Multi-Dimensional and Multi-Level Authentication Techniques

Tanvi Naik
Final year Engineering
Department of Information
Technology, SKNCOE, Pune

Sheetal Koul
Asst. Professor
Department of Information
Technology, SKNCOE, Pune

ABSTRACT
Current authentication schemes suffer from many weaknesses. Textual passwords are widely used; however users tend to choose meaningful words from dictionaries. This makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords face lack of space. Smart cards or tokens can be lost or are prone to theft. Many biometric authentications have been proposed but users tend to resist using them because of their intrusiveness on their privacy. The three-dimensional (3-D) password is a multifactor authentication scheme i.e. it combines most of the existing authentication schemes such as textual passwords, graphical passwords, and biometrics into a single virtual three-dimensional environment. Users navigate through this virtual environment and interact with the objects placed in it. The combination of all the actions and inputs towards the virtual three-dimensional environment constructs the user's 3D password.
Simple approach for a secure authentication is to use one or more of the above mentioned authentication techniques in combination for multi-level authentication, so that, the probability of breaking such a password is reduced to a large extent. Hence multi-level authentication technique can be used for ensuring a more stringent authentication.

General Terms
Password, Security, Algorithm, Complexity, Authentication, Encryption, Concatenation, Authorization

Keywords
Three dimensional, four dimensional, Biometrics, Virtual environment, USB drives

1. INTRODUCTION
Authentication is basically a process of validating who the user is. Many techniques are used for this purpose. Some of the commonly used techniques are-

1) Textual Passwords
2) Graphical Passwords
3) Token-based Passwords
4) Biometric Authentication

Each of these techniques has its own set of advantages and disadvantages [1]. Textual passwords are one of the most widely used authentication techniques. They are easy to implement. But as per a survey it was found out that 25% accounts out of 15,000 accounts having alphanumeric passwords were easily guessed by using a well formatted dictionary of 3X106 words [2]. This is mostly due to the user's carelessness in selecting a known password rather than a random one. Graphical passwords are hard to guess [3][4][5] but they are prone to shoulder-surfing attack. I.e. the attacker observes the legitimate user perform the graphical passwords and then imitate it. Tokens do not require the user to memorize the password [6] but they are vulnerable to loss or theft. Biometric passwords are unique for every individual. Unlike textual passwords they need not be memorized and they cannot be stolen [1]. But many users refrain from using biometric passwords due to intrusion on their privacy. Also special scanning devices are needed to authenticate the users which aren't available everywhere.
To overcome these drawbacks, 3-D passwords are introduced. The 3-D password is a multi-factor authentication scheme. I.e. it has the ability to combine all the existing authentication schemes in a single three dimensional virtual environment. Along with the correct authentication, the sequence of undergoing verification tests is also important. It is simply a sequential combination of user interactions that occur in the 3-D virtual environment.
For advanced security, multidimensional passwords can be implemented at multiple levels in the organization. I.e. Combining one or more passwords entered at various levels which will together act as a new password. This can be done by concatenating the passwords entered at various levels. This implementation of passwords at different levels will provide additional security along with prevention of unauthorized user access even if one of the passwords from the generated string is known.

2. MULTI-DIMENSIONAL AUTHENTICATION
Multi-dimensional authentication is the combination of the existing authentication techniques into one virtual environment. The user will perform series of authentications to verify him to the system. Authentication techniques like textual & graphical passwords, tokens and biometrics can be included in the virtual environment as per the availability of devices. The best example of multi-dimensional authentication is a 3-D password.

2.1 Three-Dimensional (3-D) Passwords
In 3-D passwords on entering user's login ID, for accepting the password, a virtual three dimensional environment opens up [7]. In this environment, the user can interact with various objects (refer Figure 1). For example, the user's password can comprise of the following steps-

1) He can walk from one place to another (The curser can be used for this purpose)
2) Move objects from their current places
   This change of location can be from one place i.e. (x1, y1, z1) co-ordinates to other place (x2, y2, z2) co-ordinates.

Objects can be placed at these positions to depict the co-ordinates and for simplicity of finding the exact positions. For e.g. if the virtual environment depicts a library, as a part of the password, if a book needs to be shifted from one place to another, then two racks can be placed at positions (x1,y1,z1) and (x2,y2,z2) respectively.

3) Play an audio
   (The music clip can be the one from the available ones in the device or from some external inputs. E.g. USB drives)
4) Give biometric inputs
   (By using touch pads for finger tip security, web cameras for face recognition, etc.)

Etc.

These interactions with the virtual environment will together form the password of the user [8].

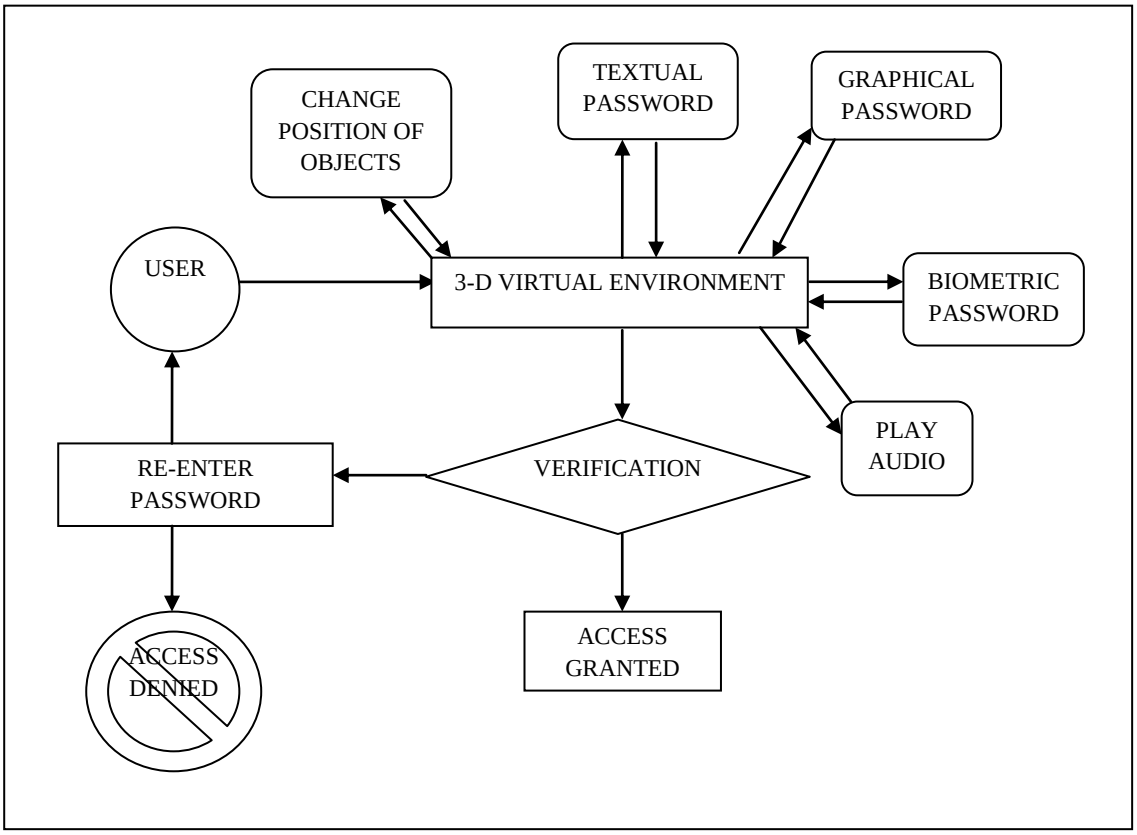

Figure 1: Graphical representation of 3-D passwords

For e.g., for accepting the password, a virtual environment will open up which will resemble a room. The user can walk in the room and switch on particular lights and fans. Then he can walk to the music system and play a particular song from one of the available albums. Then he can go to one of the windows and draw the curtains. Performing all these actions in the same sequence will form the user's password.

Correct selection and performance of actions and that too in the same sequence will grant access to the user[9]. I.e. for the above mentioned example, the user on entering the room will need to switch on the correct number of lights and fans out of all the available ones by clicking on them or by pressing the buttons on the switch. Then he needs to walk to the place where music system is placed. Out of the many available albums placed in the rack, the user needs to select the right one by clicking on it. Then he needs to walk towards one of the windows in the room. He can draw the curtains by clicking on them and then dragging them to one of the sides.

Action performed at each stage gets encrypted. Later all the encrypted codes are concatenated. This forms the final password for the user [10]. Change in the sequence of these actions will not grant access to the user [11].

2.2 4-D Passwords

For additional security, a fourth dimension can be added. The user will need to perform some actions in front of the camera as one of the components of his password. These actions can be in the form of hand movements, gestures, etc. This will increase the complexity of the password tremendously. Hence the probability of the attacker cracking the password and entering the system will be significantly reduced [12].

Time required by the user to perform the series of actions can be recorded and saved. Next time whenever the system will be accessed, time taken by the user to enter the password will be checked too. Minute variations in time can be ignored by the system. But if any other unauthorized person is trying to access the same system, he will not get time to think and perform the actions. This will greatly reduce the chances of successful breakthrough of the attacker. Even if a robot is trying to crack the system, he will be unsuccessful as he will require time close to 0 seconds to perform the same action.

In general, 4-D password = 3-D password + gesture

2.3 Advantages of Multi-Dimensional Passwords

Multi-dimensional passwords are hard to crack, as inclusion of more than one authentication technique increases the complexity of the password. The user can select which authentication techniques he should use to create his password. This selection can be done on the basis of available devices. For e.g. biometric devices may not be available everywhere. So in such cases, the user can opt for combination of textual, graphical and token based password for creating his 3-D password. 3-D passwords are easy to remember as they consist of sequence of events and actions. User can select the type of virtual environment he wants. For e.g. Room, Library, Workplace etc. Provision of timer will further decrease the probability of trespassing the system.

3. MULTI-LEVEL AUTHENTICATION

This technique authenticates data at multiple levels. It generates passwords at multiple levels and then concatenates them into one single password [13]. The main difference between multi-level authentication and multi-level authentication is that, in multi-dimensional authentication, entire password must be entered at once. In multi-level authentication, password is entered in stages. On each correct password, privileges for that level are granted. Resources corresponding to that level and the levels below can be accessed by the user. This helps to keep a check on the privileges/access rights available for the user. The first level of authentication is at organizational level. On entering the correct password at this level, basic access to the organization is granted. Unauthorized users/hackers are terminated at this level. The second level of password can be at departmental level. This helps in securing data of individual departments. In this way, the system can ask for authentications at multiple levels.

Password for next level will be concatenation of the passwords entered for previous levels and the one required for the next level. This will ensure that the user has undergone all the necessary security checks of the previous levels.

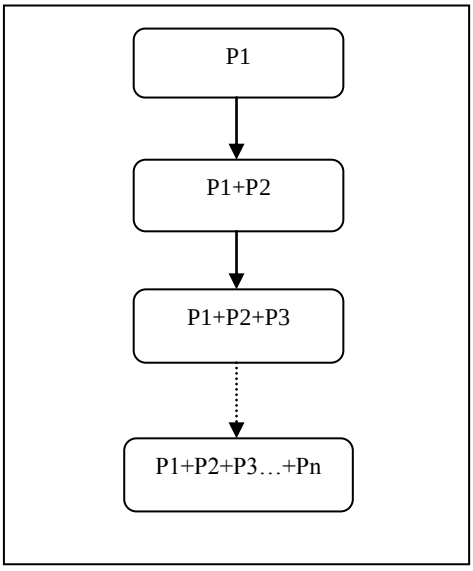

Figure 2: Implementing passwords at multiple levels

Figure 2 indicates structural implementation of multi-level password authentication. To access Level-1, password 'P1' is required. On correctly entering P1, privileges for Level-1 are granted. To access Level-2, correct entering of P1 as well as P2 is required. On entering password P2, passwords P1 and P2 are concatenated. If both are right, only then the access to Level-2 is granted. Now the user can access privileges of Level-1 as well as Level-2. So, even if a user directly enters the correct password- P2 for accessing Level-2, access will be denied as password for Level-2 is the concatenated password of Level-1 and Level-2 respectively. Similarly, for accessing Level-3, correct entering of passwords P1, P2 and P3 is necessary. After their concatenation and verification of the generated string, access to Level-3 is granted. In the same way, this system can be applied to n levels.

3.1 Algorithm

Enter P1
If P1 is correct
    Grant access to Level-1
    Enter P2
    Concatenate P1 and P2
    If generated string is correct
        Grant access to Level-2
        Enter P3
        Concatenate P1, P2 and P3
        If generated string is correct,
            Grant access to Level-3
            .
            .
            …Similarly for levels up to Level-n

3.2 Advantages of Multi-Level Authentication

Multi-level authentication makes the security measures of the organization more stringent. Even if the intruder is aware of a particular password, it will not be of any help to him as password to any new level is the concatenation of the new password with all the passwords belonging to the previous levels. Hence circumnavigating the security measures is not possible unless and until all the passwords are known. Inclusion of biometric passwords as one of the security measure in the authentication process will make the system almost impossible to crack.

4. PROPOSED METHODOLOGY

Multi-dimensional and multi-level passwords have a lot of advantages over normal security measures when any one of the available authentication techniques is applied individually. Hence for higher security, these two techniques can be combined. I.e. application of multi-dimensional password at each level as an authentication measure. This will drastically increase the security of the system. It will make it difficult for the intruder to crack the system.

Application of this methodology can be done in two ways-

1) Lateral Application
2) Hierarchical Application

4.1 Lateral Application

This approach is similar to multi-level authentication. Data is secured level wise. I.e. for every series of correctly entered passwords, data belonging to that particular level will be made accessible. For example, consider figure 3.

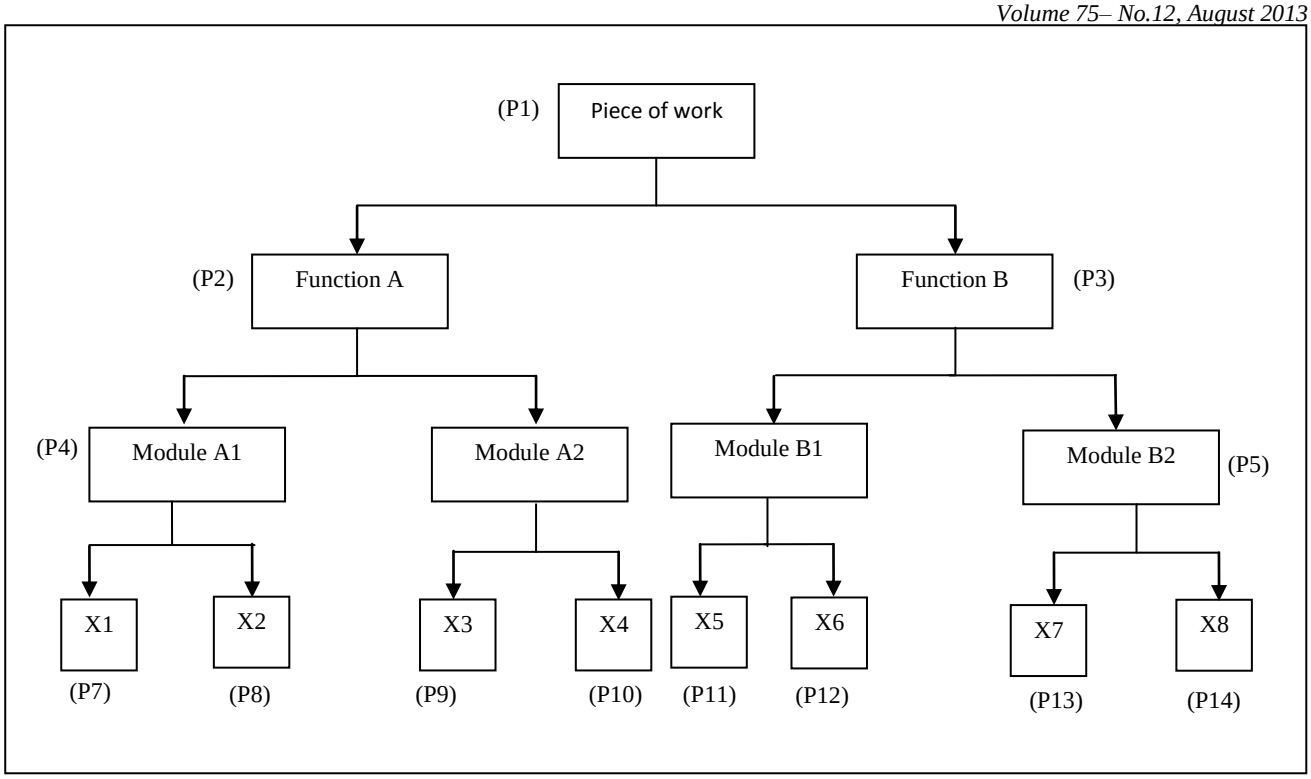

Figure 3: Lateral application implementation of multi-level passwords

For accessing piece of work, password P1 is needed. If correct, access to resources at the most superficial level is granted. I.e. information about the piece of work can be accessed. This piece of work is further divided into two functions- Function A and Function B. For accessing Function A, passwords P1 and P2 are required. If after concatenation, the generated string is right, then access to Level-2 is granted.

Thus at this level, information about Function A is accessible. Similarly for Function B. Function A is divided into modules A1 and A2. To access module A1, concatenation of correct passwords P1, P2 and P4 is requires. Thus the process continues further for n number of levels. At the last level, individual data is accessible. Hence at this level, password for every individual (X in this case) is different.

This method is useful in an organization where work is divided into subparts which are further divided into individual components. Thus data is secured functionally as well as level wise. Data belonging to one function is protected from the other functions. Inside a function, data is protected in a similar way but at a modular level. Two modules are protected from each other. At the end of the system there are individuals. Their data too is protected from each other by individual passwords. Thus this method ensures functional/modular security.

For effective security, Multi-dimensional passwords can be used at every stage for secured authentication. Usage of biometric passwords as one of the authentication measure will ensure complete uniqueness of passwords, especially at individual level. The usage of Tokens will mark each and every person's entry in the system [6].

4.2 Hierarchical Application

In this application, various hierarchical levels of the organization are secured by passwords. First level of authentication will be at the most generalized level. I.e. in this case (Figure 4) it is at the Employee level. On entering the correct password, access to data/resources available at Employee level will be granted. To access data available at Team Leader level, correct entering of passwords concatenation of P1 and P2 matches with the initially set password, only then access to resources at Team Leader level is granted. Similarly for accessing data at managerial level, correct entering of passwords P1, P2 and P3 is necessary.

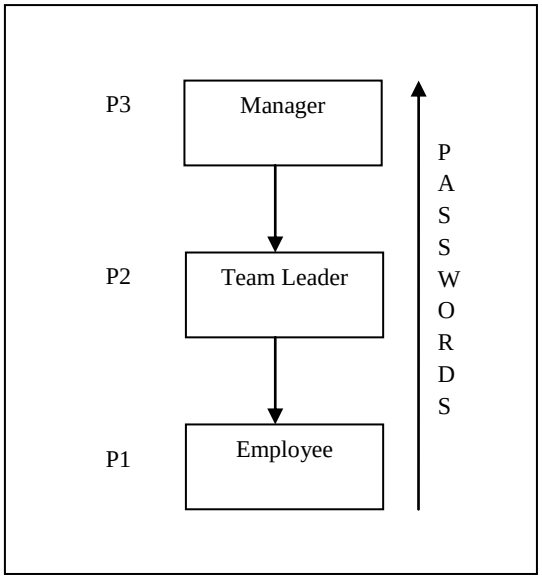

Figure 4: Hierarchical application implementation of multi-level passwords

If passwords P1, P2 and P3 are multi-dimensional passwords, then the complexity of the overall passwords is greatly increased. Information tends to get more confidential as there is rise in managerial levels. This method helps to ensures higher security as the managerial levels increase. I.e. security for information available at Managerial level is higher than that at Employee level.
This method can be implemented to n number of hierarchical levels in the organization and ensure data security across various organizational levels of the institution.

4.2.1 Mathematical Calculations

Consider a system as shown in Figure 5. It consists of 2 managerial levels- Level A and Level B. Multi-dimensional passwords are applied at each level for security purposes. I.e. passwords A1, A2 and A3 together form the password for Level A and B1, B2 and B3 together form the password for Level B. Therefore, to access resources or privileges available at Level B, the expected password will be A1A2A3B1B2B3.

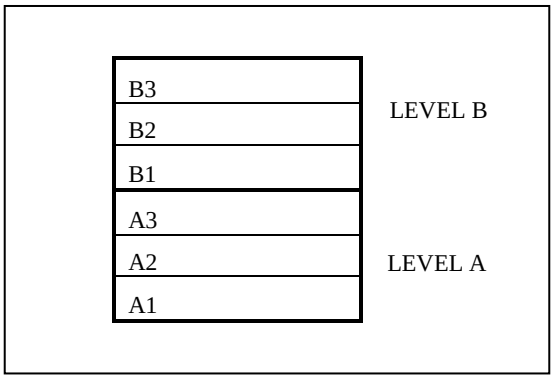

Figure 5: Application of multi-dimensional passwords at multiple levels

Let E be the event of cracking the system password. The event can either be a success or a failure. Let 'k' be the probability of success at each sub-level. So in order to crack the system, initially Level A needs to be cracked and then Level B. Therefore, the probability of cracking Level A successfully is $P(E)=k^3$. Assuming k=0.1, the possibility of successfully cracking A will be 0.001.
I.e. P(A)=0.001
Similarly probability of successfully cracking Level B will be 0.001.
I.e. P(B)=0.001
Probability of cracking Level B will be taken into consideration only when Level A is successfully cracked. Hence the probability of completely cracking the system is very less. This depicts a high degree of authentication offered by the system.

4.2.2 Drawbacks

If the manager betrays the organization, the entire system is likely to be exposed. This is because the manager is aware of all the passwords of his subordinate levels. To overcome this drawback, the password can be split among two or more people as shown in Figure 6.

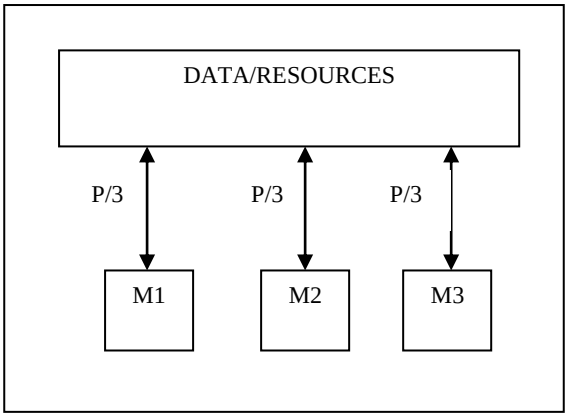

Figure 6: Splitting up of a password among two or more people

In Figure 6, M1, M2 and M3 are the three managers who have access to the same data/resources at the managerial level. P is the password that is required by the system to grant access to this data. In order to overcome the drawback of the above mentioned betrayal problem, the password is divided into same number of parts as the number of people. In this case, the password is divided into three parts. Each manager is aware only about his one-third part. But in order to access the resources, all three of them need to enter their part of the password. Hence even if one of them decides to betray the system, the entire system will not be exposed as the access to the data is not solely based on one person's password. Inputs from all three of them and that too in the right order are necessary [14].

5. FAULT TOLERANCE

This system is safe from brute force and dictionary attacks. 3-D passwords are easy to remember. They cannot be imitated easily. Usage of biometrics and gestures (4-D password) make the authentication process even more stringent. Multi-level passwords prevent unauthorized users from entering the system even if they are aware of one of the passwords. Combined application of Multi-dimensional and Multi-level passwords gives superior security to the system and makes it almost impenetrable. Dividing a password among two or more people in such a way that each one is aware only of his own share,

gives extra secure edge to the system as leakage of one of the passwords will not expose the entire system.

6. DISADVANTAGES

In order to implement multi-dimensional passwords at multiple levels, large amount of memory space is required. One needs to remember a series of passwords. It is also a time consuming process considering every person needs to give multiple authentications at various stages in the organization. The need of biometric devices increases the cost of the system considerably.

7. CONCLUSION

Multi-dimensional passwords are proven to be far more secure as compared with the current authentication techniques implemented individually. Passwords at multiple levels in the organization ensure higher security by eliminating unauthorized users at the very initial stages. Combination of both these techniques continue to provide higher security to the organization's resources. Concatenation of various passwords across various levels makes the authentication process more stringent. For further improvising the security measures, the password can be split among two or more people in order to prevent exposure of system in case one of them is unable to guard the password.

8. ACKNOWLEDGMENTS

We sincerely thank all the staff of SKNCOE, friends and family for their constant support and encouragement.

9. REFERENCES

[1] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon: "Authentication using graphical passwords: Basic results." In Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25-27 2005

[2] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik: "A Novel 3-D Graphical Password Schema". VECIMS 2006- IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, La Coruña – Spain, 10-12 July 2006

[3] Arash Habibi Lashkari and Samaneh Farmand: "A survey on usability and security features in graphical user authentication algorithms." IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.9, September 2009

[4] Darren Davis, Fabian Monrose and Michael K. Reiter: "User choice in Graphical Password Schemes." Proceedings of the 13th USENIX Security Symposium, San Diego, August 2004

[5] X. Suo, Y. Zhu, G. S. Owen: "Graphical passwords: A survey" in Proc. 21st Annual Computer Security Application.

[6] Xuguang Ren ; Xin-Wen Wu: "A novel dynamic user authentication scheme." Communications and Information Technologies (ISCIT), 2012 International Symposium on Digital Object Identifier: 10.1109/ISCIT.2012.6380995

[7] Mr. Namdev A. Anwat, Mr. Dattatray S. Shingate and Dr. Varsha H. Patil: "A Secure Authentication Mechanism using 3D Password" International Journal of Advance Research in Science, Engineering and Technology, Vol.01, Issue 01, pp. 29-37

[8] Duhan Pooja, Gupta Shilpi, Sangwan Sujata and Gulati Vinita: "Secured Authentication: 3D Password". International Journal of Engineering and Management Sciences VOL.3(2) 2012: 242 – 245

[9] Ms. Vidya Mhaske-Dhamdhere and Prof. G. A. Patil: "Three dimensional Object Used for Data Security". 2010 International Conference on Computational Intelligence and Communication Networks

[10] Praseeda K Gopinadhan, Renjith P R, Biju Abraham Naremparambil: "Passaction: A New User Authentication Strategy Based on 3D Virtual Environment" *IRACST* - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol. 2, No.2, April 2012

[11] Daniel V. Klein: "Foiling the Cracker: A Survey of, and Improvement to Passwords Security." Proceedings of the USENIX Security Workshop, 1990

[12] Grover Aman and Narang Winnie: "4-D Password: Strengthening the Authentication Scene" International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012, ISSN 2229-5518

[13] Dinesha H A and Agrawal V K: "Multi-level Authentication Techniques for Accessing Cloud Services". CORI, Bangalore. Karnataka

[14] Harn, L.: "Group Authentication" Computers, IEEE Transactions on Volume: 62 , Issue: 9 Digital Object Identifier: 10.1109/TC.2012.251 Year: 2013