ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Improving ATM Security Using 3D Password

Shivani A. Patil[1], Shamli A. Hage[2]

UG student, Dept. of EXTC, Prof Ram Meghe College of Engg & Managment, Badnera, Maharashtra, India [1]

UG student, Dept. of EXTC, Prof Ram Meghe College of Engg & Managment, Badnera, Maharashtra, India[2]

ABSTRACT: Normally the authentication scheme the user undergoes is particularly very strict. Throughout the years authentication has been a very interesting approach. With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or to hack someone's password. Many users resist the biometric system because of their intrusive responses and their effect on privacy. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key is called as 3D password. The 3D password authentication scheme is based on a combination of multiple sets of factors. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen and user navigates with the virtual environment. In this paper we represent our contribution in improving security at ATM machines by using the 3D passwords.

KEYWORDS: 3D password, ATM Security, User Authentication, Virtual Environment, System Security.

I.INTRODUCTION

3D passwords are more customizable and very interesting way of authentication. Today's passwords are based on the fact of human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. An alternative approach is used to use the 3D passwords system with the existing systems. Once the 3D password is implemented and we log in to a secure site, the 3D password GUI opens up. 3 D passwords is an XML-based protocol designed to be an additional security layer for online transactions. This technology was originally developed by Arcot Systems, Inc and first deployed by Visa with the intention of improving the security of Internet payments and is offered to customers under the name Verified by Visa. Services based on the protocol have also been adopted by MasterCard as MasterCard Secure Code, and by JCB International as J/Secure.

II.NEED OF 3D PASSWORD

The dramatic increase of computer usage has given rise to many security concerns. 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. 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. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess. Klein 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 × 106 words. Klein showed that even though the full textual password space for eight-character passwords consisting of letters and numbers is almost 2 × 1014 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. Therefore we present the idea of 3D passwords which is customizable and very interesting way of secure authentication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

III.ADVANTAGES

1. This system provides security in addition to the existing system for security.
2. 3D password can't be stole by any other person.
3. 3D password has no limit of size.
4. 3D password can change easily.
5. This password helps to keep personal detail.

IV.DISADVANTAGES

1. This system is expensive
2. Requires computer technology.
3. Blind person can't use this technology.
4. Lot of program coding is required.

V. EXISTING SYSTEM

Generally current authentication systems are plagued or suffer by many weaknesses. Commonly, textual passwords are used to secure data or user accounts. However these can be cracked by the application of various brute-force algorithms as the maximum password length is fixed and there are a finite number of possibilities which exist. Presently existing graphical passwords have password space which is lesser than or equal to the textual password space. The 3D password system is a multifactor authentication scheme. It can combine multiple authentication schemes in a single 3D virtual environment to the user. Where the user can navigates and interacts with the multiple objects that may present in 3D virtual environment. The user 3D password can construct depending upon the sequence of action and interaction to-words the object inside the 3D virtual environment. The 3D password is combination of many existing authentication scheme such as textual password, graphical password, and various types of biometrics scan in a 3D virtual environment which providing an extremely high degree of security to the user.

VI.PASSWORD CARD AUTHENTICATION & DISADVANTAGES

The increased usage of computer applications has given a rise for many security concerns. Out of these security concerns the authentication is one of the most serious issues of security. Instead of security concerns the authentication is one of the most serious issues of security. In general, human authentication techniques can be classified as:

Knowledge based:
Knowledge-based authentication can be further divided into two categories as follows: 1) recall based and 2) recognition based. 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, that the user selected before. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

Token based & Graphical based:
In banking authentication systems, not only require a knowledge based system but also token based system is required. However, many reports have shown that tokens are vulnerable to fraud, loss or theft by using simple techniques. 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. Generally 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.

Biometrics based:
Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

VII.SUPPLEMENTARY AUTHENTICATION

The 3-D password is a multifactor authentication scheme. The 3D password scheme uses a combination of RECOGNITION + RECALL + BIOMETRIC + TOKEN in a 3D virtual environment based authentication system. The 3D password can be thought of a multiple parameter based authentication scheme. It may combine two or more pre-existing authentication schemes to form a single 3Dvirtual environment. This environment should contain several 3D object with which the user can have sequence of interaction. The type of interaction sequence stored as a password scheme depends on the user according to his need. The 3D password is therefore nothing else but the sequence of interaction with the virtual object. Therefore this system constitutes interaction with only those objects that perform acquisition of information from the user that he comfortable to provide. It ignores interaction with the rest of the objects that might demand the information which the user might not want to provide to the system. For example, if a 3D object requests a scanning of biometric based authentication system but the user doesn't want to perform this scan for himself the user is then free to not to interact with the system.

VIII.WORKING OF SYSTEM

Consider a three dimensional virtual atmosphere space that is of the size G*G*G. Each point in the three dimensional atmosphere space represented by the coordinates. (x, y ,z)[1….G]* [1….G]. The entities are distributed in the three dimensional virtual environment. Every entity has it's own (x, y,z) coordinates. Assume the user can navigate and walk through the three dimensional virtual environment and can see the entities & interact with the entities. The input device for interaction with entities can be mouse, a keyboard, stylus, a card reader, a microphone etc. For example, consider user who navigates through the 3D virtual environment that is nothing but a room area. Let us assume that the user enter in room that is virtual area. After entering the user in the room the door is closed which is located in position (9, 16, 80).The user moving away the curtain which is located in position (12,6,24). Then user walks towards the chair then the AC is turn on which is located in the position (10, 5,25). Then play mp3 player which is located in position (15, 6, 20) which is placed above the table. Then user set a volume down of the song which is located in position (55, 3, 30). After user choose a knowledge book from set of books which is located in position (42,01,70). The user then presses the login button. The initial representation of user actions in the 3D virtual environment can be recorded as follows:-

(9,16,80) Action = Closed the door;
(12,6,24) Action = Move away the window curtain ;
(10,5,25) Action = Turn on AC;
(15 ,6 20) Action = Play mp3 player;
(55,3,30) Action = Set volume down;
(42,01,70) Action = Choose knowledge book ;

As shown in below figure any 3D environment can be considered for authenticating the user. For ex in above figure the user may have to enter his password in the given 3D environment ATM machine and then have to choose the one of image place on the right side of the machine.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

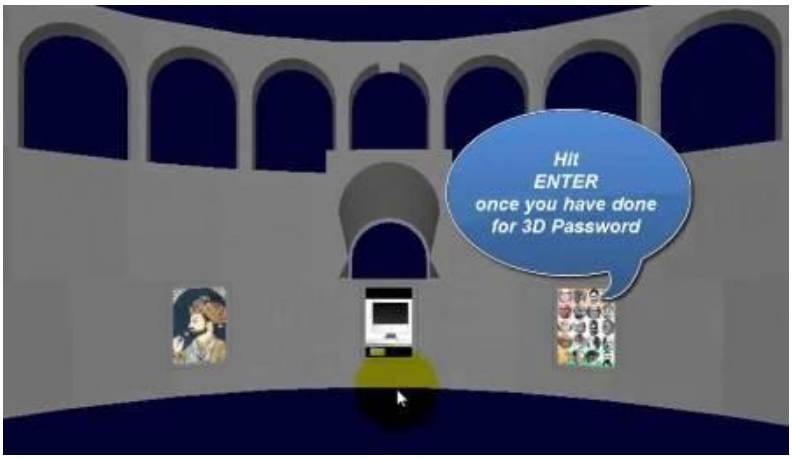

Fig 1: Example of virtual 3D environment

IX.FLOWCHART APPROACH

Following is the flowchart for the proposed system. As shown is the flowchart below the user comes at the ATM machine. He then swipes his card and and enters his password. If the password is correct then the user is provided with 3D virtual environment. The 3D environment which is provided to the user depends on the ATM service provider. In the 3D environment the user performs his recorded actions. If the actions are correct then the user is authenticated. If the action in 3D environment is wrong then user is not authenticated and access is denied.

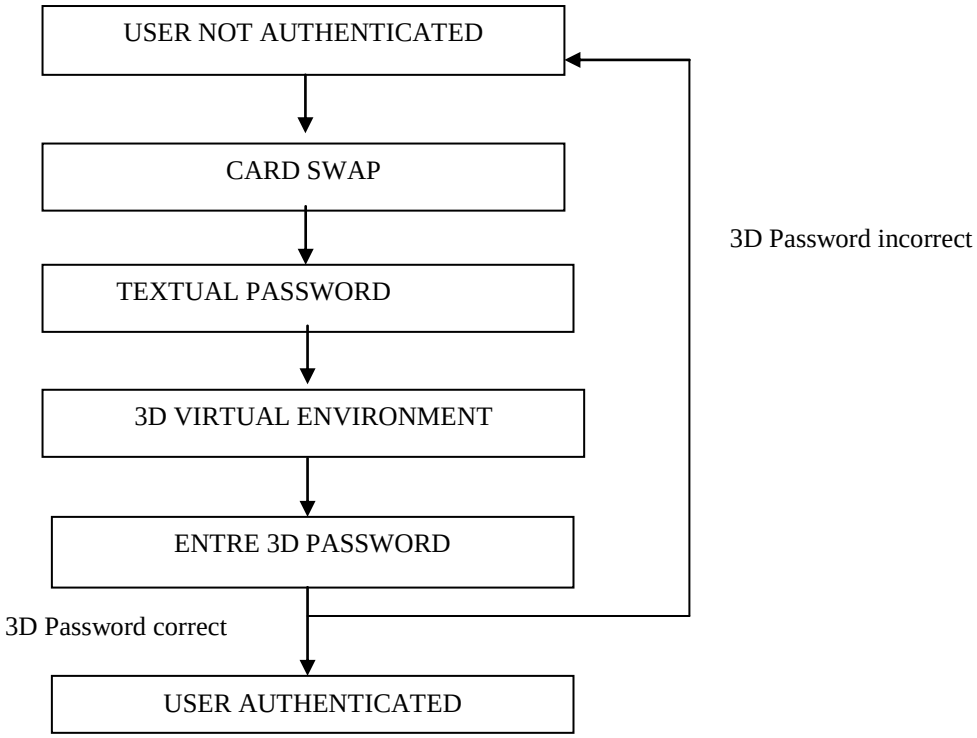

Fig 2: Flowchart of the proposed system

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

X. USEFULLNESS OF SYSTEM

1. This system Provides security.
2. 3D password can't take by any other person.
3. 3D password has no limit.
4. Password can change easily.
5. This password helps to keep personal detail.

XI.CONCLUSION

In the existing systems, Textual password and Tokens based passwords are the most common user authentication designs. Many other designs are also there like graphical passwords, biometric authentication design etc. which are used in different fields. The main goal of this paper to have design security of ATM using 3D password, combination of any existing or upcoming, authentication designs into a one design. While using 3D password, users have freedom to select whether the 3D password will be solely recall, biometrics, recognition or combination of two designs or more. Users do not have provide their fingerprints if they not comfortable. Users do not have carry cards if they do not want to. They have choice to construct their 3D password according to their choice and their needs. A 3D password's probable password space can be reflected by the designs of 3D virtual environment, which is designed by the system administrator. The 3D virtual environment can contain any entities that the administrator feels that the users are familiar with.

REFERENCES

[1] N .M. Paul , M. Shanmugham , Minimal Utilization of Space & Vast Security Coupled With Biometrics For Secure Authentication (IJATER), Vol 2, Issue 4, July 2012.
[2] A .B. Gadicha , V .B. Gadicha , Virtual Realization Using 3D Password , International Journal of Electronics & Computer Science Engineering , Vol 1, number 2pp 216-222
[3] N.A. Anwat , D.S. Shingate , V.H. Patil , A Secure Authentication Mechanism Using 3D Password , International Journal of Advance Research in science Engineering & Technology , Vol. 01, Issue 01, pp. 29-37
[4] T. Kognule , Y. Thumbre , S. Kognule , International Conference on Advance in Communication & Computing Technologies (ICACACT) 2012