Virtual Environments Provide Mammoth Security for Critical Server

R. N. Muneshwar, S. K. Sonkar

Abstract: Security is the key factor of resolution of computer era. In every field of computer it may be cloud computing, neural network, data ware house, data mining, or grid computing in every field the security is central theme. We can provide the security by means of authentication process. Authentication is nothing but the process of validating who you are to whom you claim to be. The most common approach for authentication is alphanumeric passwords. Traditionally, alphanumeric passwords have been used for authentication. The textual passwords meets with the two conflicting things a) Passwords should be easy to remember, at the same time (b) Passwords hard to guess.

Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Now day's graphical passwords are other alternatives. Our paper reports to the comparison study between the different graphical password schemes and the alphanumeric passwords.

Through we present and evaluate the 3-D password. The 3-D password is a multifactor authentication scheme. The 3-D password

presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified.

Keywords— Authentication, biometrics, graphical passwords, multifactor, textual passwords, 3-D passwords, 3-D virtual environment.

I. INTRODUCTION

One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. In general, human authentication techniques can be classified as knowledge based (what you know), token based (what you have), and biometrics (what you are). Knowledge-based authentication can be further divided into two categories as follows: 1) recall based and 2) recognition based [1]. Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected before [1]. One of the most common recall-based authentication schemes used in the computer world is textual passwords. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks. Currently, most graphical passwords are still in their research. In this paper, we comprehensively analyze and discuss the 3-D password [3]. The 3-D password is a multifactor authentication scheme. It can combine 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 observing the actions and interactions of the user and by observing 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 avoids interacting 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 3-D passwords will increase.

II. LITERATURE SURVEY

Klein [2] collected the passwords of nearly 15 000 accounts that had alphanumerical passwords and he reached the following observation: 25% of the passwords were guessed by using a small yet well-formed dictionary of 3×10^6 words. Furthermore, 21% of the passwords were guessed in the first week and 368 passwords were guessed within the first 15 min. Klein [2] stated that by looking at these results in a system with about 50 accounts, the first account can be guessed in 2 min and 5–15 accounts can be guessed in the first day. Klein [2] showed that even though the full textual password space for eight-character passwords consisting of letters and numbers is almost 2×10^{15} possible passwords, it is easy to crack 25% of the passwords by using only a small subset of the full password space. It is important to note that Klein's experiment was in 1990 when the processing capabilities, memory, networking, and other resources were very limited compared to today's technology.

Many authentication systems, particularly in banking, require not only what the user knows but also what the user possesses (token-based systems).

Manuscript received on February 13, 2013.

R.N.Muneshwar, Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner, India.

Prof. S.K.Sonkar, Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner, India.

However, many reports [3]–[5] have shown that tokens are vulnerable to fraud, loss, or theft by using simple techniques. Graphical passwords can be divided into two categories as follows: 1) recognition based and 2) recall based

III. 3-D PASSWORD SCHEME

In this section, we present a multifactor authentication scheme that combines the benefits of various authentication schemes. We attempted to satisfy the following requirements. 1) The new scheme should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall-, recognition-, biometrics-, and token-based authentication schemes. 2) Users ought to have the freedom to select whether the 3-D password will be solely recall-, biometrics-, recognition-, or token-based, or a combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Some users do not like to carry cards. Some users do not like to provide biometrical data, and some users have poor memories. Therefore, to ensure high user acceptability, the user's freedom of selection is important. 3) The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess. 4) The new scheme should provide secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others. 5) The new scheme should provide secrets that can be easily revoked or changed. Based on the aforementioned requirements, we propose our contribution

A. 3-D Password Overview

The 3-D password is a multifactor authentication scheme. The 3-D password presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified.

B.Proposed Algorithm

1. Creating 3-D objects & virtual environment.
2. Registering a user by storing the 3-D password created by him/her.
3. Moving inside virtual 3D environment
    a. Performing actions and interaction in environment
    b. Changing object status
4. Verify at login time
5. Exit

C. System Requirement:

Hardware Requirements

512 MB RAM
PENTIUM-4 Processor

Software Requirements

OS: WINDOWS XP
C#.net
SQL Server

IV. SYTEM DESIGN

Three dimensional passwords is multi-factorial scheme. Multi-factorial means is combination of all existing authentication scheme in one scheme. Different schemes are Textual password, Graphical password. In paper three different environment proposed by which user can registration. By using three different environments user can select any environment will be the part of three dimensional passwords.

For accessing the system the user must followed the following steps.

1) Registration
2) Login.

A. Registration

While constructing the three dimensional password first the user registers himself by filling all fields, the registration form is consist of different field they are, full name field contain of name of user who wish to register, full address of user can put in address field. State of user in state field, city fields contain the city of user, telephone number fields store the personal telephone number of user, mobile number, Email id provided in to Email field, user name contain in user fields, and password is selected in password.

After filling all fields in registration form the different environment are available so that user can select any environments. Now user can select any environment which will be part of his three dimensional password. Here three different environment available users may select any one.

B. Environment One

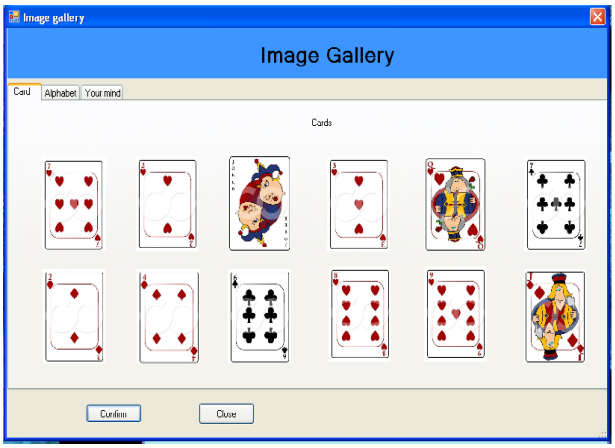

Fig 1: - environment-one showing twelve card

Environment one consist of three different graphical virtual environments.

1) Cards
2) Alphabets
3) You mind i.e. your password

Now user navigates through environment and performed some action and interaction with 3d environment. After performing all action and interaction in three dimensional virtual environments it constructs his/her 3D password. In first part there are twelve cards now user can select any card among twelve cards, whichever the card selected its action and interaction of user toward the environments.

Finally the selected card is part of users three dimensional password. After selecting any card second part of

environment comes in to picture that is another challenge for attacker now user is free to select any alphabet among set of alphabet which were displayed.

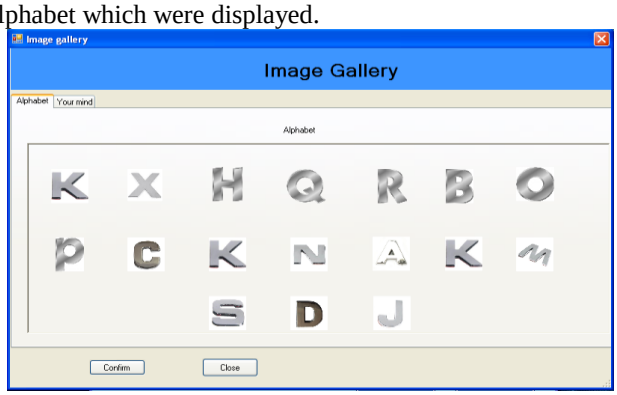

Fig 2:- environment-one providing alphabet

In this environment user can select any alphabet whichever the alphabet get selected which is part of 3d password here seventeen different alphabets are displayed. Now user can able to select any alphabet. After selecting alphabet next environment is appeared in which user can puts whatever is in its mind in form of alphanumeric password.

In textual field user can select its password, user can select password having the length of six characters. User can set password in the form of textual password, numeric password or combination of both that is alphanumeric password. In practical alphanumerical passwords are more recommended because of it produces more challenges to attacker to indentified the same password.

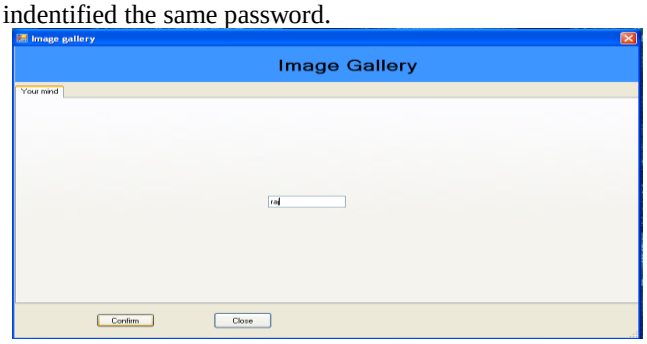

Fig3: Environment showing user select alphanumerical password.

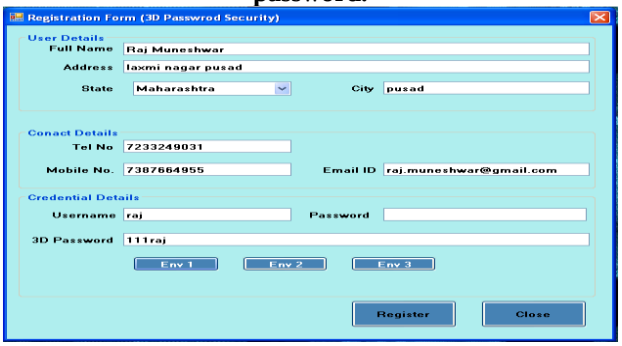

Fig 4: 3D password can be constructed

From fig4 shows action and interaction with different environments made by user. So the card got selected, alphabet, textual password all together forms a **three dimensional password** in environment one**.**

If the user can produces the secrete that he set at the time of registration then whichever the 3D password it will produce is correct. In above case the user identified all the respective field it's rightly interacts with different environment then 3D password is produces it's given as 111raj, which is match with the database and system will show the message you have logged in successfully.

Fig: successful login in environment One

In login form is meanly consist of login name in which user have to mention the login name as well text password. After that it selects the environments which were selected by him at the time of registration. In above form the user selects the first environment and selects the correct card among twelve cards, and select appropriate alphabet among seventeen alphabets. After select the correct card and alphabet, the user selects the alphanumeric password. After that the recorded data field show 3d password which on the basis on how the user interact with different environment.

In authentication process this recorded data match with the database if it's same then and then only the user will authenticate and it can access the system otherwise the access denied.

C. Environment Two

At the time of registration the user have three different environment lists. In figure5 the user is selected second environment for construction of 3D password. The second environment meanly consist of tic tack toe game in which there are sixteen different cells are available now user can select any number of cell as a part of his 3 D password. In paper it's recommended that user have to select more cells because it will produces the more challenges to the intruder or third party. Example if user select only one cell as part of password then 16C1=16 different possibilities are there to select right choice. But if we select 9 cell then it will produce 16C9=11440 possibilities.

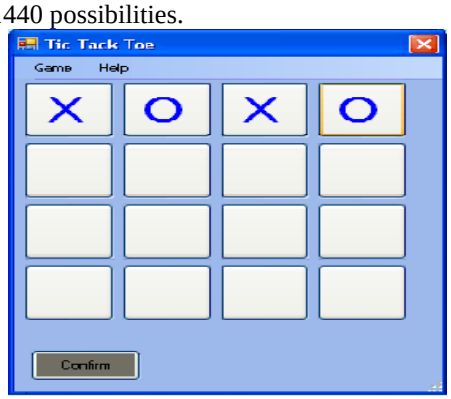

Fig5: - Environment two shows tic-tack Toe 4 * 4

The tic tack toe environment is type of graphical environment having 16 number of cell, now user can select any number of cells in diagonally, row wise, column wise or as per his/her convenience. Whichever the cell selected by user is part of three dimensional password. In snapshot user select 4 cells in first row in fig5.

D. Environment Three

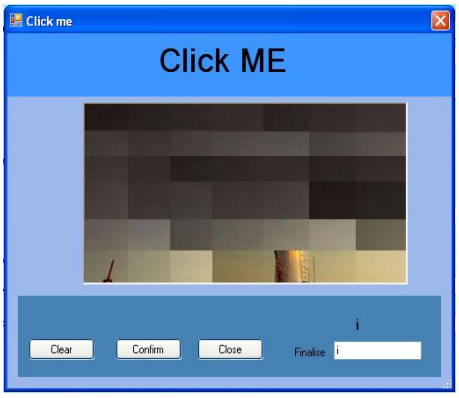

Fig6: Environment Three Click me.

In given click me environment there are six row and seven column 42 different cells are available in which user can click on different images (cell) which form the three dimensional password. Here the user has two performed 9-15 different click then submit confirm button. While performed all clicking the button shows the letter by which the user remember all entries by making some story of letters.

E. 3-D Virtual Environment Design Guidelines

Designing a well-studied 3-D virtual environment affects the usability, effectiveness, and acceptability of a 3-D password system. Therefore, the first step in building a 3-D password system is to design a 3-D environment that reflects the administration needs and the security requirements. The design of 3-D virtual environments should follow these guidelines. 1) *Real-life similarity:* The prospective 3-D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real-life situations. Object responses should be realistic. The target should have a 3-D virtual environment that users can interact with, by using common sense.

2) ***Object uniqueness and distinction:*** Every virtual object or item in the 3-D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position.

3) Three-dimensional virtual environment size: A 3-D virtual environment can depict a city or even the world.

4) *Number of objects (items) and their types:* Part of designing a 3-D virtual environment is determining the types of objects and how many objects should be placed in the environment.

V.SYSTEM RESISTANT AGINST ATTACK

A. The sum Rule: If the first task can be done in n1 ways and a second task in n2 ways and if these two tasks cannot be performed simultaneously, then there are n1+n2 ways of performing either task.

B. The Product Rule: Suppose a procedure can be broken down into two tasks T2 and T2, if the first task T1 can be performed in n1 ways and the second task T2 can be performed in n2 ways after the first task T1 has been done, then the total procedure can be carried out in the designated order in n1*n2 ways.

C. System Immune: Now the part comes in which we have to calculate the system immune, how the system is strong? Whether the different attacks can possible on system or not?

Now in paper I calculate the different possibility break the system. The attacker or third party first login the system by valid user name. After that the textual password in paper recommended that the user can select any alphanumeric password which having minimum 8 character or more than that.

Now here we calculate the how many different possibilities are there to break the password which having minimum eight character in length. By using the total probability theorem the intruder have to calculate the total possibilities so he can perform the brute force attack. Now we calculate the different possibilities.

Total possibilities= (All 8 are Char's) Or (7 are Char's And 1Number.) Or (6 are Char's And 2 are Numbers.) Or (5 are Char's And 3 are No's.) Or (4are Char's or 4 are Numbers.) Or (3 are Char's And 5 are Numbers.) Or (2 are Char's And 6 are Numbers.) Or (1 is Char And 7 are Numbers.) Or (8 are Numbers.)

$$=(26^8)+(26^7*10^1)+(26^6*10^2)+(26^5*10^3)+(26^4*10^4)+(26^3*10^5)+(26^2*10^6)+(26^1*10^7)+(10^8)$$

Total possibilities $=\mathbf{3.39*10^{11}}$

Total no of possibilities and challenges to attacker to find out the correct password= $3.39*10^{11}$…..(A)

If the password consist of six characters then the total possibilities are calculate by using total probability theorem. Total possibilities = (All 6 are Char's) Or (5are Char's and 1is Number) Or (4 are Char's And 2are No's.) Or (3 are Char's And 3 are No's) Or (2are Char's And 4are No's) Or (1 is Char And 5 are Numbers) Or (All 6 are Numbers)

$$=(26^6)*(26^5*10^1)*(26^4*2)*(26^3*10^3)*(26^2*10^4)*(26^1*10^5)*(10^6)$$

$$=5.01*10^8$$

Total possibilities or challenges to attacker the correct password=$\mathbf{5.01*10^8}$…… (A)

D. Resistant offer in Environment One

Now we thing regarding to the attacker point of view then as per the environment one is get concern. In environment one the different graphical password are there which contributes for making the 3D password.

In environment three different graphical environments are available they are

1) Cards in this scheme there are twelve different cards offered in among that the attacker have to select any correct card. The probability for selecting the correct card is 12 C1=12 different ways are here to select any card. Among that one is corrects and others are incorrect.

2) After selecting the card second graphical password is displayed in which we are offering the seventeen alphabets now the challenge to attacker is to select correct car among seventeen cards. There for there are 17C1=17 possibilities to select the correct card.

3) In third graphical environment the attacker wants to find out the textual password. The textual password is alphanumeric password, Or numeric password or only textual password which consists of only character.

Total challenges in environment one=12C1*17C18*$5.01*10^8$=$1.02*10^{11}$

Now we calculate how many possibilities are here for

selecting the correct password in environment one.
Total challenges= (find out password which having 8 character in lengths) * (selecting the correct card among the twelve cards) * (selecting the appropriate alphabet among seventeen alphabets)* (find out the correct 6 character password).
Total challenger to find out correct password in environment one=$3.39*10^{11}*1.02*10^{11}$
Total challenger to find out correct password in environment one =$\mathbf{3.46*10^{22}}$
Here are three dimension passwords which is sequence of action and interaction. Now for breaking the system the attacker has to perform all correct action and interaction then only he will be in position to break the system. If in any points he selects the incorrect input then he will not break the system hare if he select incorrect card or incorrect alphabet then it not produces correct password. For selecting the correct 3D password in environment one it has to perform all correct action and interactions toward the virtual environments. For breaking the system we produce $3.46*10^{22}$ possible password or challenges to attacker to produce the correct password.

E. Resistant offer in Environment Two

In environment two consist of the tic tack toe environment in which the different sixteen cells are available in which the user can select the four cells at the time of registration. User can select any number of cells as far his convince get concerned. We select only four cells but user may select five, six, seven or more than that.
Now here we are going to show how much our system is strong? How the system has immune against the available attacks? How many challenges we can produce? Now calculate the different possibilities regarding to the environment two. For the attacker first it should be calculate how many cells are get selected by user at the time of registration. So no option is available with him and as per brute force attack is get concerned he will try all possible keys. So he will start to selecting one cell, two cells, three cells, four cells and so on up to 16 cells. Total numbers of cells are sixteen.
The number of way to select one cell= 16C1=16
The number of way to select two cell= 16C2=120
The number of way to select three cell= 16C3=560
The number of way to select four cell= 16C4=1820
The number of ways to select five cells= 16C5=4368
The number of way to select six cell= 16C6=8008
The number of way to select seven cell= 16C7=11440
So on for number of way to select sixteen cell=16C16=1
For breaking the second environment attacker should correct predicts the eight character password and correct sequence of cell selected in tic tack toe environment.
Therefore the total possible combinations are = $(3.39*10^{11}*16C1)+(3.39*10^{11}*16C2)+(3.39*10^{11}*16C3)+(3.39*10^{11}*16C4)+(3.39*10^{11}*16C5)+(3.39*10^{11}*16C6)+(3.39*10^{11}*16C7)+(3.39*10^{11}*16C8)+(3.39*10^{11}*16C9)+(3.39*10^{11}*16C10)+(3.39*10^{11}*16C11)+(3.39*10^{11}*16C12)+(3.39*10^{11}*16C13)+(3.39*10^{11}*16C14)+(3.39*10^{11}*16C15)+(3.39*10^{11}*16C16)$

Total possibilities = $2.22*10^{16}$

For breaking the system that is our second environment attacker has to face $2.22*10^{16}$ challenges. In brute force attack the attacker should have used this amount of combination keys for breaking the system.

F. Resistant offer by Environment Thee

In click me environment there are 6 row and seven columns are available therefore total 42 cells. In this environment the user clicks different 15 cells at the time of registration. Now for attacker or third party all fifteen click should be correctly identified then only the proposed system will break for that it having so many possible keys to identified the password.

After predicting the correct eight characters password attacker come across the click me environment. For this environment it should correctly identified the fifteen clicks in different cell among 42 cells. Assume after correct recognition of alphanumeric password he don't know how many click was selected by user at the time of registration, so he will apply all possible way. He will select one click then two and three and so on up to 42 cells. Total Combinations=$(3.39*10^{11}*42C1)+(3.39*10^{11}*42C2)+(3.39*10^{11}*42C3)+\ldots+(3.39*10^{11}*42C42)$

Total Combination= $1.49*10^{24}$

For selecting the correct password attacker apply all these number of combination for break the system. Among all these combination one is correct password but for apply that much combinational key it is big headache for him also.

G. Application

Critical Applications:

1. Critical Servers.
2. Nuclear & Military Facilities.
3. Airplanes & Jet Fighters etc.

Usual applications:

1. ATMs.
2. Desktop computers & laptops.
3. On Networks.
4. PDA etc.

VI. EXPERIMENTAL RESULT

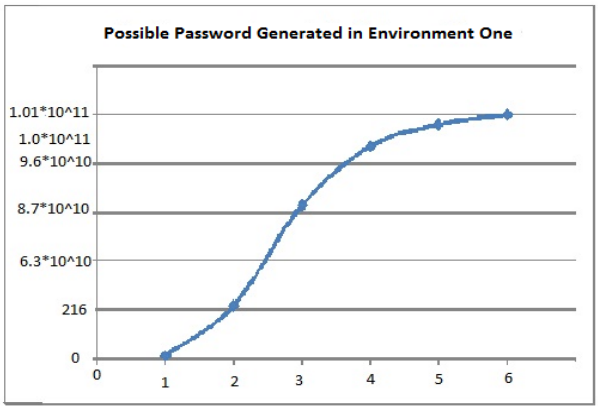

Fig 7: Possible password generated in Environment One

The above graph shows the action and interaction of user on Y-Axis whereas on X-Axis number of possible password which was generated on the basis of number of action and interaction made by user.

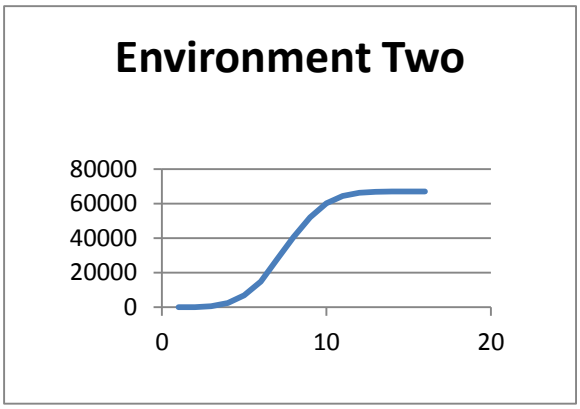

Fig 8: total number of password generated.

The above graph shows the action and interaction on X-axis, and on Y-axis show total number of password generated. Here the password generation is proportional (exponential) to the action and interaction made by user.

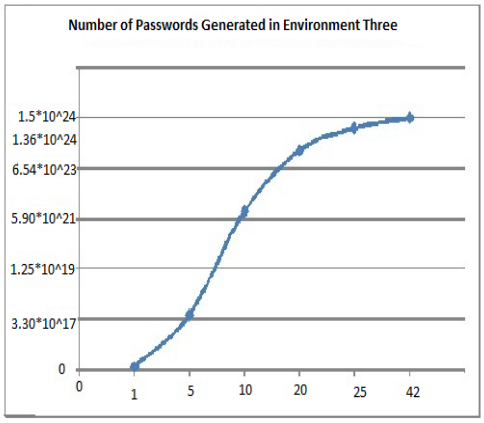

Fig9: Showing passwords generated in environment three.

Above graph showing generated password while user performing action and interaction in environment three.

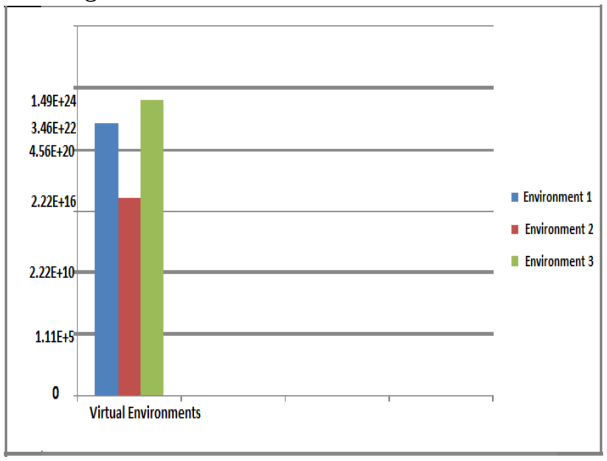

Fig10: Comparatively study of all environments.

Here the graph showing the comparatively study among the three different environment. All environments gives the high degree of security over any alphanumerical password. The environment three gives Mammoth security as per as the calculation and experimental result is get concerned.

VII. CONCLUSION

In this paper we have represented the three different virtual environment, all are being able to provide more security as compared to any other authentication scheme like textual password. In same paper we are combined the different authentication scheme in to one called as the 3D password, which is multi-factorial authentication scheme. In Experimental result section we have shown the result of each environment and in the last we compared all these three environments on the basis of calculation, the environment three gives the mammoth security to the critical server.

REFERENCES

1. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Proc. 21st Annu. Comput.. Security Appl. Conf.*, Dec. 5–9, 2005, pp. 463–472.
2. D. V. Klein, "Foiling the cracker: A survey of, and improvement to passwords security," in *Proc. USENIX Security Workshop*, 1990, pp. 5–14.
3. NBC news, *ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs*, Dec. 11, 2003.
4. T. Kitten, *Keeping an Eye on the ATM*. (2005, Jul. 11). [Online]. Available: ATMMarketPlace.com
5. BC news, *Cash Machine Fraud up, Say Banks*, Nov. 4, 2006.
6. G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.
7. R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in *Proc. 9th USINEX Security Symp.*, Denver, CO, Aug. 2000, pp. 45–58.
8. Real User Corporation, *The Science Behind Passfaces*. (2005, Oct.). [Online]. Available: http://www.realusers.com
9. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th USENIX Security Symp.*, San Diego, CA, Aug. 2004, pp. 1–14.
10. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proc. Symp. Usable Privacy Security*, Pittsburgh, PA, Jul. 2005, pp. 1–12.
11. 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.
12. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Pass Points: Design and longitudinal evaluation of a graphical password system," *Int. J. Human-Comput. Stud. (Special Issue on HCI Research in Privacy and Security)*, vol. 63, no. 1/2, pp. 102–127, Jul. 2005.
13. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, Washington DC, Aug. 1999, pp. 1–14.
14. J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in *Proc. USENIX Security*, San Diego, CA, Aug. 9–13, 2004, p. 10.

AUTHORS PROFILE

Muneshwar Rajesh N. Received the B.Tech degree in 2009 from Sri guru Gobindji Institute of Engineering and Technology, vishnupuri nanded which is an autonomous institute, Maharashtra. Pursuing Master of Computer Engineering Degree in Amrutvahini college of Engineering, Sangamner, Maharashtra.

Sonkar S.K. working as Assit. Porfessor in Amrutvahini College of Engineering, Sangamner. Pursuing P.H.D. from JJTU University. Is research work in network security.