WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

3D Password- A Desirable Unification of Pre-Existing Authentication Techniques.

Rahul Thakran

UG Student , SGT University,India

A B S T R A C T

Authentication means a process which provides security and protection to any system. Access to any automated system mostly employs textual or alphanumeric passwords. There are multiple authentication techniques available like textual, biometrics etc. Textual password commonly follows an encryption algorithm to provide security to the system. Each of these techniques has certain drawbacks and limitations. Also, most of the end users face difficulty to remember a password which is long and random in nature. As An Alternative, they usually use brief, easy, and insecure passwords. To overcome those drawbacks, a new multi factor authentication technique is now present, known as 3D Password. Graphical passwords could be devised to make passwords more unforgettable and simpler for the end users to use and, consequently, system will be more secure now. Also, using a graphical password or 3D password, users click on images instead of any alphanumeric characters. It consists of a user environment which looks like real time but is not real in nature. 3D password is more secure technique of authentication as compared to other techniques as it is difficult to break and quite simple to use.3D offers the advantage of high security as it combines the authentication of existing system. In this paper, we review and evaluate a new scheme of authentication, based on a virtual three-dimensional environment, and uses the passwords based on the fact of Human memory.This paper aims to concentrate on the notion of the innovative authentication method, its working, and the purposes of 3D password.

Keywords: 3D password, authentication techniques, security, 3D virtual environment, system security

1. INTRODUCTION

3D is a multifactor authentication scheme that combines all existing authentication schemes into a single 3D virtual environment. Authentication is the method of confirming who you are to the one you claimed to be. Generally, four human authentication techniques are available:

1. What do you know (which is knowledge based).
2. What do you have (which is token based).
3. What you are in real (a part of biometric analysis).
4. What do you recognize (recognition-based technique).

* *Corresponding author.*
E-mail address: *rthakran9818@gmail.com*

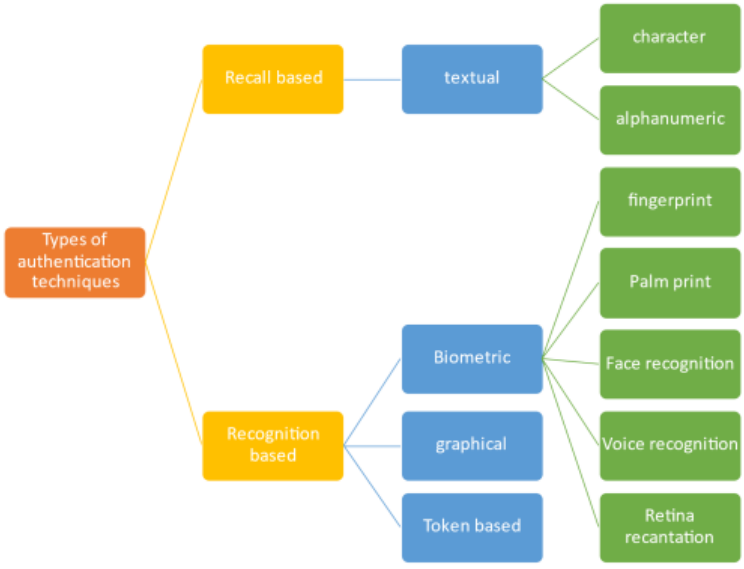

Figure 2.1 – types of human authentication techniques

Textual passwords are the most familiar authentication techniques used in the world of computers. Both recognitions based and recall based authentication techniques have few downsides & constraints when they are used independently or used sole authentication scheme at a time. To overcome such complications a new authentication scheme which combines both textual as well as graphical got introduced, known as 3D password.

3D password, an XML-based protocol, is devised to be an additional security layer intended for online transactions. It was initially developed by Arcot Systems, Inc and first implemented by Visa with the objective of enhancing the security of Internet payments and is presented to clients under the name Verified by Visa. The 3D password is authentication technique that is very user-friendly, and at the same time very interesting. Usually, passwords are set based on human memory. Typically, simple passwords such as names of pets, places and phone numbers are set because they are quick to remember. Klein obtained a database of nearly 15,000 user accounts that had alphanumerical passwords and asserted that 25% of the passwords were conjectured using a small, yet well-formed dictionary of about (3×106) words. Although the full textual password space for 8- character passwords which consists of letters and numbers is about (2×1014) possible passwords and by using a small subset of the full space available, 25% of the passwords were easily guessed accurately. This fact is due to the user's negligence in picking their textual passwords and to the fact that most users do not choose random passwords.

The 3D password has a substantial number of potential passwords because of the high number of workable actions and interactions regarding every object and for the three-dimensional virtual environment authentication is centered on what a person holds, i.e., the aspects of a human being like biometry. There are possibilities that the items which are under possessions may be lost and information may be forgotten. But this does not happen with biometrics. Constraints of these 3 techniques can be overcome only if we take advantage of all three methods in a single system. The central driving force in the wake of biometrics-based authentication getting more and more recognition day-by-day. The intention of using biometrics is to deliver a tool to identify a person with the assistance of his/her own characteristics and to get rid of the use of much troublesome ways of recognition which are based on password, physical keys, ID card etc. This 3D virtual environment encompasses numerous objects or items with which the user can interact easily.

Figure 2.2 – snapshot of a 3D password

Texture based password is fundamentally a recall-based technique that obliges the operator to retell or replicate the confidential text that user had created

before. Textual Passwords ought to be easy for user remember but at the same time tricky to guess by another. This system has a common shortcoming as it can be easily guessed accurately by using brute force dictionary. But in case of 3d scheme, human memory needs to embark on the particulars of recalling, recognition, biometrics, or token-based authentication in one single authentication system. When the 3d password is executed and we log in to a safeguarded site, the 3D password GUI commences where in 3d password system user can merge the pre-existing schemes such as textual, graphical, biometrics, token-based techniques etc., and that too in a single 3D virtual environment available. The user is offered the approval for picking the kind of authentication strategy which he is finds comfortable and simpler to use. A user who is excellent at remembering the password may prefer to opt for textual or graphical password scheme as a feature of their own 3d Password. Furthermore, a user who frequently fails to remember textual passwords prefers to select biometrics or smart cards as element of their 3D Password. Thus, users are offered full freedom to choose and select how the ideal and preferred 3D Password will be created.

The 3D password methodology combines recognition, recall in one authentication system, with the notion that can be simply outlined as follows-

The user navigates through a 3D virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the 3D virtual environment structures the user's 3D password. Hence, the user can stroll in the virtual environment and type something on a computer that exists in (x1, y1, z1) position, then move into a room that has an image gallery, chooses any image occurring in position (x2, y2, z2) from it. The combination and the sequence of the earlier two actions towards the specific objects build the user's 3D password. Users can circumnavigate across a 3D virtual environment that can include any virtual object and of any type. Some of the possible objects to elucidate the idea are-

An object can be:

1. A computer that the user can employ type in
2. A white board that allows the user to draw on
3. Any kind of Graphical password scheme present
4. Any real-life object available to the user
5. Any forthcoming authentication scheme

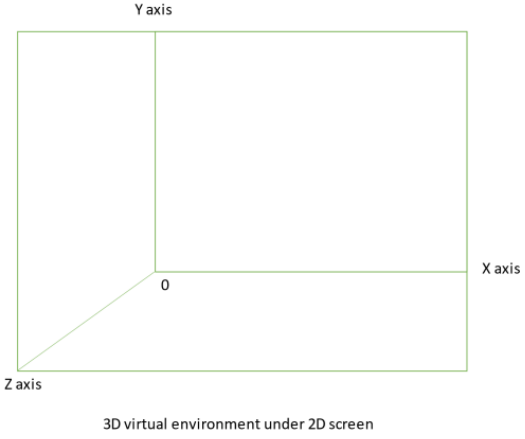

Figure 2.2 – 3D virtual environment under 2D screen.

2. RELATED WORK AND PROBLEMS ASSOCIATED WITH THEM-

There is a large-scale increase in the use of computers nowadays due to which many security concerns have emerged. Among the many security concerns, authentication is the most important, which is a process that validates a user. Generally, the human authentication techniques can be classified as follows-

1) textual based-it is a recall-based technique that requires a user to reproduce a secret again which was twisted before to classify and be aware of the secret or a part user carefully chooses this password. One of the major disadvantages of this technique is that inconsistent requirement in the selection process of password which are quite easy to remember but at the same time they are hard to guess and can be easily cracked by the hacker. (Sindhuja V. et al., 2016)

2) graphical based- Those users who cannot recall and distinguish textual passwords but can easily differentiate between films better than words, make use of graphical based password. But the problem with graphical password is that they are time consuming and are more exposed to shoulder surfing attacks. Also, graphical password is still in the examination phase and cannot be trusted enough. (Sindhuja V. et al, 2016)

3) token based-in case of banking authentication structures, not only textual and graphical based systems are required but also token based systems are very much required. But they are more prone to loss and theft by employing simpler techniques by the hacker. (Kumawat R.P. et al., 2015) For example, any swipe guard or ATM card is token based. (Raval D. et al, 2015)

4) Biometric based: apart from the above techniques, certain biometric schemes have also been proposed which includes face recognition, fingerprint recognition, voice recognition, retina recognition and other potential characteristics of humans. But every scheme inculcates certain limitations and constraints based on factors like uniqueness, acceptability, and consistency. Major drawback being inappropriateness upon the user's personal characteristic. For example, if system utilizes thumbnail expression as authentication system, then whenever the system registers a new user it will initially take the thumbnail expression and store it as an image format in the system database and next time whenever user logs in, the thumbnail expression would be detected, if it validates the image to be correct then the system gives permission and if the thumbnail expression is validated to be incorrect then the

system gives an error message to the user. (Khatpe A.A. et al.,2014)

To overcome the pros and cons of pre-existing systems of authentication, a new authentication system was introduced based upon formerly existing ones and was named as 3D password which is a combination of passwords. This multifactor scheme combines all the above discussed recall, recognition, graphical and biometric based schemes, and many other schemes which have not been stated here.

3D passwords are flexible, and they provide unlimited password possibility where, the timing attacks which are based on the time required to complete successful login using 3D password needs to be well studied and possess a problem for the attacker to study the whole password scheme and therefore it provides a better security to the user.

3. - PURPOSE

1. To avoid key logging, make use of a 3-step authentication protocol.
2. Normal login along with Visual Authentication using QR code and 3D Password.
3. To provide an easy interface to the user
4. To reduce the user overhead for memorizing too many passwords.
5. To avoid total dependency on a single entity and propose another entity to improve security.
6. To Offer improved usability and experience.

4. - LITERATURE SURVEY-

Literature survey and review is the basis for the research and better study of various concepts which are required for a particular domain. Several national and International Journal papers which formed the basis of this review paper and helped in the selection of domain and proper application of the project were studied. The papers which were referred are-

1st-**3D password-based authentication system using multilayers**-

It is stated that to access any automated system, there is a requirement of certain textual and alphanumeric password and users mostly find it difficult to remember them because they are long and random appearing. Hence, they choose short,simple and insecure passwords. Therefore, graphical based passwords are designed to make them more memorable and to provide a security to the user which is a major element of 3D password authentication technique.

2nd-**3D password-more secure authentication scheme**-

It proposed an evaluated and new scheme of authentication based on virtual 3D environment where the passwords are based on the fact of human memory because simpler password are set so quickly to recall them, that they are vulnerable to the attacker. It showed that once the user crosses first authentication, a virtual 3D room will open on the screen where the user navigates and interacts with other objects and the sequence of actions and interactions towards the other object inside that environment constructs the user's 3D password which proves to be more secure.

3RD- **Study on 3D password authentication system**-

It stated that authentication validates the user and provides a security to the data but in certain cases the data gets illegally accessed by the attacker, which could culminate into potential threat. Various techniques like text based, token based, biometric based etc. are available but they have their own drawbacks which needs to be overcome to provide a better security technique. There comes the idea of 3D password which is a new strategy based on all preexisting recognition patterns and consists of a 3D virtual environment which encompass a real time object scenarios and is hard to break and proves to be more secure.

4TH-**security using 3D password**-

Authentication provides security to our system and includes various techniques example, textual ones but have certain limitations associated with them. Those can only be overcome by using a new technique which is a multifactor authentication technique and is a unification of former ones. It proposed that that advantage of 3D password is that it combines all the previous ones and provide high security to the users.

5th-**3D password modern approach to security**-

It proposed that to ensure that only authorized people can have the right to use or handle the system and related data, various authentication schemes and algorithms must be combined so that their shortcomings can be overcome easily.

5. - METHODOLOGY-

1.1. Proposed system-

The proposed authentication scheme is an amalgamation of different authentication schemes altogether. It combines both recall based (textual) and recognition based (graphical) passwords so that multifactor and a multi password authentication known as 3D password could be generated. Refer to the figure number-

Here, a new virtual environment is introduced which is termed as 3D virtual environment where a user can navigate and move in that environment to create a password based on both the schemes. In the proposed system, the biometric scheme has not been included because of some potent drawbacks like shoulder surfing attacks, venerability, increase in the cost of scheme and hardware parts needed.

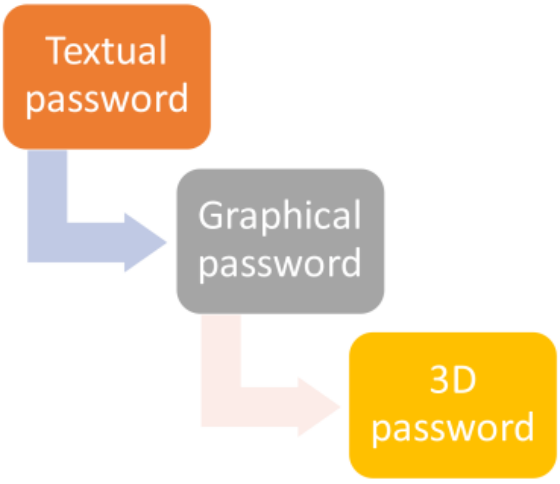

Figure 6.1.1 – sequence of authentication in 3d password scheme

1.2. Architectural study-

This section gives an idea about the creation of 3D password and different schemes used to complete that, along with its nature so that many other password schemes can be used as a part of 3D password. Selection of distinct schemes relies on the type of users who are going to use the scheme in their systems. Figure-shows all simple state diagram for the creation of 3D password.

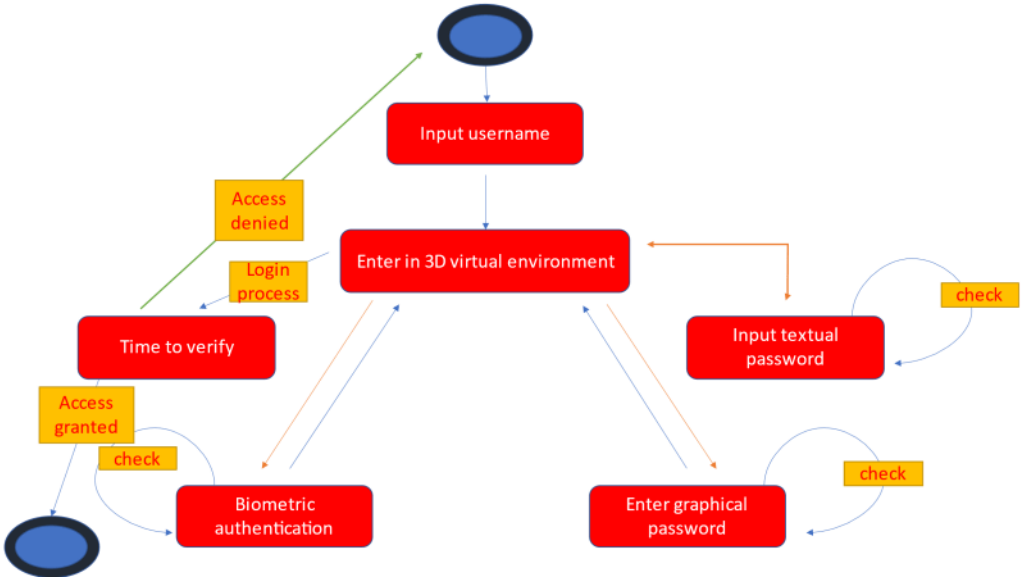

Figure 6.2.1 – architecture of 3D password authentication (Rawal D. et al.; 2015)

1.3. **a 3D virtual environment-**

a3D authentication system has a basic building block which is known as a 3D virtual environment that is created inside a 2D screen and that too in a real time scenario as seen by people in day-to-day life. Any real time object can be used as an environment, for example, room or village but for its simplification, small environment like room is usually used.

Sequence of objects are selected based upon simplicity, easiness and efficiency of algorithm known as convex hull algorithm and the points which are selected are stored in the form of 3D coordinates (x,y,z) in a simple text file. (Kohle v. et al., 2013) It keeps in mind certain design guidelines related to 3D environment such as-

a) a virtual environment which is selected should be like the real-lifeobject.
b) every object must be unique and distinct from other object.
c) size of the virtual environment should be taken into consideration while construction.

figure 6.3.1 convex hull algorithm

Figure 6.3.2 – a 3D virtual environment

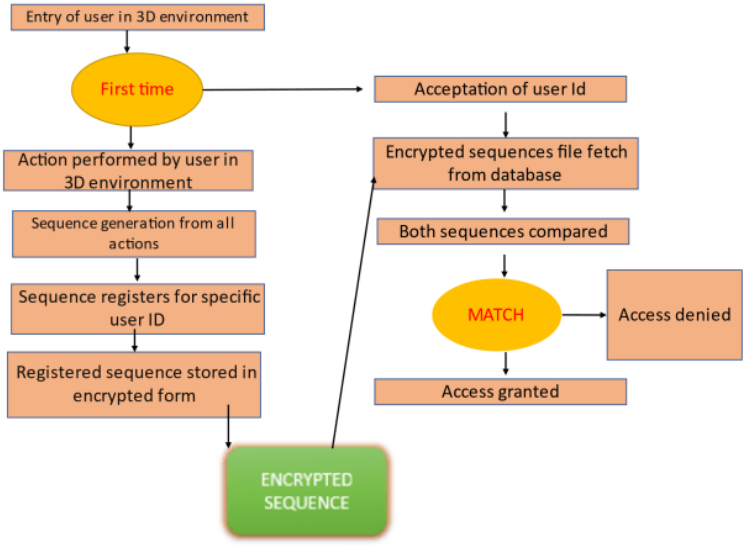

Figure 6.3.3 – sequence of events in 3D virtual environment

1.4. working of a 3D password scheme

a) Registration

1- whenever a new user tries to register, he must enter all the details are available in the registration form.

2- now the user enters a virtual environment where he must input textual password an also select images from the multiple images option available.

3- all these interactions now get stored in the database in an encrypted form.

b) authentication-

1-user must enter the username and password

2- then he needs to click on the images in a proper sequence

3-after that, all the interactions getfetched from the database and get compared one after another

upon the grant of the access to authorized user, now he can access all the application.

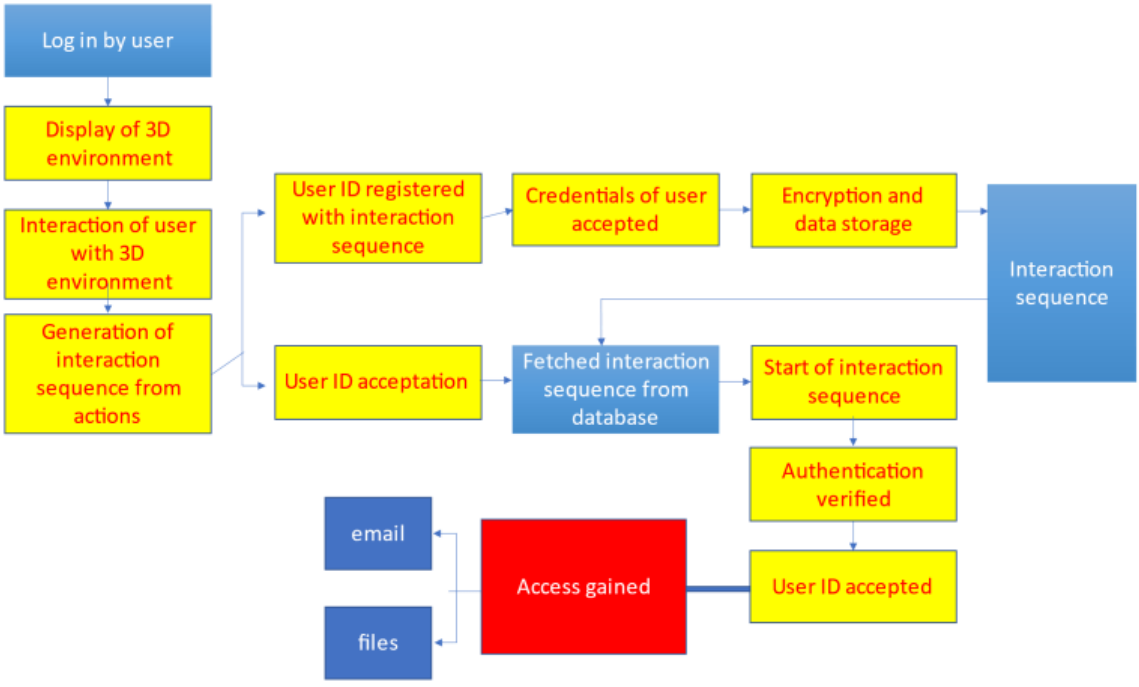

Figure 6.4.1 – working of a 3D environment. (Rawal D. et al.; 2015)

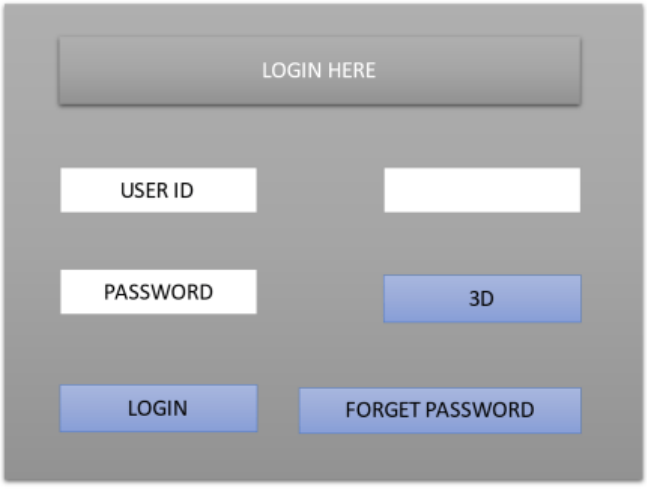

Figure 6.4.2 – a 3D password dialogue box

1.5. **Authentication schemes**-

Multiple authentication schemes are utilized to give access to the data and system for an authorized user and to provide security for the same which can be-

1-text authentication

2-graphical authentication

3-token authentication

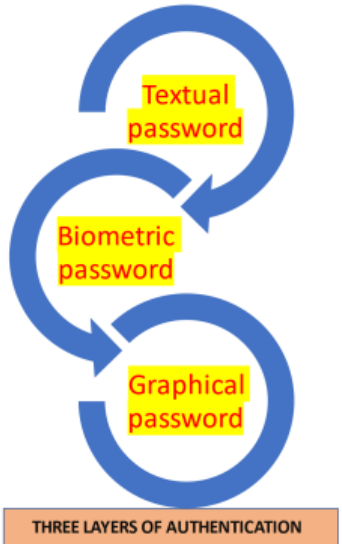

Figure 6.5.1 – three layers of authentication in 3D password

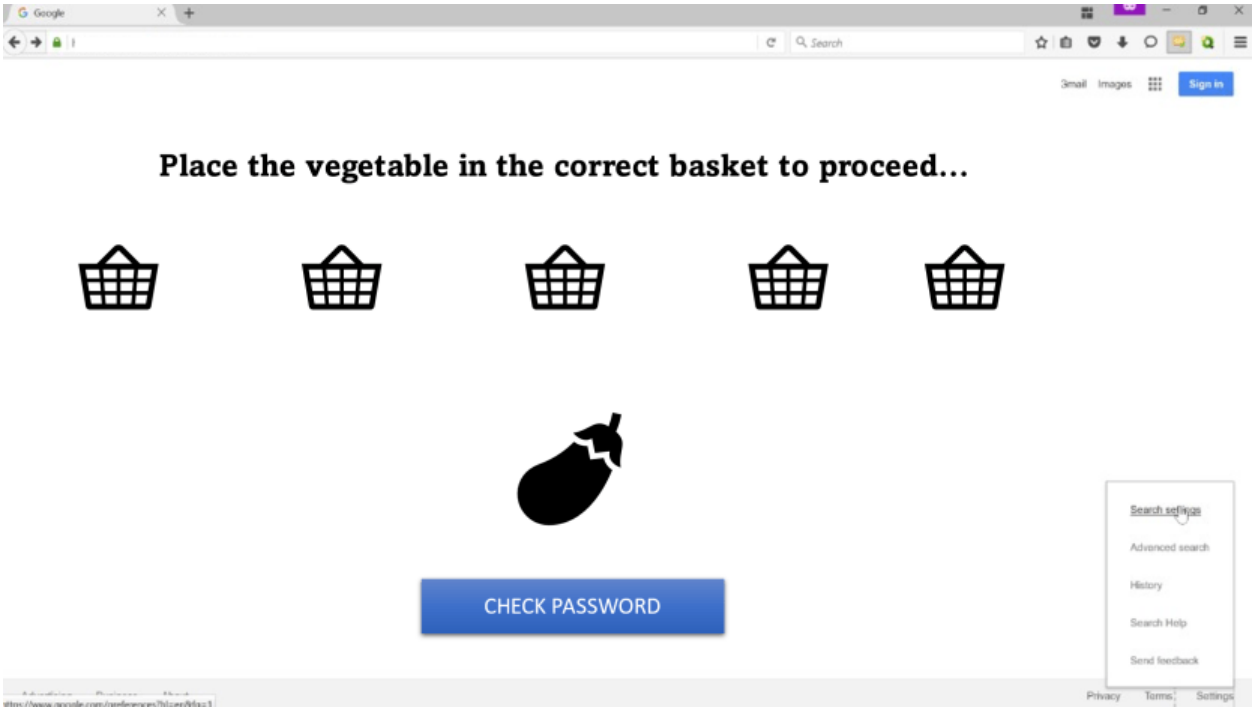

Figure 6.5.2 – snapshot of a 3D password, including graphical password.

6. -. SECURITY ANALYSIS-

Security analysis is done to understand the level of security and protection the 3D authentication can provide. It is used to check whether the proposed system is immune against any attack and if it is found to be vulnerable, what the countermeasures need to be taken to prevent them. (Khurana S. et al., 2016) Followingis some of the security analysis methods that could be employed in the case of 3D password-

brute force attack-

In this case, a recall based password is more secure in comparison to the recognition based technique. In case of first layer, the text based password is taken for authentication and leaves no space to generate combination of character and numerals. It is hard to do this attack on graphical password and even harder to succeed in the next two layers of biometric and graphical password. (Gadicha A.B. et al., 2016; Khurana S. et al., 2016)

guessing-

It is quite difficult to guess the graphical password by mere human interaction, for that purpose the user must enter the graphical password for the system authentication which cannot be guessed.

social engineering-

It is hard to crack the password because it involves certain graphical passwords as a keyboard input which are not present as words in the dictionary.

spyware attack-

This type of attack is impossible in case of graphical password. Although screen recording is possible, but no such spywares have been generated till date, which could detect the graphical password.

7. - ADVANTAGES-

1. It is multi-feature and multi-password authentication method.
2. It cannot be hacked easily.
3. It has larger password key space because it has no specific size limit.
4. it can be effortlessly changed.
5. extra secure as compared to others. (Shivani A. et al., 2915; Bilapatte S. et al., 2014)
6. It offers user options to pick the type of authentication of his/her individual choice.
7. It removes a brute force attack.

Protected against a software like key logger

8. - DISADVANTAGES-

1. 3d scheme is quite expensive in comparison of others.
2. Requires the proper expertise of computer.
3. Visionless people find it challenging to use this technique.
4. Lot of program coding is needed.
5. Lot of time and memory expending.
6. Shoulder-suffering attack is yetfunctioning and can interrupt this scheme. (Shivani A. et al., 2915; Bilapatte S. et al., 2014)

9. APPLICATIONS-

A 3D password has a large password space in comparison to other schemes and provides protection to critical systems and resources. It has various applications and some of them are listed below-

1) **Critical servers-**The large organization makes use of certain critical servers which are protected using a textual password, but a 3D password can prove to be a better substitute for them. (Kumawat R.P. et al, 2014)
2) **Banking**- Here the 3D passwords are used in creation of credit cards for online transactions and ATM cards also. Apart from these, they are also used to secure certain important data in the banking sector.
3) **Jet fighters and airplanes-** There's always a recurring threat of misusing the airplanes and jet fighters for various agendas like religious, political etc. and they must be protected by the usage of certain powerful authentication system like the 3D password. (Gadicha A.B. et al., 2016; Kohle v. et al., 2013)
4) **Other potential applications**- Apart from the above stated ones, some other potential applications where it proves to be an important part includes personal digital assistants, web authentication, login in laptop, desktop computers, ATM etc. (Gadicha A.B. et al., 2016; Kohle v. et al., 2013)
5) **Networking**- It involves the usage of 3D password in areas such as client server architecture where it is important to secure the information from unauthorized people such as securing the emails. (Gadicha A.B. et al., 2016; Kohle v. et al., 2013)
6) **Nuclear and military areas**- Because of the large probable password space, 3D password is employed to secure the nuclear and military areas and information associated with them. (Kumawat R.P. et al, 2014; Gadicha A.B. et al., 2016; Kohle v. et al., 2013)

10. FUTURE SCOPE-

Currently the passwords that are in usage includes textual and token based ones for authentication purpose, but these schemes have narrow scope, and they are more vulnerable to attacks by the unauthorized people. Since 3D password provides freedom to the user to select the kind of password, they want to use where the password will be solely based on recall, biometrics recognition or it can be a combination of two or more schemes. Also, it does not employ any requirement of fingerprints or proper cards for the authentication of the system and provides the choice to the user to create or constructtheir own password, according to their preferences. It revolves around a 3 dimensional virtual environment which is usually designed by the system administrator and has a large password space. Also, 3D virtual environment contains the objects which the user feels familiar with and can relate to the real world, for example, a classroom or any room can be simulated as a 3D environment.

11. CONCLUSION

There are various schemes of authentication which are available and includes textual password, biometric analysis, token based passwords, graphical passwords etc. but these authentication techniques are vulnerable to various kinds of attacks, example brute force attack, shoulder surfing attack, timing attack etc. A 3D password being a multi feature, multifactor, desirable amalgamation of other schemes etc. is a better authentication technique that not only combines the benefit of single technique but also several other techniques and uses a 3D virtual environment. Being a new technique, it is still in the budding stage because designing the kind of environment, deciding the proper password space, interpretating users' feedbackand experiences, enhancing and improving the users experience etc. requires certain time. Security can be achieved because only legal user knows that what kind of images are selected andits sequence, whenever it employs the usage of graphical password along with it. 3D password provides flexibility to the user to create a password according to its preference and this makes the usage of 3D password user-friendly.

Thus, this paper talks about a study regarding the new authentication scheme, which is still in its early stages. Implementing 3D password as well as a 4D password for mobile handset can be a future work for better authentication for the user.

REFERENCES

- Alsulaiman, F.A.; El Saddik, A., "Three- for Secure, "IEEE Transactions on Instrumentation and measurement", vol.57, no.9, pp 1929-1938.sept. 2008
- Bhaidkar N., Prasad P., Kamble A., Multifactor Authentication using 3D Password,
- Bilapatte S., Bhattacharjee S.- "3D Password: A novel approach for more secure authentication" International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, pp150-156, 2014.
- Chiasson S.,Forget A., Stobert E., Oorschot P.V., and Biddle R., "Multiple Password Interference in Text and Click -Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.
- GadichaA.B.,GadichaV.B -"Virtual Realization using 3D Password" International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956, pp216-223, 2016.
- Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices", NI STt NISTIR 7030, 2003
- KannanN.,"How to catch some next big things and lose others" Online: http://blogs.ittoolbox.com/bi/entrepreneur/archives/000574.asp March 2004.
- Kelkar A., Mukadam K., 3D Password Modern Approach to Security, International Journal of Computer Engineering and Applications, Volume IX, Issue XI, Nov. 15 www.ijcea.com ISSN 2321-3469.
- Khatpe A.A., Patil S.T., More A.D., Waghmare D.V., Shitole A.S.- "3DLogin for More Secure Authentication" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, pp2992-3000, 2014.
- Khurana S.,Patel M., Singh P.K.- "Study of 3D and 4D password Security" International Journal for Research in Computer Science, pp49-56, 2016.
- Kognule T.M., Gole M.G., Dabade P.T., Gawde S.B., 3D Password – More Secure Authentication Scheme, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 3 Issue 2, February – 2014
- Kolhe V., Gunjal V., Kalasakar S., Rathod P.- "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology, ISSN: 2319-5967, pp99-105, 2013.
- Kumar K., Goyal D., 3D Password Based Authentication System Using Multiple Layers,International Global Journal for Engineering Research Volume 9 Issue 1 –2014
- Kumawat R.P.,Bhosale S.S.,Ratnaparkhi P.R.- "3D Graphical Password Authentication System" International Journal for Research in Applied Science & Engineering Technology, ISSN: 2321-9653, pp319-325, 2015.
- Nayana S., Niranjanamurthy M., Chahar D., Study on Three Dimensional (3D) Password Authentication system, 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.
- Patil S.A., Hage S.A.- "Improving ATM Security Using 3D Password" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2278 – 8875, pp8308-8312, 2015.

- Raval D., Shukla A.- "Security using 3D Password" International Journal of Computer Applications, pp36-38, 2015.
- Sindhuja V., Shiyamaladevi S.,Vinitha S.- "A Review of 3D Protected Password" International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, pp3995-4001, 2016.
- Sobrado, L and Birget, J. "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.
- Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, An association-based graphical password design resistant to shoulder surfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005