3D PASSWORD AUTHENTICATION

[1]Mrs. Ashwini B P, [2]Ms. Bhumika J, [3]Ms. Chinmayee T S, [4]Mr. G M Akshay Bhat, [5]Mr. Naveen Kumar N

[1]Assistant Professor, [2,3,4,5]UG Students
Department of Computer Science and Engineering
Siddaganaga Institute of Technology
Tumakuru, 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 and secure but having some drawback.**
The 3D password is a multifactor 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 type of interaction varies from one item to another. The 3D 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 + TOKEN 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.

Keywords: **3D Password, Multi-factor Authentication, Recall, Recognition, Token, Virtual Environment.**

I. INTRODUCTION

The authentication system which we are using is mainly very light or very strict. Since man 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. Authentication schemes are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc.

Generally there are two types of authentication techniques are available such as:

1. Human Authentication Techniques are as follows:
- Knowledge based: means what you know. Textual password is the best example of this authentication scheme.
- Token based: means what you have. This includes Credit cards, ATM cards, etc. as an example.
- Biometrics: means what you are. Includes Thumb impression, etc.

2. Computer Authentication Techniques are as follows:
- Textual Passwords (Recall Based)-Recall what you have created before.
- Recognition Based: means what you recognize. Includes graphical password, iris recognition, face recognition etc.

II. DRAWBACKS OF EXISTING AUTHENTICATION SCHEMES

- When a person uses textual passwords, he likely chooses meaningful words from dictionary or their nick names, girlfriends names etc. which can be cracked easily. And if a password is hard to guess then it is hard to remember. Users face difficulty in remembering a long and random appearing password, because of that they create small, simple, and insecure passwords that are easy to attack.[1]
- Graphical passwords can also be used. Their strength comes from the fact that users can recall and recognize the pictures more than the words these type of password are susceptible to well-studied attack.
- 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, thumb impressions etc. But biometrics can also be easily hacked with the help of chemicals etc.[1]
- 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 can be very easy to hack the passwords.

III. LITERATURE SURVERY

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

- Textual passwords**:** The most commonly used password now a day 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.

The drawbacks of the textual password lead to new authentication called token based passwords. [3][4]

- Token based passwords: These are the passwords that appear in the form of token such as combination of numbers, jumbled letters, symbols etc. ATMs, swipe cards, 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 lose his token. The drawbacks of the textual password and token based passwords leads to new authentication called graphical passwords. [3][4]

- 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.

The drawbacks of the textual password, token based passwords and graphical passwords leads to new authentication called Biometrics. [4]

- 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.

Hackers may use some chemicals and they can easily hack the thumb impression of the user, also some people hate the fact to carry their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning), as the age goes on, the biometrics may slightly vary.[4]

IV. PROPOSED SCHEME

A. Goal

The key goal of the proposed system is to build 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.

Following are the objectives in proposed scheme:

- The new scheme must offer more secure authentication when compared to existing authentication scheme.
- The new scheme must be built in such a way that it is a combination of Recall, Recognition and Token based authentication techniques.
- The new scheme must be built in such a way where it is easy to understand and provides very user –friendly authentication technique.
- 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.
- The new scheme must provide secrets that are easy to recall or memorize and at the same time hard to guess for the hackers.

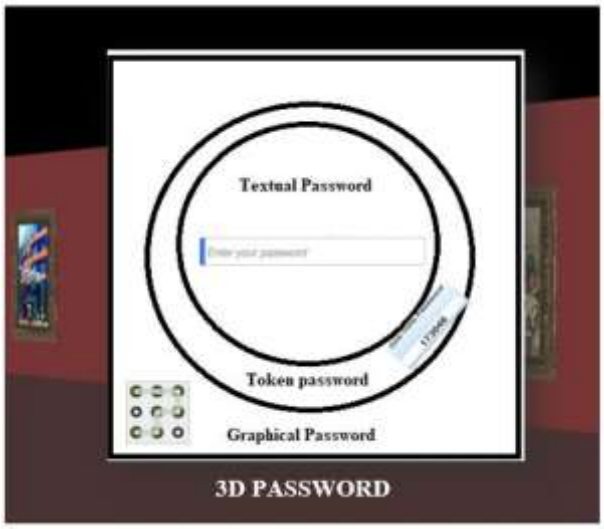

Fig 1: 3d Password as Multifactor Authentication.

The 3D password 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 can navigates and interact with various objects in the 3D environment. The sequence of actions and interactions with objects inside the 3D environment constructs the user's 3D password. The 3D password is a combination of existing authentication schemes such as textual passwords, graphical passwords, and token passwords into a single 3D virtual environment.

3D password is organised into two phases REGISTRAION phase and the LOGIN phase. Already registered user can use login phase to unlock his password, if the user has not registered (new user) he can make his entry using registration phase.

B. System Architecture

3d password is divided into two phases Registration (Fig 3) and the Login phase (Fig 7). New user registers the 3d password by giving the necessary information such as email-id, password in the registration phase after the successful registration 3d environment (Fig 4) is displayed and user interacts with the 3d environment and interaction sequence gets registered with user-id and the interactions gets stored in the database indicating successful registration. After the successful registration user logs into login phase followed by entering into the 3d environment by giving user-id and password as a one-step authentication after successful authentication, 3d environment is displayed and user interacts with the environment, also the new interaction sequences are verified with the existing interactions stored in the database, after the successful interaction, authentication gets verified indicating successful login (Fig 8) and user gains access to the applications such as files, folder etc.

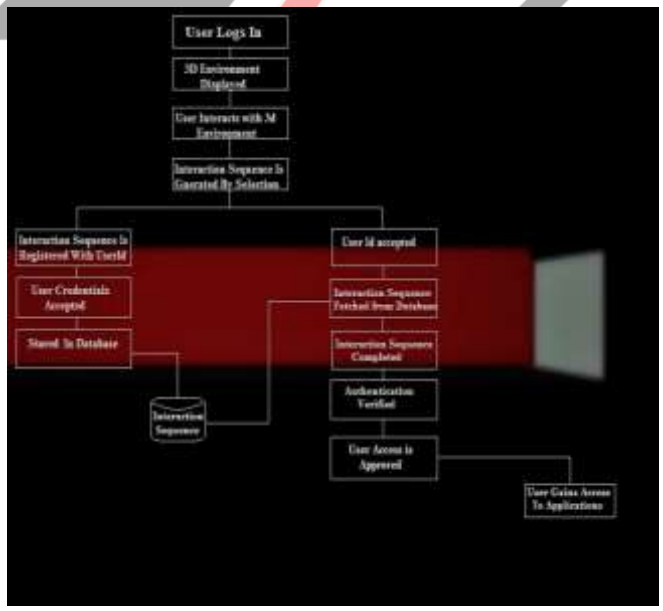

Fig 2: System Architecture.

V. RESULTS

Fig 3: Registration phase.

Fig 4: 3d virtual environment.

Fig 5: virtual objects in virtual environment.

Fig 6: Successful registration after the user interactions.

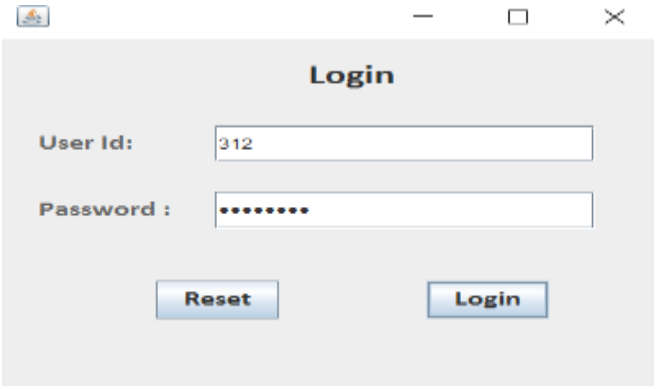

Fig 7: Login Phase.

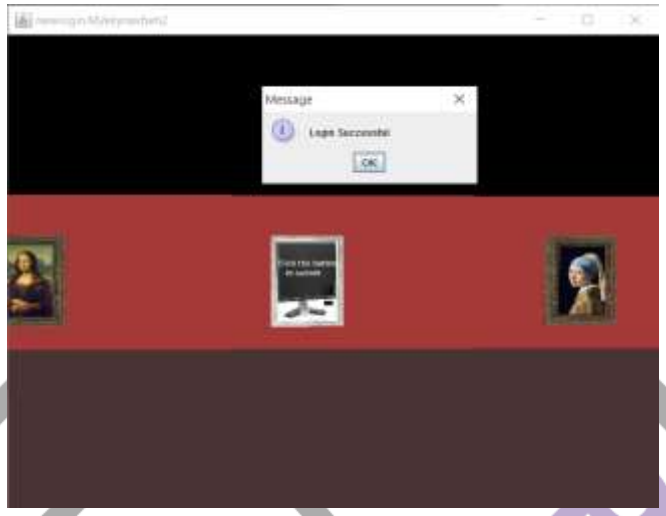

Fig 8: Successful login after the interactions are verified.

V. SECURITY ANALYSIS

- 3D Password space size ¬ To determine the password space, we have to count all possible 3D passwords that have a certain number of actions, interactions, and inputs towards all objects that exist in the 3D virtual environments.
- 3D password distribution knowledge ¬ every user has different requirements and preferences when selecting the appropriate 3D Password. This fact will increase the effort required to find a pattern of user's highly selected 3D password. In addition, since the 3D password combines several authentication schemes into a single authentication environment, the attacker has to study every single authentication scheme and has to discover what the most probable selected secrets are. Since every 3D password system can be designed according to the protected system requirements, the attacker has to separately study every 3D password system. Therefore, more effort is required to build the knowledge of most probable 3D passwords.
- Attacks and Countermeasures - To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods. We have to study whether the authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the counter measures that prevent such attacks.

Following are the possible attacks and its counter measures:

➢ Brute Force Attack: The attacker has to try all possible 3D passwords.
○ Time required to login: The total time needed for a legitimate user to login may vary depending on the number of interactions Therefore, a brute force attack on a 3D password is very difficult and time consuming.
➢ Well-Studied Attack: The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment.

VI. APPLICATIONS

- 3D password's main application domain are protecting critical systems and resources, as 3D password is the combination of several authentication schemes they can be used in nuclear and military facilities, airplanes and missile guiding.

- Many large organizations have critical servers that require high security but such servers are protected by simple textual passwords or a token based passwords, since 3D password is a multifactor authentication it can be used to protect these server as a result high security can be gain to the servers.
- 3D virtual environment can be used in ATMs, personal digital assistance, desktop computers and laptops, web applications etc.

VII. ADVANTAGES

- Since 3D password is a combination of various authentication schemes it provides greater security than existing authentication scheme.
- This 3D password is difficult to hack by others.
- Password can remember easily; it can be remembered in the form of a story.
- This password server as an authentication mechanism to store the personal details.

VIII. DISADVANTAGES

- Difficult for blind people to use this technology.
- Requires sophisticated computer technology.
- 3d password is an expensive authentication scheme.
- 3D password is a combination of various technology, a lot of programming is required.

IX. CONCLUSION

The 3-D password is a multifactor authentication scheme that combines these various authentication schemes into a single 3-D virtual environment. The design of the 3-D virtual environment, the selections of objects inside the environment, and the object's type reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. It is the user's choice and decision to construct the desired and preferred 3d password.

Acknowledgment

We offer our humble pranams at the lotus feet of His Holiness, Dr. Sree Sree Sivakumara Swamigalu, Founder President for bestowing upon his blessings. We deem it as a privilege to thank Dr. M N Channabasappa, Director, SIT, Tumakuru and Dr. K P Shivananda, Principal, SIT, Tumakuru for fostering an excellent academic environment in this institution, which made this endeavour fruitful. We would like to express our sincere gratitude to Dr. R Sumathi, Professor and Head, Department of CSE, SIT, Tumakuru for her encouragement and valuable suggestions. We thank our guide and convener Mrs. Ashwini B P, Assistant Professor, Department of Computer Science and Engineering, SIT, Tumakuru for the valuable guidance, advice and encouragement. Above all, we would like to express thanks to our parents for their support all along.

References

[1] Tejal Kognule, Yugandhara Thumbre, Snehal Kognule, 2012, "3D PASSWORD" International Conference on Advances in Communication and Computing Technologies (ICACACT).

[2] Ganesh Jairam Raj Guru, "Secure Authentication with 3D Password", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 68-75.

[3] Nayana S, Dr. Niranjanamurthy M, Dr. Dharmendra Chahar, October 2016," Study on Three Dimensional (3D) Password Authentication system," International Journal of Advanced Research in Computer and Communication Engineering.

[4] Prof. Dr.G.M.Bhandari, Naikwadi Shradha, Deshpande Gandhali, Tapkire Priya, Nawale Sanchita, September 2016, " A Survey on 3D Password," International Journal of Innovative Research in Computer and Communication Engineering.

[5] https://www.uniassignment.com/essay-samples/information-technology/secured-authentication-3d-password-information-technology-essay.php

[6] https://en.wikipedia.org/wiki/Multi-factor_authentication

[7] https://en.wikipedia.org/wiki/3-D_Secure

[8] http://1000projects.org/cse-projects.html