Enhanced Multifactor Authentication Scheme

Devender Kumar[1], Vikram Singh [2]

[1] Student M.Tech. Dept. of Computer Science & Applications, Chaudhary Devi Lal University, Sirsa, Haryana, India

[2]Prof. Dept. of Computer Science & Application, Chaudhary Devi Lal University, Sirsa, Haryana, India

***Abstract*—** *A novel user authentication scheme has been presented in terms of added dimension to the 3D password paradigm. The three dimensional password is an authentication method that combines recognition, recall, tokens and biometrics in one authentication system. This paper presents the study of 3D password in virtual environment and proposes the addition of new dimensions, namely, pattern lock and time recording.*

Keywords — *Pattern Lock, Authentication, 3D Virtual Environment, Security.*

I- INTRODUCTION

There are several physical means by which you can provide your authentication credentials to the system. The most common, but not the most secure is password authentications. The smart cards and biometric authentication types provide an extra protection. Network security hinges on two very simple goals:

1. Allowing only the authentic users to gain access to system.
2. Ensuring that authorized user can access the resources they need and unauthorised users are kept away from using the resources.

There are number of ways to accomplish these goals. One way is to assign access permissions to resources that which user can or can not access those resources and under what circumstances. Access permissions, however, work only if you are able to verify the identity the user who is attempting to access the resources. That's where authentication comes in.

In theory, authentication is simple. A user provides some sort of credentials- a password, smartcard, finger print, digital certificate- which identifies that user as the entity which it claims to be. There are, however, a multiplicity of methods and protocols that can be used to accomplish this. Regardless of the method, the basic authentication process remains the same. Authentication is an absolutely essential element of a typical security model.

Duhan et al. [4] represents 3D password system, that includes all existing authentication schemes included in a 3D virtual environmant The 3-D Password is a authentication methodology that comines recognition, recall, tokens and biometric in one authentication system. The user navigates through three dimentional virtual environment. The combination and sequence of the users actions and the interactions towards the objects in the three dimentional virtual environment constructs the users 3D password.(see fig 1)

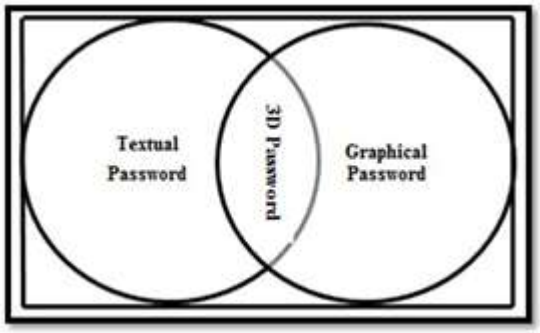

Fig. 1 : 3D Password based Multifactor Authentication Scheme

Therefore, the user can walk in the virtual environment and type environment and type something on a computer that exist in (x1,y1,z1) position, then walk into a room that has a white board that exist in a position (x2,y2,z2) and draw something on the white board. The combination and the sequence of the previous two actions towards the specific objects construct the user 3D password. The virtual object can be of any type. An object can be

1. A computer that the user can type in
2. An ATM Machine that requires a smart card and PIN
3. A light that can switched on/off
4. Any Biometric device
5. Any graphical password scheme
6. Any real life object
7. Any upcoming authentication scheme

3D Password Selection and Inputs

Consider a 3D virtual environment space that is of the size G*G*G. Each points in the three dimensional environment spaces represented by the coordinates (x,y,z) belongs to [1..G]* [1..G]* [1..G]* . The objects are distributed in the three dimensional virtual environment. Every object has its own (x,y,z) coordinates. Assume the user can navigates and walk through the 3D virtual environment and can see the objects and interact with the objects. The inputs devices for interaction

with objects can be mouse, a keyboard, styles, a card reader, a microphone etc.

User actions, interactions and input towards the objects and towards the three dimensional virtual environment are mapped into a sequence of three dimensional coordinates and actions, interactions and inputs. For example consider a user navigates through the three dimensional virtual environment [2] and types "ABC" into a computer that exists in the position of (20,7,35). The user then walks over and turns off the light located in (20,10,13). The user then presses the login button. The representations of user actions, interactions and inputs towards the objects and 3D virtual environment cab be represented as the following"

=>(20,7,35) Action = Typing "ABC"
=> (20,10,13) Action = turning the lights, off.

Two 3D passwords are equal to each other when the sequence of actions towards every specific object is equal and the actions themselves are equal towards the objects [4, 5].

3D Virtual Environment

3D virtual environment is used as basic building block of 3D password Scheme. The 3D virtual environment is created with help of a 2D screen (see fig 2).

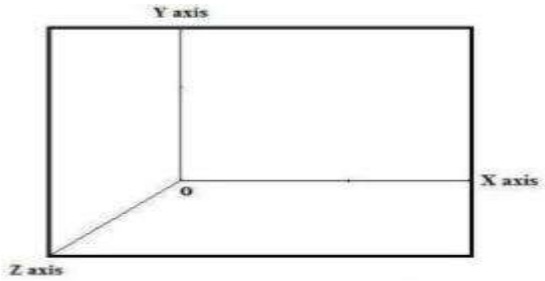

Fig. 2 : 3D Environment under 2D screen

It is a real time scenario seen by people in their daily life, which is virtually created in 3D virtual environment. Design of a 3D virtual environment affects the usability, effectiveness and acceptability of a 3D password authentication system. The design of the 3D virtual environment should follow some of the following guidelines.

1. The objects should be similar to real life.
2. Object should be uniqueness and distinction.
3. The size of virtual environment should be carefully taken.
4. No of objects and their types.
5. Position/ Alignment of the objects.
6. System importance.

II. RELATED WORK

This section describes the reviews about different authentication techniques proposed by different researcher and also shows the limitations associated with the proposed techniques using security parameters.

David et al. [6] describes a new authentication technique that is called multi-tier authentication or multi-factor authentication. This describes different authentication and authorization model which states that all the application should use more than one-tier for authentication to secure the information. This also specifies that use one time generated secret code which will be sent to the email address or mobile number.

Federal et al. [7] describe that there are various techniques that can be used to authenticate a user. These techniques include a user's password, personal information numbers (PINs), digital certificates using public key infrastructure (PKI), and physical devices such as smart cards, one-time passwords (OTP) or other type of 'tokens', biometric identification. This includes various factors for authentication.

William et al. [8] describes the use of Shared secrets for authentication. A user and service providers only know the secret password (something a person knows), nobody else knows the secret. This secret makes you differ from other users for accessing the same service. An authentication system verifies the password or shared secret to access the requested service. Examples are a password, a private key.

William et al. [8] also describes the use of Tokens for authentication. Physical devices (something the person has) are generally known as tokens. Tokens are used in all the two-factor authentications. In authentication system, first user has to provide their username and password as a first-tier authentication and then these tokens are used as second-tier authentication. Examples are a ATM card, a smart card.

Single-factor authentication process is less secure than the multi-factor authentication as stated by [7, 8] because single-factor authentication suffers from many attacks like brute-force attack, keylogger, well studied attack etc. So, there is a better choice to verify user using more than one factor for accessing the service.

Maninder Singh and Sarbjeet Singh [9] represents the design and implementation of multi-tier authentication scheme. This authentication scheme makes use of biometrics technique to verify

the user by their physical characteristics. This scheme also uses the non-hardware base one time password (OTP) scratches card. A scratch card has been given to user for one time password. At the time of authentication, the user had to provide a secret number which is provided on the scratch card. This scheme also use the out of band (OOB) authentication technique which act as a two-tier authentication in which user has to provide a username and password as a first-tier and provide secret code which is received by a user on their mobile number that is acting as second-tier. This scheme also uses the Internet Protocol Address (IPA) Location and Geo-Location. This technique works on the geographical position in which an authentication system detects the current location of the user and assumes that they will do another transaction from the same location.

Ashish et al. [10] represents a technique in which users have to authenticate themselves with the single-sign on (SSO) server for accessing the multiple services. SSO will handle all the subsequent authentications for different services, once the users are authenticate to the SSO server. Single-Sign On (SSO) is an access gaining process in which user has to authenticate once for issuing services from different applications. But the disadvantage of this technique is that the entire service system is compromised if SSO server's user credentials are hacked.

Dinesha et al. [11] represents an authentication technique in a cloud environment in which the authentication system verifies the user at different access level of cloud platform. This technique generates each level password and concatenates the all level passwords to gain an access of a requested service. At each level user provides password to gain access of each level. This technique uses the multi-factor authentication model to authenticate the user which gives an advantage over single-factor authentication. The problem arises in this technique is that user has to remember each level password which is very hectic for the user. The user has to reconsider all the level passwords if the user forgot the password of each level.

Duhan et al. [4] represents 3D password system that includes all existing authentication schemes included in a 3D virtual environment. This 3D virtual environment has different objects. User has to navigates through this environment and perform different actions. It is user's choice to select the object with which he want's to interact. The sequence of action interacting with objects will constitute the password. This paper serves a baseline for developing a multi-factor authentication scheme.

In a high security environment, multi-factored authentication adds extra protection. In other words, you can require that the user can provide more than one type of credential, such as both a fingerprint and a logon password. This further decreases the chances of an authorized person circumventing the security system. In the proposed method, not only includes all existing authentication schemes but also enhance the security of the 3D authentication system by adding pattern lock and time recording to the 3D authentication scheme.

III. ENHANCED MULTIFACTOR AUTHENTICATION SCHEME

The Enhanced multifactor authentication scheme is built in to 4th dimension of the security. The proposed methodology is an attempt to create the existing scheme even more secure, robust and powerful. We propose to add another key to the current scheme, this can lend a lot of stability and make the attacks on user privacy even tougher to reach.

This key what we have propose to refer to as the "Forth Dimension" would be an encrypted string or message that encapsulates a pattern that the user is meant to create with his fingers/stylus on a devices such as PDAs, aside from his password. Hence the final form of the password will be

Pattern Lock + 3D Password

In this authentication technique, the user shall draw a pattern by joining points on a 3*3 matrix in his/her chosen order. This pattern must involve minimum of 4 points of the matrix are registered in a numbered order starting by 0 in the upper left corner and ending by 8 in the bottom right corner. The system works by matching the input pattern with the stored pattern at the time of password registration (see fig 3).

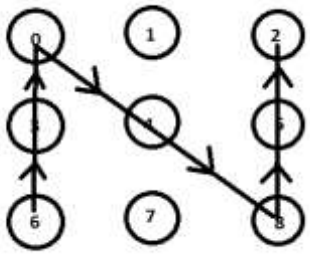

Fig. 3 : 3*3 Pattern

Originally pattern lock was introduced in 2008 and was presented as both easier and more secure alternatives to traditional numeric passcodes. While standard four digit pin gives users 10000 possible combinations, a secure lock pattern with 9

distinct nodes can yield 389112 possible patterns, while one might think that this makes system inherently secure. The 3*3 points of the pattern lock can be represented by numbers, in fact, the points are registered in order starting 0 to 8. The pattern lock data is stored in an unsalted SHA-1 encrypted bytes sequences format. This means that, for example instead of storing directly 6405862, it stores an encrypted byte array in a system file.

In addition of the above, this approach ensures that the physical presence of individual person for login session and not an automated program are there. One more constraint is applied here, the measure of total time taken for the 3D authentication by the user. This time is also considered a part of the user's authentication and user must perform subsequent authentication within the same time period or it may be take few seconds more or less is also taken into consideration by the system itself.

This "new security approach " lets you avoid any undesired taps on the system and it will ask to authorize its access. This manipulation seems to be complicated and secure enough.

IV. MODUS OPERANDI

Fig. 4 shows the working of enhanced multifactor authentication scheme.

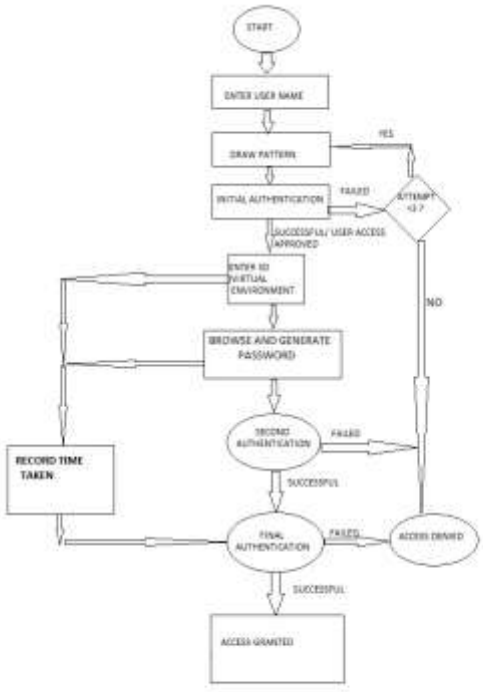

Fig. 4 : Working of Enhanced Multifactor Authentication Scheme

V. *Signup Process/ Registration Process:*

The user has to perform following steps for sign in authentication process;

1. The user has to choose an username.
2. Then it will be redirected to the password generation phase.
3. It will enter the 3D virtual environment.
4. In the 3D environment, the user has to perform certain action.
5. Then user has to exist from the 3D virtual environment and submit these actions
6. Then user has to draw pattern by joining points on a 3*3 matrix in his/her order on PDAs. Once this pattern is successfully captured then it will be saved.
7. The user has to remember it for subsequent attempts at login signup process is complete.

B. Logging in:

When user logs in**,** he/she has to enter the user name and draw the pattern. After successful submission and verification of it, the user will enter into the environment and perform the password or sequence of actions. Then user will exit and submit it. Once it is verified, the user will be allowed to access the services.

In enhanced multifactor authentication scheme, the addition of pattern lock gives more secure way of authentication, This " new security approach" lets you avoid any undesired taps on the system and it will be asked to authorize its access. This manipulation seems to be complicated and secure enough.

In addition to the above, this approach ensures that the physical presence of individual person for login session and not an automated program are there. One more constraint is applied here, the measure of total time taken for the 3D authentication by the user. This time is also considered a part of the user's authentication and user must perform subsequent authentication within the same time period or it may be take few seconds more or less is also taken into consideration by the system itself. On the basis of the time taken, certain conclusion can be drawn:

1. If the time taken by the user to the last authentication is very large, then it may be possible that some unauthorized user is attempting to do illegal action.
2. If the time taken by the user is close to zero, it might be attempt made by an automated system program to hack the authentication procedure.

The addition of time factor will make the authentication process more powerful and robust.

Security Analysis

A. Brute Force Attack:

Brute force attack is difficult in the proposed scheme because the unauthorized user has to try all the possible combination of all the objects and remember the sequence of actions performed with these objects. There are large number of objects in the 3D virtual environment, but similar kind of objects may be there which may confuse to unauthorised user. The addition of pattern lock with time limit makes this authentication scheme stronger against brute force attack. It will be difficult for the attacker due to following reasons:

1.) The 3D virtual environment contains text, graphics, biometric recognition object and token based objects, the attacker has to forge all text, graphics, biometric information and all required tokens. The cost of forging such information is high.

2.) The time required for the authentication process may be vary from 20 sec to 2 min or more, depends upon the actions performed with objects, types of actions and size of 3D virtual environment. Therefore a brute force attack is very difficult and time consuming.

3.) Memory utilization is very high thanks to large 3d password space. The computer may freeze before reaching the key combination due to the high complexity of the algorithm required.

1.) Keylogger:

A keylogger is a type of surveillance software, considered to be either software or spyware that has the capability to record every keystroke you make to a log file. A key logger recorder can record instant messages, e-mails and any information you type at any time using your keyboard. In this way the unauthorised user tries to record the user's password, but in this authentication, it will not be able to capture the pattern, graphical, biometric, token so the software will be a total failure.

2.) Well Studied Attack:

In this threat, the unauthorized user will study the whole authentication process followed with the most probable password use by the user and for the 3D password, the attacker try to know the sequence of actions perform on objects. In enhanced multifactor authentication method, the addition of pattern lock makes it impossible for the attacker. It becomes difficult for the attacker to unlock the pattern and get the 3d password, because addition of pattern lock prevents the functionality of 3D virtual environment.

V. CONCLUSIONS

It has been shown that multifactor authentication surely makes the login process much easier and also provides the user a hassle-free login. This also provides the users flexibility to choose the level of desired security as per their preference or requirement. The enhanced multifactor authentication scheme combines the features of existing authentication such as biometric scanning, text and graphical passwords, token recognition scheme and also add new dimension to the 3D password virtual environment i.e. pattern recognition system.

The enhanced multifactor authentication scheme is much better and by randomizing it with different authentication schemes, can be used effectively, which makes the system sustainable and secured against the guesswork of hackers. It is also very powerful against attacks. The first two layers text and graphics can be easily broken via conventional brute force and shoulder surfing techniques. The addition of pattern lock with time constraint to the 3D authentication makes it stronger and ensures the physical presence of the authorised user to access the system.

The proposed authentication scheme is flexible in terms of number of permutation and combinations, for multiple factors such as pattern lock, biometric, graphical and textual password are combined to create a security barrier. Further, the proposed authentication scheme provides the user a freedom to create multilevel security. Owing to a very large password space it can be used for providing security to nuclear, military, and cloud computing facilities

ACKNOWLEDGMENT

The authors would like to thank the publishers, researchers for making their resources available and Dr.Dilbag Singh, Chairman, Deptt. Of Computer Science & Applications, CDLU, Sirsa for their guidance. We would also thank the dept. Authority for providing the required infrastructure and support. Finally, we would like to extend heartfelt gratitude to friends and family members.

REFERENCES

[1] X.Suo, Y. Zhu, and G.S Owen (2005), *"Graphical Passwords: A survey,"* in Proceeding of 21st Annual Computer Security Conference, December 5-9, 2005, pp. 463-472.

[2] Vishal Kolhe, Vipul Gunjal, Sayali Kalasar, Pranjal Rathod (2013), *"Secure Authentication with 3D Password,"* International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 2, Issue 2, March 2013.

[3] Grover Aman, Narang Winnie (2012), *"4-D password: Strengthening the authentication scene,"* International Journal of Scientific and Research Publications, volume 3, Issue 10, October-2012.

[4] Duhan Puja, Gupta Shilpi, Sangwan Sujata and Guwati Vinita, *"Secured Authentication: 3D password",* in International Journal of Engineering and Management Sciences (IJEMS).

[5] Banita Chadha, Dr Puneet Goswami (2014), *"3D Password- A secure tool,"* International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4 issue 1, pp. 890-893, January 2014.

[6] David Chou, (2008), *"Strong user authentication on the web,"* on website http://msdn.microsoft.com/en-us/library/cc838351.aspx, August 2008.

[7] Federal Financial Institutions Examination Council. Authentication in an internet banking environment, 2011.

[8] William E Burr, Donna F Dodson, and William T Polk (2004), *"Electronic authentication guideline,"* Citeseer, 2004.

[9] Maninder Singh and Sarbjeet Singh (2012), *"Design and implementation of multi-tier authentication scheme in cloud,"* International Journal of Computer Science Issues (IJCSI), vol. 9, no. 5, 2012.

[10] Ashish G Revar and Madhuri D Bhavsar (2011), *"Securing user authentication using single sign-on in cloud computing,"* in NUICONE2011, Nirma University International Conference on Engineering, pages 1-4, IEEE, 2011.

[11] HA Dinesha and VK Agrawal (2012), *"Multi-level authentication technique for accessing cloud services,"* in ICCCA2012, International Conference on Computing, Communication and Applications, pages 1-4, IEEE, 2012.