DOI: https://doi.org/10.53555/nncse.v2i3.491 **Publication URL: http://nnpub.org/index.php/CSE/article/view/491**

4-D AUTHENTICATION SYSTEM USING MOUSE GESTURE

Prof. Nilima Nikam[1]*, Karishma Mane[2], Minal Kalkute[3], Ankita Sankhe[4], Leena Mondkar[5]

*[*1,2,3,4,5]Department of Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Bhivpuri Road, Karjat*

Corresponding Author-:

Abstract: -

*Computer technology is reaching new milestones with every passing day but **authentication schemes** are still weak in their approach. Many cases of forgeries hacked accounts are coming up every day. Many authentication schemes have been proposed but each has some drawbacks. Hence, the 3D authentication scheme has been introduced. The 3D password is a multi-layer, multifactor authentication mechanism. It consists of a 3D virtual environment on which a user has to perform certain actions. The sequence of user interactions determines the user's 3D password. It combines all existing authentication schemes like textual, graphical and bio-metrics into a single 3D virtual environment. This report presents a study of the 3D password and an approach to strengthen it by way of adding a Fourth dimension (4D), that deals with gesture recognition and time recording, and that would help strengthen the authentication paradigm altogether. Hence, we attempt to propose a **4D password** as a super class of 3D password.*

Keywords: - *Authentication, Biometrics, 3d environment, Graphical password, Textual password, Virtual Environment, 4D passwords*

I. INTRODUCTION

AUTHENTICATION

is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a user name and password? Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:

1. Knowledge Base (What you know)
2. Token Based (What you have)
3. Biometrics (What you are)
4. Recognition Based (What you recognize)

Computer Authentication Techniques are as follows:

1. Textual Passwords
2. Graphical Passwords
3. Biometric schemes (fingerprints, voice recognition etc.)

Since many years it has become an interesting field of study. Also, with the development in means of technology, improvement in the methods for authentication has also given way to more sophisticated means of attacking an individual's privacy, or what we know as hacking. We are provided with many password types such as textual passwords, bio-metric scanning, tokens or cards (such as an ATM card) etc. But there are many weaknesses in current authentication systems. The most common computer authentication method is to use alphanumerical user names and passwords. One of the main problems is the difficulty of remembering passwords. Users tend to pick short passwords as these are easy to remember. But these passwords can also be easily guessed or broken. Since user can only remember a limited number of passwords, they tend to write them down or use the same passwords for several accounts. A solution to problems with traditional user name password authentication is, alternative authentication methods, such as bio-metrics [2, 6] .Bio-metric scanning is your "natural" signature and Cards or Tokens prove your validity. Graphical passwords can also be used. One of the strong point for graphical passwords is that pictures are easier to remember than text strings. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords. Token based techniques, picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images user selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that user created or selected earlier during the registration stage.

II LITERATURE REVIEW

Several authentication protocols have been proposed to integrate bio-metric authentication with user name and password authentication and/or graphical authentication. However, given the limited candidate faces on the screen, the security of Pass faces is vulnerable to trial attacks. Convex Hull Click [1] is developed to overcome the problem of passwords that are vulnerable to shoulder surfing in a public environment. It motivates the users to log in quickly and accurately. The suggested number of icons to ensure a large password space makes the screen crowded for users to find out the right click region. It was also be found that, the Convex Hull occasionally formstoo narrow a space for users to click on. Another shoulder surfing resistant graphical password scheme is obtained by adding a light graphic layer to traditional textual-based password scheme [8]. The scheme has proved to be effective against shoulder surfing attacks, and yet as it is alphanumeric-based, it contains the inevitable drawbacks of alphanumeric passwords. Token based techniques, such as key cards, bankcards and smart cards are widely used. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images user selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that user created or selected earlier during the registration stage

III AUTHENTICATION SCHEMES

What is BIOMETRICS?

"Bio metrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with bio-metrics is security. However, bio-metrics identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities.

A number of bio-metric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics, we mean the using the features such as face, iris, fingerprint, signature etc. The method of identification based on bio-metric characteristics is preferred

over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on bio-metric techniques obviates the need to remember a password or carry a token. A bio-metric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Bio-metric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".
A bio-metric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification – One to Many: Bio-metrics can be used to determine a person's identity. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.
Verification – One to One: Bio-metrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan. Bio-metric authentication requires to compare a registered or enrolled bio-metric sample (bio-metric template or identifier) against a newly captured bio-metric sample (for example, the one captured during a lo-gin). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process. During Capture process, raw bio-metric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw bio-metric sample and convert into a processed bio-metric identifier record (sometimes called bio-metric sample or bio-metric template). Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the bio-metric - not the original bio-metric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed bio-metric sample only. The original bio-metric sample cannot be reconstructed from this identifier.

Advantages
1. 3D Password scheme is combination of re-call based, recognized based, Bio-metrics. etc into single authentication technique.
2. Due to use of multiple schemes into one scheme password space is increased to great extent. More secure authentication scheme over currently available schemes.

Disadvantages
1. Time and memory requirement is large.
2. Shoulder-suffering attack is still can affect the schema.
3. More expensive as cost required is more than other schemes

IV.3D-AUTHENTICATION SYSTEM
The 3D Password scheme is a relatively new authentication scheme that combines **RECOGNITION+RECALL+TOKENS+BIOMETRIC** in one authentication system. The 3-D password is a multifactor authentication scheme. It can com- bine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by combining the actions and interactions of the user and the sequences of such actions. It is the user's choice to select which type of authentication techniques will be part of their 3-D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user simply skips interaction with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large number of objects and items in the environment, the number of possible 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password.

System Implementation
Since the 3D password is a multifactor authentication scheme [8], it presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of the user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and bio-metrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and bio-metric data to be verified. For example, the user can enter the virtual environment and type something on a computer that exists in (x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the user can
go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user's 3D password. Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions towards the real-life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password. We can have the following virtual objects, for instance:

1. A keyboard wherein the user can type an alphanumeric user name and password.
2. A fingerprint reader that requires the user's fingerprint.
3. A biometric recognition device.
4. A paper or a white board that a user can write, sign or draw on.
5. An ATM machine that requires a smart card and PIN.
6. An appliance that can be switched on/off.
7. A television or radio where channels can be selected.
8. A staple that can be punched.
9. A car that can be driven.
10. A chair that can be moved from one place to another.
11. Selecting any spot from a picture which is implementation of graphical password scheme

Working:
Consider a three-dimensional virtual environment space that is of the size S×S×S. Each point in the three-dimensional environment space represented by the coordinates (x, y, z) € [1...S] × [1...S] × [1...S].
The objects are distributed in the three- dimensional virtual environment. Every object has its own (x, y, z) coordinates. Assume the user can navigate and walk through the three-dimensional virtual environment and can see the objects and interact with the objects. The input device for interactions with objects can be a mouse, a keyboard, stylus, a card reader, a microphone etc. For example, consider a user who navigates through the 3D virtual environment that consists of a ground and a classroom. Let us assume that the user is in the virtual ground and the user turns around to the door located in (10, 16, and 80) and opens it. Then, the user closes the door. The user types "HELLO" into a computer that exists in the position of (18, 5, and 20). The user then walks over and turns off the light located in (15, 6, 20), and then goes to a white board located in (55, 3, 30) and draws just one dot in the (x, y) coordinate of the white board at the specific point of (420,170). The user then presses the lo-gin button. The initial representation of user actions in the 3D virtual environment can be recorded as follows:
(10, 16, 80) Action = Open the office door; (10,
16, 80) Action = Close the office door; (18, 5, 20)
Action = Typing, "H"; (18, 5, 20) Action = Typing, "E"; (18, 5, 20) Action = Typing, "L"; (18, 5, 20) Action = Typing, "L"; (18, 5, 20) Action = Typing, "O"Action = Turning the Light Off; (55, 3, 30) Action = drawing , point = (420,170);
After the user has performed these actions, he will exit out of the 3-D environment. After back-end verification, access will be granted.

Drawbacks:
- Time and memory requirement.
- Cost of Implementation and maintenance.
- Limited mobility: When a 3-D Secure confirmation code is required, if the confirmation code is sent by SMS on mobile phone (assuming she/he owns one) the customer may be unable to receive it depending on the country he currently is in (not every mobile network accepts SMS). The system is also not convenient for customers who tend to change mobile numbers from time to time - such as due to travel-ling (and some banks require a visit to their office to change the mobile number on the account).

V.4-D AUTHENTICATION SYSTEM

The 4-D Password scheme is an attempt to make the existing scheme even more robust and powerful. We propose to add another dimension to the current scheme, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. This key, what we propose to refer to as the 'FOURTH DIMENSION would be an encrypted string that encapsulates a gesture that the user is supposed to make with his mouse pointer, apart from his password. This will help ensure that the user is physically present for lo-gin. Hence, the final password of the user would be: Mouse Gesture + 3-D Password. Now let's have a closer look as to how this gesture would be generated and saved. We have a mapping function F(x), such that if we put V as the input string, then it creates F (V), which is our final encrypted key. The user does not need to bother with any of these. All he needs to do is remember the gesture, which would be captured as a binary string S. The String V would then be encrypted and appendedto the already existing password. Hence, the end result would be a password that looks like this:P = 3-D password + F (V).

METHODOLOGY

Consider a web-based repository of research work for scientists, wherein each scientist has his own account which stores his files and folders

This repository employs the 4-D password scheme. As a new user, user will sign up as follows:
1. Choose a username.
2. User will be redirected to the password generation page.
3. User will enter the 3-D environment.
4. Inside the environment, user will perform interactions with virtual objects in the virtual environment.
5. User will exit out of the environment and submit actions. These interactions will be saved as 3-d password.

6. User will then be asked to perform a gesture with mouse. This gesture, once successfully captured, will be saved. User will be notified of the time that user had taken to perform this gesture this time.
7. User will need to remember the gesture for subsequent attempts at lo-gin. Sign up process is complete.

Logging In
Now when User log in, User will have to enter user name, and then perform gesture. Once this is submitted and verified, User will enter the 3-D environment and perform interactions. User will exit and submit it. Once that is verified, user will be granted access.

Mouse Gesture Detection
In computing, a pointing device gestureor mouse gestures a way of combining movements and clickswhich the software recognizes as a specific command. Pointing device gestures can provide quick access to common functions of a program.

A. Gesture Creation
The gesture creation module is a simple drawing application used to ask the participant to freely draw a predefined set of gestures. The main purpose of this module is to make the participant draw the gestures in his own way to replicate them later on. It is important to note here that the gestures are not tied to any language and they do not necessarily have a meaning. They can be any drawing that can be produced in a uni-stroke. Also, the gesture creation module serves as a practice step for the participants to get familiar with the idea of drawing mouse gestures.

B. Data Acquisition and Preparation
The data acquisition and preparation module involves three main components, namely, data acquisition, data preparation, and data smoothing.

1) Data Acquisition:
The data acquisition component loads the gestures, created initially by presents the user using the gesture creation module, and them to the user to replicate. The data acquisition module records the user interaction while drawing the gesture. 2) Data Prepossessing:The data acquisition module prepossess the collected preliminary gesture from the computer mouse in such a way that some noise patterns are ignored or dropped. This is required since the data produced by the pointing devices is usually jagged and irregular. This kind of prepossessing will filter data resulting from a common problem of the pointing devices, specifically pivot points generated with the same time-stamp.3) Outlier Removal and Data Smoothing: To build the user profile, we remove outliers from the data and then smooth it. Data smoothing is generally used to eliminate noise and extract real patterns from data. In our framework, we use smoothing to smooth the data among the different replications obtained for each user. Generally, humans cannot draw the same gesture with the same exact detail twice under the same conditions. This will result in some variability in the replicas produced by the same individual for the same gesture. Data smoothing allows us to smooth such variability and minimize its effect on the learning process.

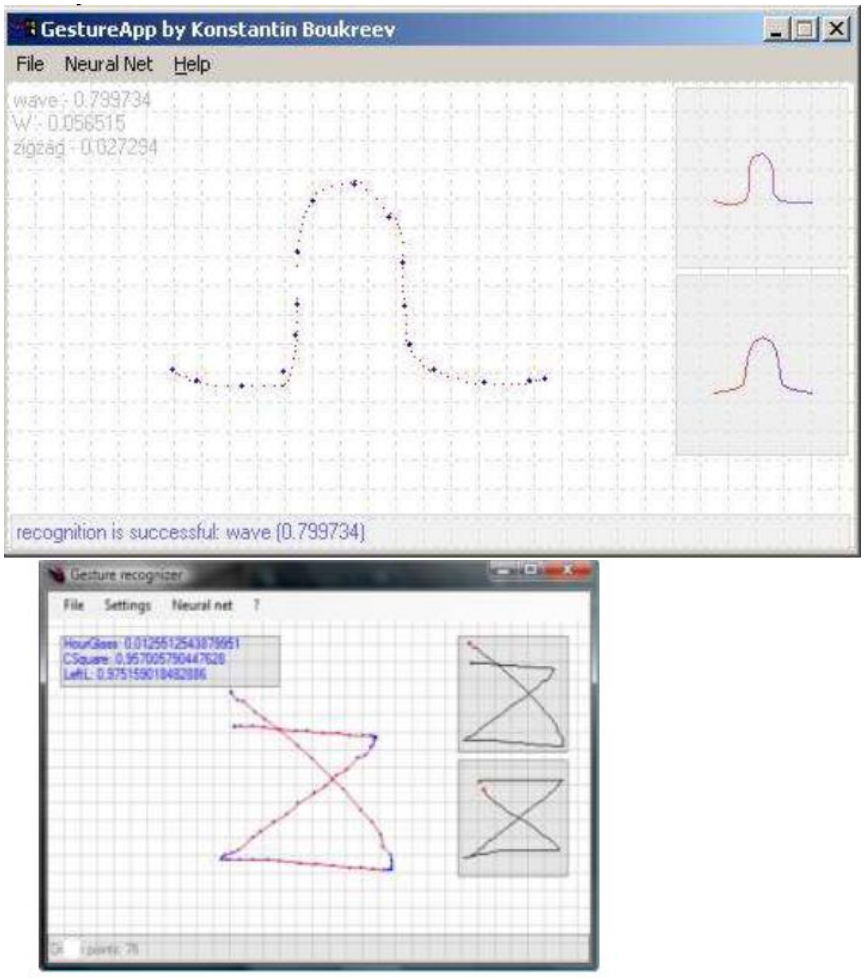

Fig1: Mouse Gesture captured during initial login with pivot points.
Fig 2: Gesture pattern matched trying to pass through same pivot points

VI.SECURITY ANALYSIS

Key logger

In many cases, the attacker installs an invisible software called a key logger, which is designed to capture all keys typed through the user's keyboard and output them as a stream in a text file. This way the attacker finds out the user's password by browsing through the file. But here, since the nature of pass- word is not textual, this attempt will be a total failure.

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 pass- word distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack. Even then, the probability of a successful attack is extremely scarce. With a 4-D password, there is the extra process of determining the gesture as well.

The chances that an attacker can guess the gesture, out of thousands of possible human movements, is going to be as hard as it sounds. Plus, both the gesture and the 3-D password need to guess correctly. So chances of a successful attack in this case are bleak, to mention the least.

Shoulder Surfing Attack

An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical Passwords. However, the user's 3D password may contain bio-metric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be per- formed in a secure place where a shoulder surfing attack can- not be performed. Also, with the 4-D password, the nuances of the gesture, even if visible to the attacker, may not be emulated successfully, and also the physique will have to match with the user, since the system would compare it with the earlier recording.

Timing Attack
The Attacker observes how long it takes the legitimate user to perform correct log in using 3D Password which gives an indication of 3-D Passwords length. This attack cannot be successful since it gives the attacker mere hints. Also this would lend the attacker no help in finding out the extra gesture; which is exclusive of the 4D password only.

Brute Force Attack
The attack is very difficult because
1. Time required to lo-gin may vary from 20s to 2 min therefore it is very time consuming.
2. Cost of Attack: A 3D Virtual environment may contain a bio-metric object, and the attacker has to forge all bio- metric information.

Significance
The addition of an extra gesture will create an unlimited host of password combinations. Also, it will ensure that there is a person attempting to lo-gin, and not some automated program, or bot. Another check that can be applied here, is the measure of the total time taken for the 3-D Authentication by the user. This time can be considered a part of the user's authentication, and the user must perform subsequent attempts within the same time limit, give or take a few more seconds. So each password can then have a time window associated with it.
On later attempts, a timer can be made to run in parallel to the 3-D browsing session. Based on the total time taken, certain conclusions can be drawn out:
1. If time taken tends to zero, it might be an attempt made by an automated hacking process.
2. If time taken is very large, it may well be possible that another user is attempting to replicate the user's actions, step by step. This additional check will provide more soundness to the 4- D password scheme.

Advantages
1. **Flexibility:** 4D Passwords allows Multifactor Authentication. Bio-metric, graphical and textual passwords can be embedded in 4D password technology.
2. **Strength:** This scenario provides almost unlimited passwords possibility. Hence, the strength.
3. **Easy to Remember:** Can be remembered in the form of short story.
4. **Privacy:** Organizers can select authentication schemes that respect the user's privacy.

APPLICATION
1. **Critical Servers:** Many organizations are using critical servers which are protected by a textual password. 4D password authentication scheme proposes sound re- placement for these textual passwords.
2. **Banking:** Almost all the Indian banks started 3D Password service for security of buyer who wants to buy online or pay online. We have to go to our bank's website and then, click 3D secure service and then write our card number, CVV, pin no., and write our password and rewrite it and then click OK or submit." After this we get a 'thank you message.
4. **Airplanes and Jet fighters:** Since airplanes and jet planes can be misused for religion and political agendas, they should be protected by a powerful authentication scheme.
5. **ATM's, Desktop and Laptop Log ins, Web Authentication:** In ATM also nowadays this technique is being used due to more security and best comfort with this type of technology. Also, desktops and laptops are now safer with this authentication.
6. **The Cloud:** Cloud computing is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing re- sources. It provides various services over internet such as software, hardware, data storage and infra- structure.

VII. CONCLUSION AND FUTURE WORK
Cloud computing provides various internet-based, on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to the intended customer, it is a better option to use sophisticated and robust password generation and authentication technique. A strong authentication technique would ensure strict authentication and authorization. The security levels of cloud environment can be further improved by multi-level of authentication. This is the future work of our research. Our future work will be carried out in adding multidimensional pass- word generation method to multi-level authentication technique. This amalgamation of techniques can lead to another revolutionary concept of authentication, [10] that even surpasses the utility and robustness of the current authentication schemes, the best of which is the 3D password at present. Of course, the fourth dimension makes it totally unsurpassable.

VIII. ACKNOWLEDGEMENT
We would like to express our deepest appreciation to all those who provided us the possibility to complete this report. A special gratitude we give to our internal guide, **Mrs. Nilima Nikam,** whose contribution in stimulating suggestions and encouragement, helped us to coordinate our research especially in writing this report. Furthermore we would also like to acknowledge with much appreciation the crucial role of the staff of computer department, who gave the permission to use all required equipment and the necessary material to complete the task "**4-D Authentication System Using Mouse Gesture**". A special thanks goes to other members who help us to assemble the parts and gave suggestion about the task

"4-D authentication system". Last but not least, many thanks go to the whole team who have invested their full effort in guiding the report and in achieving the goal. We have to appreciate the guidance given by other supervisor as well as the panels to improve our presentation skills, thanks to their comment and ad-vices.

VIII.REFERENCES

[1]. International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.
[2]. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
[3]. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
[4]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[5]. M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.
[6]. A. Gilbert, "Phishing attacks take a new twist," in CNET News.com, May 04, 2005.
[7]. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.
[8]. 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.
[9]. Fawaz A. Alsatian and Abdulmotaleb El Saddik,"Three- Dimensional Password for More Secure Authentication," IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008J.
[10]. Thorpe, P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords.
[11]. USENIX Security 2004, San Diego, August 9-13, 2004. J. Williams, "Narrow-Band Analyzer," PhD dissertation, Dept. of Electrical Eng., Harvard Univ., Cambridge, Mass., 1993. (Thesis or dissertation) D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th USENIX.