objects we can make use of an efficient 3D Quick hull algorithm which is known as convex hull algorithm. This algorithm stores the selected points in the form of 3D co-ordinate(x, y, z) in a simple text file[5].

Design Guidelines:

When we design a well-studied 3D virtual environment affects the usability, effectiveness, and acceptability of a 3D password authentication system. Therefore, the first step to build a 3 Dimensional password system is to design a 3D environment such that it reflects the administration needs and the security requirements. The design of 3 Dimensional virtual environments should follow some of the below guidelines.

1) Real-life similarity: The prospective of a 3 Dimensional virtual environment should reflect what people are used to do in their day to day life. The objects used in virtual environment should be relatively similar in size to that of real objects (sized to scale). The possible or obvious actions and interactions towards virtual objects will reflect in real-life scenarios. The object response should be realistic in nature. And the target should have a 3 Dimensional virtual environment so that users can interact with, by having common sense.

2) Object uniqueness and distinction: Every other virtual object or item in the 3 Dimensional virtual environments should be unique and distinct from any other virtual object. The uniqueness can be determined from the fact that each and every virtual object has its own identifiable attributes such as position of an object. Thus, the prospective interaction with the object 1 is not equal to the interaction with the object 2.
Therefore, the design of the 3 Dimensional virtual environments should be considered in such a way that every other object should be distinguishable from other objects. However, by having similar objects for example 20 computers in one place will confuse the user. Similarly, when designing a 3 Dimensional virtual environment, it should be easy for users to navigate and distinguish between all the objects. The distinguishing factor increases as the user's recognition of objects increases. Hence, it improves the systems usability.

3) Three-dimensional virtual environment size:3 Dimensional virtual environment can depict a village or city or even the whole world. It can also depict a space as focused as a single office or room. The size of a 3 Dimensional virtual environment should be carefully studied and taken care. A large 3D virtual environment will increase the time required by the user to make use of 3D password.

However, a large 3 Dimensional virtual environment can contain a large number of virtual objects. Therefore, the probability of a 3 Dimensional password space broadens. Moreover, a small 3 Dimensional virtual environment usually contains only a few virtual objects. Thus, performing a 3 Dimensional password will take less time.

4) Number of objects (items) and their types: This is part of designing a 3 Dimensional virtual environment is determining the type of objects and also how many objects should be placed in the virtual environment. The type of objects will reflect what kind of responses will be received. For example, consider requesting a fingerprint or a textual password as an object response type so that selecting the right object response types and the number of objects that affects the probable 3D password space.

5) Position of objects/Alignment: In a 3D virtual environment there should be no obvious set of movements that the user will tend to create a password. For example in following scenario, where users are more likely to choose 1st 3 computers as password which will be very easy for hackers to guess the password.

6) System importance: A 3D virtual environment should be considered in such a way that what systems will be protected by a 3D password. The number of types of objects that have been used in a 3D virtual environment should be reflected for the importance of the protected system. [10] [12]

VI. SECURITY ANALYSIS

In order to determine the password space we have to count all the possible 3D passwords that will have a certain number of actions and interactions.

Every user has different requirements and preferences while selecting the appropriate 3Dpassword because every 3D password system can be designed according to the protected system requirements the attacker password system. So we try to propose countermeasures for such attacks [6]

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

1. TIMING ATTACK: Here the attack is based on how much time is required by the legitimate user in completing successful log in using 3D password scheme which gives the attacker mere hints and with this observation attacker can get a clue regarding authenticated user's 3D password length. Yet this attack is not very much effective as it gives mere clues to the attacker.

Thus, it would perhaps be performed as a part of either brute force attack or well-studied attack. If 3D virtual environment is poorly designed then timing attacks can be effective. [12]

2. BRUTE FORCE ATTACK: In this kind of attack the attacker has to try n number of possibilities of a 3D password. As these attacks considers following two points.

1. Required time to login: In a 3d password, time required for successful login varies and depends on number of obvious actions and interactions, the size of a 3D virtual environment.
2. Cost required to attack: A 3d password scheme requires 3D virtual environment and cost of creating such an environment is quite expensive.[2] [6]

3. WELL STUDIED ATTACK: In this attack the attacker tries to find the whole password scheme. In order to launch such an attacker, the attacker has to acquire knowledge of the most probable 3d password distributions and this is very difficult because the attacker has to study all the existing authentication schemes that will be used in the 3D virtual environment it also requires a study of the user's selection of object for creating 3d password. [6]

4. SHOULDER SURFING ATTACK: Here an attacker uses a camera to record the user's 3 Dimensional password or the attacker tries to watch the legitimate user creates a 3d password. This kind of attack is the most effective than any other attacks on 3 Dimensional passwords. Therefore, the 3 Dimensional password must be performed in a secure place where shoulder surfing attack can't be performed. [2] [6]

VII. APPLICATIONS

A 3 Dimensional password can be used in wide area where more security is needed to the system. Some of the areas are as follows:

1) Critical servers: Many organizations have critical servers that are normally protected by a textual password. A password authentication scheme proposes a sound replacement for a regular textual password. However, entrances to such locations are usually protected by PIN numbers and access cards. Therefore, a 3 Dimensional password can be used to protect the entrance to such locations and usage of such critical servers. [9]

2) Networking: This involves many areas of computer networks such as client-server architecture, critical servers, etc. In order to provide more security to server of this architecture a 3D password mechanism can be used. It is very efficient and more secure way to keep the data or information that is important should be secured from unauthorized people. For applications such as email, 3 Dimensional password is most secure and easier scheme to be used. [2] [5]

3) Nuclear and military areas: These are the important areas where more security is needed. These areas should be protected by the most powerful authentication systems. The 3 Dimensional password has a large probable password space, and since it can contains token-, biometrics-, recognition-, and knowledge-based authentications in a single authentication system, it is a choice for high level security locations. [2] [5] [9]

4) Airplane and jetfighters: There are major chances of misuse of airplanes and jetfighters for religion-political agendas. In such cases airplanes should be protected by a powerful authentication system and 3- Dimensional password is recommended for these systems. In addition, 3- D passwords can be used in less critical systems. [2] [5]

5) Other areas: We can make use of 3 Dimensional password authentication scheme to areas such as Cyber cafes, Critical servers, ATM, web services, Industries and many more. [2] [5]

IV. CONCLUSION

Currently there are many authentication schemes available and they are based on user's physical and behavioral properties, where as some other authentication schemes are based on user's knowledge such as textual and graphical passwords. The textual passwords and graphical passwords or combination of both are commonly applied. But both of the authentication schemes are vulnerable to certain attacks. And, there are many such kind of authentication schemes are currently under study and they require additional time and effort to be applicable for commercial use. The 3 Dimensional password is a multifactor authentication system that combines various authentication schemes into a single one. The virtual environment in the 3 Dimensional password authentication scheme can contain any existing authentication scheme or any upcoming authentication schemes. The system administrator should design the environment to select the appropriate object which reflects the protected system requirements. However, designing a simple and easy to use 3- Dimensional virtual environment is a factor that leads to a higher user acceptability of a 3-D password system. Based on user's preference and requirements the choice of what authentication schemes should be part of the user's 3D password. On the other hand, users who

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

finds difficulty to remember might prefer to opt for biometrics or smart cards as part of their 3D password. Therefore, a user can choose and decide to construct the desired and preferred 3D password so that it can be used many application areas as discussed earlier.

Thus, this paper tells about our study about 3D password, is still in its early stages. Implementing 3D password as well as 4D password for mobile handset is another important future work of this paper.

ACKNOWLEDGMENT

I thank **Dr. T. V. Suresh Kumar**, Prof. and Head, Dept. of MCA, MSRIT, Bangalore-54. for his continuous support and encouragement for completing this research paper and also thanks to MSRIT management.

REFERENCES

[1] A.B.Gadicha, V.B.Gadicha-"Virtual Realization using 3D Password" International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, pp216-223, 2016.
[2] A.B.Gadicha, V.B.Gadicha-"Virtual Realization using 3D Password" International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, pp216-223, 2016.
[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] Pooja M. Shelke, F. M. Shelke, Mr. B. G. Pund-"Advance Authentication Technique: 3D Password" International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, pp632-635, 2016.
[5] Vishal Kolhe, VipulGunjal, SayaliKalasakar, PranjalRathod-" Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology, ISSN: 2319-5967, pp99-105, 2013.
[6] SmritiKhurana, Mili Patel, Prateek Kumar Singh-" Study of 3D and 4D password Security" International Journal for Research in Computer Science, pp49-56, 2016.
[7] AnaghaKelkar, KomalMukadam-" 3D PASSWORD MODERN APPROACH TO SECURITY" International Journal of Computer Engineering and Applications, ISSN 2321-3469, pp31-38, 2015
[8] Shivani A. Patil, Shamli A. Hage-"Improving ATM Security Using 3D Password" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2278 – 8875, pp8308-8312, 2015.
[9] Mr. Rakesh Prakash Kumawat, Mr. SachinSampatBhosale, Mr. PrashantPrabhakar Ratnaparkhi-"3D Graphical Password Authentication System" International Journal for Research in Applied Science & Engineering Technology, ISSN: 2321-9653, pp319-325, 2015.
[10] NishaSalian, SayaliGodbole, ShalakaWagh-"Advanced Authentication Using 3D Passwords in Virtual World" International Journal of Engineering and Technical Research, ISSN: 2321-0869, pp120-125, 2015.
[11] DhatriRaval, Abhilash Shukla-"Security using 3D Password" International Journal of Computer Applications, pp36-38, 2015.
[12] 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.
[13] KalpanaRathi, Nidhi Sharma, Urmila Jangid-"The survey paper: 3d password" International Journal of Innovative Computer Science & Engineering, ISSN: 2393-8528, 2014.
[14] Mr.Jaywant N. Khedkar, Ms.Pragati P. Katalkar, Ms.Shalini V. Pathak, Mrs.RohiniV.Agawane-" Integration of Sound Signature in 3D Password Authentication System" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320 – 9801, pp447-452, 2013.
[15] Ashwini A. Khatpe, Sheetal T. Patil, Amruta D. More, Dipak V. Waghmare, Ajit S. Shitole-"3DLogin for More Secure Authentication" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, pp2992-3000, 2014.