3D Password- Future of Digital Lockers…
It will Work!!!

Mr. Kartik Ramesh Patel
Industrial Electronics Department
Lecturer, at V.E.S. Polytechnic
Mumbai, India
kartik.patel@ves.ac.in

Mr. Santosh Krishna Mulye
Computer Technology Department
Lecturer, at V.E.S. Polytechnic
Mumbai, India
santosh.mulye@ves.ac.in

Abstract

Digital Locker is one of the key initiatives under the Digital India Programme. Digital Locker is aimed at minimizing the usage of physical documents and enable sharing of e-documents across agencies. The sharing of the e-documents will be done through registered repositories thereby ensuring the authenticity of the documents online. Residents can also upload their own electronic documents and digitally sign them using the e-sign facility. These digitally signed documents can be shared with Government organizations or other entities. One of the prime requirements of such a facility provided by the government is high level of security. The multilevel password technique called 3D password can work for such an initiative. 3D passwords are more customizable and very interesting way of authentication. Now the 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. Once implemented and you log in to a secure site, the 3D password GUI opens up. 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.

Keywords

Security, Authentication, password, virtual environment, input.

I. Introduction

Digital Locker is one of the key initiatives under the Digital India Programme. Digital Locker is aimed at minimizing the usage of physical documents and enable sharing of e-documents across agencies. The sharing of the e-documents will be done through registered repositories thereby ensuring the authenticity of the documents online. Residents can also upload their own electronic documents and digitally sign them using the e-sign facility. These digitally signed documents can be shared with Government organizations or other entities.

Digital Locker is a service launched by Government of India in February 2015 to provide a secure dedicated personal electronic space for storing the documents of resident Indian citizens. The storage space (maximum 1GB) is linked to the aadhar number of the user. The space can be utilized for storing personal documents like University certificates, PAN cards, voter id cards, etc., and the URI's of the e-documents issued by various issuer departments. There is also an associated facility for e-signing documents. The service is intended to minimize the use of physical documents and to provide authenticity of the e-documents. It will also provide secure access to Govt. issued documents. It is also intended to reduce administrative expenses of Govt. departments and agencies and to make it easy for the residents to receive services.

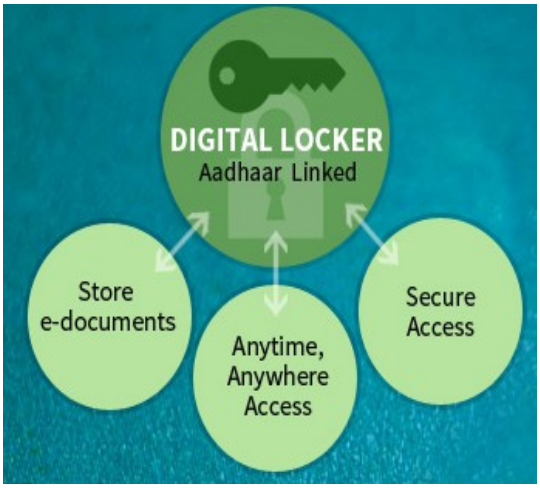

Figure 1: Idea of Digital Locker [2]

Each user's digital locker has the following sections.

- *My Certificates*: This section comprises of two sub sections:
- *Digital Documents*: This contains the URI's of the documents issued to the user by Govt. departments or other agencies.

- *Uploaded Documents*: This subsection lists all the documents which are uploaded by the user. Each file to be uploaded should not be more than 1MB in size. Only pdf, jpg, jpeg, png, bmp and gif file types can be uploaded.
- *My Profile*: This section displays the complete profile of the user as available in the UIDAI database.
- *My Issuer*: This section displays the issuers' names and the number of documents issued to the user by the issuer.
- *My Requester*: This section displays the requesters' names and the number of documents requested from the user by the requesters.
- *Directories*: This section displays the complete list of registered issuers and requesters along with their URLs.

The digital locker will be directly linked with the individual's information stored in Unique Identification Authority of India (UIDAI) database. The Unique Identification Authority of India (UIDAI) was set up by the Government of India on 28 January 2009 as an attached office of the erstwhile Planning Commission of India vide its a gazette notification [8]. The UIDAI is mandated to assign a 12-digit unique identification (UID) number (termed as Aadhaar) to all the residents of India. As per the notification, the UIDAI has been given the responsibility to lay down plan and policies to implement UID scheme, to own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis. The implementation of UID scheme entails generation and assignment of UID to residents; defining mechanisms and processes for interlinking UID with partner databases; operation and management of all stages of UID life cycle; framing policies and procedures for updation mechanism and defining usage and applicability of UID for delivery of various services among others [8]. The number is linked to the resident's basic demographic and biometric information such as photograph, ten fingerprints and two iris scans, which are stored in a centralized database [9].

Dedicated 10MB free personal storage space, linked to each resident's Aadhaar, to securely store e-documents and to store URI link of e-documents for accessing them directly from the repositories. Sharing of secured e-documents with requesters. Currently accessible via web portal, will be made accessible through mobile application also.

Figure 2: Digital Locker

The three key stakeholders in the digital locker system are the Issuer who is an entity issuing e-documents to individuals in a standard format and making them electronically available e.g. CBSE, Registrar Office, Income Tax department, etc., the requester who is an entity requesting secure access to a particular e-document stored in the repository (e.g. University, Passport Office, Regional Transport Office, etc.) and the resident who is an individual who uses the Digital Locker service based on Aadhaar and OTP (One Time Password) authentication.

II. Components of digital locker

A. Repository

Repository is a Collection of e-Documents which are uploaded by issuers in a standard format and exposing a set of standard APIs for secure real-time search and access. In revision control systems, a repository is an on-disk data structure which stores metadata for a set of files and/or directory structure. Depending on whether the version control system in use is distributed or centralized, the whole set of information in the repository may be duplicated on every user's system or may be maintained on a single server. Some of the metadata that a repository contains includes, among other things.

- A historical record of changes in the repository.
- A set of commit objects.
- A set of references to commit objects, called heads.

A version control system (or revision control system) is a system that tracks incremental versions (or revisions) of files and, in some cases, directories over time. Of course, merely tracking the various versions of a user's (or group of users') files and directories isn't very interesting in itself. What makes a version control system

useful is the fact that it allows you to explore the changes which resulted in each of those versions and facilitates the arbitrary recall of the same.

At the core of the version control system is a repository, which is the central store of that system's data. The repository usually stores information in the form of a file system tree—a hierarchy of files and directories. Any numbers of clients connect to the repository, and then read or write to these files. By writing data, a client makes the information available to others; by reading data, the client receives information from others. Figure 3, "A typical client/server system" illustrates this.

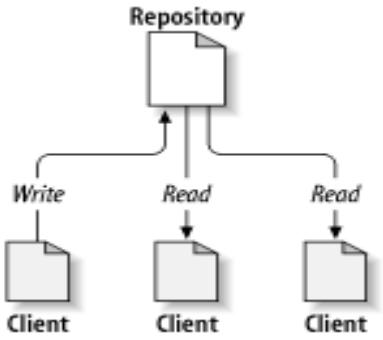

Figure 3: Client/Server system [7]

So far, this sounds like the definition of a typical file server. And indeed, the repository *is* a kind of file server, but it's not your usual breed. What makes the repository special is that as the files in the repository are changed, the repository remembers each version of those files. When a client reads data from the repository, it normally sees only the latest version of the file system tree. But what makes a version control client interesting is that it also has the ability to request previous states of the file system from the repository. A version control client can ask historical questions such as "What did this directory contain last Wednesday?" and "Who was the last person to change this file, and what changes did he make?" These are the sorts of questions that are at the heart of any version control system.

A version control system's value comes from the fact that it tracks versions of files and directories, but the rest of the software universe doesn't operate on "versions of files and directories". Most software programs understand how to operate only on a single version of a specific type of file. So how does a version control user interact with an abstract—and, often, remote—repository full of multiple versions of various files in a concrete fashion? How does his or her word processing software, presentation software, source code editor, web design software, or some other program—all of which trade in the currency of simple data files—get access to such files? The answer is found in the version control construct known as a working copy.

A working copy is, quite literally, a local copy of a particular version of a user's VCS-managed data upon which that user is free to work. Working copies appear to other software just as any other local directory full of files, so those programs don't have to be "version-control-aware" in order to read from and write to that data. The task of managing the working copy and communicating changes made to its contents to and from the repository falls squarely to the version control system's client software.

The main purpose of a repository is to store a set of files, as well as the history of changes made to those files [11]. Exactly how each revision control system handles storing those changes, however, differs greatly: for instance, Subversion has in the past relied on a database instance and has since moved to storing its changes directly on the file system [12].These differences in methodology have generally led to diverse uses of revision control by different groups, depending on their needs [13].

B. Access Gateway

Access Gateway provides a secure online mechanism for requesters to access e-documents from various repositories in real-time using e-Document URI (Uniform Resource Indicator). The URI is a link to the e-Document uploaded by an issuer in a repository. The gateway will identify the address of the repository where the e-Document is stored based on the URI and will fetch the e-Document from that repository.

In a communications network, a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions. Loosely, a computer or computer program configured to perform the tasks of a gateway. For a specific case, see default gateway.

Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

On an IP network, clients should automatically send IP packets with a destination outside a given subnet mask to a network gateway. A subnet mask defines the IP range of a private network. For example, if a private network has a base IP address of 192.168.0.0 and has a subnet mask of 255.255.255.0, then any data going to an IP address outside of 192.168.0.X will be sent to that network's gateway. While forwarding an IP packet to another network, the gateway might or might not perform Network Address Translation.

A gateway is an essential feature of most routers, although other devices (such as any PC or server) can function as a gateway. Most computer operating systems use the terms described above. Microsoft Windows, however, describes this standard networking feature as Internet Connection Sharing, which acts as a gateway, offering a connection between the Internet and an internal network. Such a system might also act as a DHCP server. Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

III. Authentication

Authentication is the act of establishing or confirming something as authentic, that is, that claims made by or about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artefact, ensuring that a product is what it's packaging and labelling claims to be, or assuring that a computer program is a trusted one. For example, when you show proper identification credentials to a bank teller, you are asking to be authenticated to act on behalf of the account holder. If your authentication request is approved, you become authorized to access the accounts of that account holder, but no others.

Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system authentication must be provided, so that only authorized persons can have right to use or handle that system & data related to that system securely. There are many authentication algorithms are available some are effective & secure but having some drawback. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

- Knowledge based**:** means what you know. Textual password is the best example of this authentication scheme.
- Token based**:** means what you have. This includes Credit cards, ATM cards, etc as an example.
- Biometrics**:** means what you are. Includes Thumb impression, etc.
- Recognition Based**:** means what you recognize. Includes graphical password, iris recognition, face recognition, etc. [1]-[7].

IV. 3D Password

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.

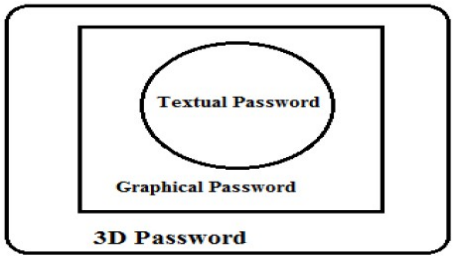

Figure 4: 3D password as multi-factor and multi-password authentication key

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate , moving in 3D virtual environment to create a password which is based on both the schemes. We don't use biometric scheme because biometric having some major drawbacks (like h/w cost is more) So that we have not included biometric authentication in our 3D password scheme. Because biometric authentication is efficient over shoulder surfing attacks. But other attacks are venerable & easy on biometric authentication. Also inclusion of biometric may leads to increasing the cost of scheme & more hardware parts needed.

(a) (b)

Figure 5: (a) 3D art gallery (b) Weather forecasting office

Figure above shows some snapshots of 3D Virtual Environment of different real time scenarios created in virtual environment like art gallery, office, etc. These virtual environments are interactive virtual environment. Because user can interact with these environment & creates his/her own 3D password easily.

A. Objective of 3D password

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password.etc).
- New scheme should be combination of recall-, recognition, biometrics-, and token based authentication schemes.

The three dimensional password (3D password) is a new authentication methodology that combines recognition, recall, what you have (tokens), and what you are (biometrics) in one authentication system. The idea is simply outlined as follows. The user navigates through a three dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the three dimensional virtual environment constructs the user's 3D password. Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x1, y1, z1) position, then walk into a room that has a white board that exist in a position (x2, y2, z2) and draw something on the white board. The combination and the sequence of the previous two actions towards the specific objects construct the user's 3D password. Users can navigate through a three dimensional virtual environment that can contain any virtual object.

Virtual objects can be of any type. We will list some possible objects to clarify the idea. An object can be:
1. A computer that the user can type in
2. A white board that a user can draw on
3. An ATM machine that requires a smart card and PIN
4. A light that can be switched on/off
5. Any biometric device
6. Any Graphical password scheme
7. Any real life object
8. Any upcoming authentication scheme

Moreover, in the virtual three-dimensional environment we can have two different computers in two different locations. Actions and interactions with the first computer is totally different than actions towards the second computer since each computer has a (x, y, z) position in the three-dimensional virtual environment. Each object in the virtual three-dimensional environment has its own (x, y, z) coordinates, speed, weight and responses toward actions.

B. 3D Password selection and inputs

Consider a three dimensional virtual environment space that is of the size G×G×G. Each point in the three dimensional environment space represented by the coordinates (x, y, z) ∈ [1...G] × [1...G] ×[1…G]. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x, y, z) coordinates. Assume the user can 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, styles, a card reader, a microphone…etc.

User actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions and inputs. For example, consider a user navigates through the three-dimensional virtual environment and types "AB" into a computer that exists in the position of (13, 2, 30). The user then walks over and turns off the light located in (20, 6,12), 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 (530,250). The user then presses the login button. The representation of user actions, interactions and inputs towards the objects and the three-dimensional virtual environments can be represented as the following:

(13,2,30) Action = Typing, "A",
(13,2,30) Action = Typing , "B",
(20,6,12) Action = Turning the Light, Off,
(55,3,30) Action = drawing , point = (530,250)

Two 3D passwords are equal to each other when the sequence of actions towards every specific object is equal and the actions themselves are equal towards the objects. As described earlier, three-dimensional virtual environments can be designed to include any virtual objects. The first step in building a 3D password system is designing the three-dimensional virtual environment. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password.

V. 3D Password applied to digital locker

The main goal of the proposed system is to design a multi feature, multi-password secure authentication scheme that combines the various authentication schemes into a single 3D virtual environment which results in a larger password space. The design of 3D virtual environment, the selection of object inside the environment, and the object type reflect the resulted password space. User have freedom to select whether the 3D password will be merely recall, recognition, or token based, or combination of two schemes or more.

A. Objective

- New scheme should provide more secure authentication compared to existing one.
- New scheme should build easy to understand and user friendly authentication technique, giving user the freedom of choice to select whether the 3D password would be solely, recall, recognition, biometrics or the mixture of any two schemes or more.
- New scheme should provide secrets that are easy to recall and at the same time tough to guess for the intruders.
- New scheme should provide such secrets that cannot be easily shared with others and difficult to note down on papers.
- New scheme should provide secrets that are mixture of merely recall, recognition, biometrics, and token based authentication schemes or combination of two or more schemes together.
- New scheme should provide secrets that are flexible, and authenticated user must be allowed to change or remove them.

B. 3D Password creation

As 3D Password is multi-feature so multiple password schemes such as textual password, graphical password, biometrics, and even token based passwords together can be used as a part of users 3D Password. Different users have different requirements so users must be given the freedom of selection and decision to choose which authentication schemes will be part of users 3D Password. The figure depicts state diagram for creating a 3D Password application.

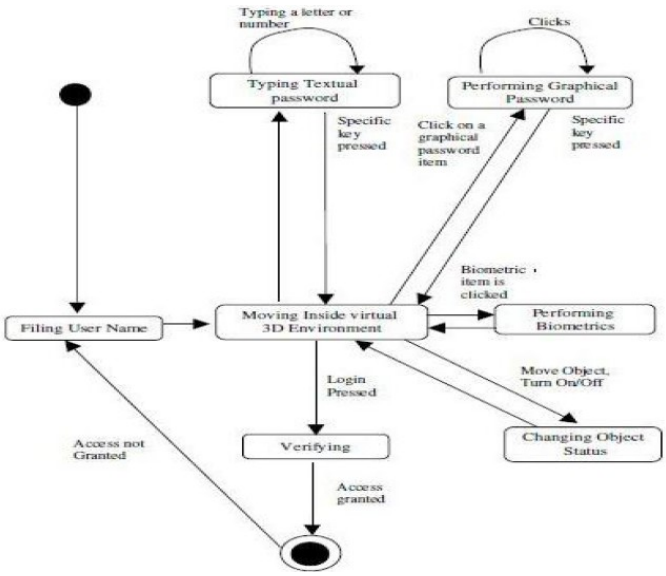

Figure 6: State diagram of creating 3D password application [1],[3],[4]

C. 3D Password creation

The first step user need to do in 3D Password is to authenticate him/her using simple textual password and is done through by providing user's username and password. Refer Fig 3.

Figure 7: User entering Textual Password in 3D virtual environment

On successful authentication, user is presented with 3D virtual environment GUI screen that consist of virtual computer and keyboard where the user need to enter password that is stored in a simple encrypted text file in the form of (x1, y1, z1) co-ordinates. After successful completion of this authentication step, user automatically enter into an art gallery (or virtual environment), where the user has to select multiple virtual objects/items present inside that gallery. The sequence in which user has clicked on moving objects, for those particular objects the sequence of points (i.e. their x, y, z co ordinates) are stored in text file in the encrypted form. In this manner, 3D Password is constructed and set for that specific user. Afterwards, when users want to access his/her account then the user has to select all the objects in same sequence which he/she has selected at the time of creating their 3D Password. Sequence is compared with the stored coordinates and if match is found then, authentication is successful and user is given the access.

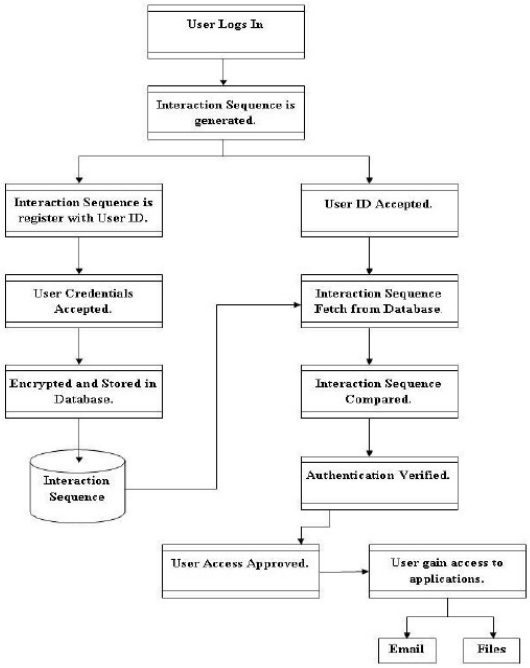

Figure 8: Working of 3D Password [2]

VI. 3D Password as more secure authentication scheme for digital lockers.

A. Attacks and counter measures

In this section, we try to cover and study different types of possible attacks that are practice against 3D Password and see how secure 3D Password is against such attacks. In addition, we try to propose counter measure for such attacks.

1) Brute force attack

In type of attack, attacker tries n number of possible combination of 3D Password. To perform these attack two things need to be considered.

Required time to login: in case of 3D password successful login time varies due to dependence on number of interactions and the size of 3D virtual environment does matter.

Cost required to attack: main requirement of 3D Password is 3D virtual environment and cost of creating such an environment is very high.

2) Well studied attack

To launch this kind of attack, attackers need to acquire the knowledge of the most probable distribution of 3D Password. To acquire such kind of knowledge attacker needs to study all the previous authentications schemes that are used in the 3D virtual environment which is very tough. For that the attacker even may need to gather the information regarding forging of all existing biometrical and token based data too. In addition, it requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3D password [1]. Furthermore, this kind of attack is hard to achieve as the attacker must need to perform a customized attack for every different 3D virtual environment design.

3) Shoulder surfing attack

To perform this attack, attackers make use of camera to capture and record the 3D Password while the legitimate user is carrying with their login process. This attack is more effective than any other attacks on 3D password. To avoid this attack, 3D Password must be performed in a secure place.

4) Timing attack

Here, attackers notices how much time it takes the authenticate user to accomplish an accurate sign-in with the 3D Password. By this observation attacker can get a clue regarding authenticated user's 3D Password length. Yet this attack is not very much effective as it gives mere clues to the attacker. Thus, it would perhaps be performed as a part of either brute force attack or well-studied attack.

B. Advantages and Disadvantages

1) Advantages

- 3D Password is multi-feature and multi-password authentication scheme.
- Large password key space.
- More secure authentication scheme as compared to existing one.
- 3D graphical password has no limit.
- Easy to Memorize
- More secure authentication scheme over currently available schemes.

2) Disadvantages

- Large time and memory requirements.
- Shoulder surfing attack is still effective and can affect this scheme.
- Expensive as compare to previous one.
- Difficult for blind people to use this technology.
- Requires sophisticated computers technology.
- A lot of program coding is required.

C. Applications

As compared to existing authentication schemes, for digital lockers 3D Password has large password key space and hence, to protect critical system and resources are 3D Password's main application domain.

1) Critical servers

Commonly, critical servers of many large organizations are protected using textual passwords. A 3D password authentication proposes a sound replacement for a textual password.

2) Nuclear and military facilities

Such facilities should be protected by the most powerful authentication systems. The 3D Password has a very large probable password space, and since it can contain token, biometrics, recognition, and knowledge based authentications in a single authentication system, it is a sound choice for high level security locations [1].

3) Airplanes and jet fighters

Because of the possible threat of misusing airplanes and jet fighters for religion-political agendas, usage of such airplanes should be protected by a powerful authentication system [1]. Furthermore, 3D Password can be applied in less critical systems where 3D virtual environment used size are small. Few such applications are as follows

- Web Application Authentication
- ATM
- PDA- Personal Digital Assistance
- Laptop and Desktop Computer logins.

4) Online banking

VII. **Conclusion**

Textual passwords and token-based passwords are the most common used authentication schemes. However, many different schemes have been used in specific fields A 3D password gives the user the choice of modeling his 3D password to contain any authentication scheme that the user prefers. Users do not have to provide their fingerprints if they do not wish to. Users do not have to carry cards if they do not want to. Users have the choice to model their 3D password according to their needs and their preferences. A 3D password's probable password space can be reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The three-dimensional virtual environment can contain any objects that the administrator feels that the users are familiar with. For example, football players can use a three dimensional virtual environment of a stadium where they can navigate and interact with objects that they are familiar with. The existing authentication schemes for digital locker are available that are vulnerable to certain kind of attacks. The 3D Password is multi-feature, multi-factor authentication scheme that combines all the benefits of existing authentication schemes into single 3D virtual environment. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3-D password. Shoulder surfing attacks are still possible and effective against 3-D passwords.

REFERENCES

[1] Alsulaiman, F.A.; El Saddik, A., *"Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.*

[2] *"Virtual Realization using 3D Password"*, A.B.Gadicha, V.B.Gadicha*, ISSN: 2277-1956, International Journal of Electronics and Computer Science Engineering*

[3] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, *—SECURED AUTHENTICATION: 3D PASSWORD‖, I.J.E.M.S., VOL.3(2),242 – 245, 2012.*

[4] Grover Aman, Narang Winnie, *—4-D Password: Strengthening the Authentication Scene‖, International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.*

[5] Manila M V*,"Three Dimensional Password for More SecureAuthentication",netlab.cs.iitm.ernet.in/cs648/2009/tpf/cs08m028.pdf ,2009.*

[6] Fawaz A Alsulaiman and Abdulmotaleb El Saddik, *"A Novel 3D Graphical Password Schema",IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.*

[7] I.Jermyn,A.Mayer,F.Monrose,M.K.Reiter,andA .D.Rubin, *"The design and analysis of 3D passwords," Special Issue on HCI Research in Privacy and Security,vol. 63,pp.102-127, July2005.*

[8] "Notification No.-A-43011/02/2009-Admn.I, 28 January 2009, Planning Commission, Government of India" (PDF). *UIDAI*. 28 January 2009. Retrieved7 July 2015

[9] "Learning with the Times: What is Aadhaar?".*The Times of India*. 4 December 2010. Retrieved 29 May2015.

[10] "SVNBook". Retrieved 2012-04-20.

[11] "Getting Started - About Version Control". Git SCM.

[12] Ben Collins-Sussman, Brian W. Fitzpatrick, C. Michael Pilato (2011). "Chapter 5: Strategies for Repository Deployment". *Version Control with Subversion: For Subversion 1.7*. O'Reilly.

[13] "Different approaches to source control branching". *Stack Overflow.* Retrieved 15 November 2014.