ISSN (e): 2250 – 3005 || Volume, 13 || Issue, 2|| Mar.-Apr. – 2023 ||
International Journal of Computational Engineering Research (IJCER)

# 3D Password Authentication

Mr. Pramod. K, *Associate professor, Nehru College of Engineering & Research Centre*
Aswathy V.S, *Department of MCA, Nehru College of Engineering & Research Centre*

***ABSTRACT***
*Today's users have access to common password stereotypes such as text passwords, biometric scanning, tokens or cards (like ATM cards), etc. The current authentication methods have numerous flaws. Text passwords are frequently used, however, users don't adhere to their criteria. Users frequently select significant terms from dictionaries, as well as names for their pets or boyfriends, etc. In tests conducted ten years ago, Klein was able to decipher 10-15 passwords per day. On the other side, a password that is difficult to guess is frequently also difficult to remember. Long and random-looking passwords are hard for users to remember. As a result, people come up with weak passwords that are brief and easy to guess. Textual passwords are thus subject to brute-force attacks and are simple to crack. Schemes for graphic passwords have been proposed. Users' greater ability to recall and recognize images than words makes graphical passwords more secure. The majority of graphical passwords are susceptible to shoulder surfing assaults, in which an attacker uses a camera to watch or record the graphical password of the authorized user. As a method of authentication, token-based devices like ATMs are frequently used in banking systems and at lab entrances.*

---

Date of Submission: 08-04-2023 Date of acceptance: 22-04-2023

---

## I. INTRODUCTION

We typically use a very lenient or extremely tight authentication method. Since then, it has evolved into a fascinating strategy. With the advancement of technological tools, it is now quite simple for "others" to crack someone's password. As a result, various algorithms have been developed, each with a unique strategy for calculating a secret key. The algorithms are designed to select a random number between 106 and 1015, therefore it is unlikely that two consecutive numbers will appear. Many different password formats are supported by authentication techniques, including text passwords, biometric scanning, tokens or cards (like ATM cards), etc

A multifactor authentication system, the 3-D password. It may create a single 3-D virtual environment from all currently used authentication methods. There are many objects or items in this 3-D virtual environment that the user can interact with. From one thing to another, the type of interaction differs. The user's interactions and activities, as well as the sequences of those interactions, are used to build the 3-D password. The user can decide which kinds of authentication methods to include in their 3-D password.

For instance, the user might choose not to interact with an object that asks for an iris scan if they feel uncomfortable doing so. Furthermore, given the abundance of things and stuff in the environment and the user's flexibility to choose the sort of authentication schemes that will be a part of their 3-D password, the number of potential 3-D passwords will rise. As a result, the attacker will have a considerably harder time guessing the user's 3-D password.

3D password Advanced Authentication Systems:

There are various security problems as a result of the increased use of computers. Authentication, which is the process of confirming that you are who you say you are, is one of the main security issues. The current authentication system has several flaws. Individuals typically utilize text passwords, however, they don't adhere to their rules. Users seek to employ words from the lexicon that has significance, yet doing so makes them more likely to be broken and attacked.

Conflicting criteria for choosing a password that is both simple to remember (for the user) and difficult to decipher are fundamental downsides of textual passwords (to prevent unauthorized access the private data).

As a solution, many biometric authentications have been proposed.These include:

- Retinal Scan
- Finger scanning
- Iris recognition
- Facial recognition
- Finger vein ID

However, users usually tend to resist biometrics because:
- because of their effect on privacy and their intrusiveness.
- moreover, biometrics cannot be revoked.

A multi-factor authentication technique, such as 3D Password, requires the user to supply more than one identity factor to access their data.
Some of these things are:
- What a user KNOWS: that is their password.
- What a user HAS: that is a smart card/hard token.
- What a user IS: that is a retinal scan/fingerprint.

We provide a 3-D virtual environment where the user can traverse and interact with numerous things to be authenticated into a safe system. The order in which things are done and how they are interacted with in the environment. Then, a password for the user is created. A virtual 3D world can be created using the password to incorporate the majority of current authentication methods, including textual and visual passwords and different biometrics. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space.

How secure is your password?
- Now with the technology change, fast processors, and many tools on the internet, cracking passwords has become child's play.
- Years back Klein performed such tests and he could crack 10-15 passwords per day.
- The 3D password is more customizable and a very interesting way of authentication.

A 3D password is a multifactor authentication scheme that combines

**RECOGNITION + RECALL + TOKENS + BIOMETRICS** in one authentication system.

A virtual environment with many virtual objects is presented via a 3D password.
The user moves about the scene and engages with the surroundings' things.
The order and combination of user interactions determine how the 3D world is created.


Fig1:3D password authentication

Brief Description of a 3D System:

In this 3D password virtual environment, the user can navigate and engage with a variety of items.

The user 3D password is created by the order in which actions are taken and with which objects are interacted in the environment.
Generally, there are two types of authentication techniques available such as**:**
Human Authentication Techniques are as follows:

- **Knowledge-based**: means what you know. A 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.

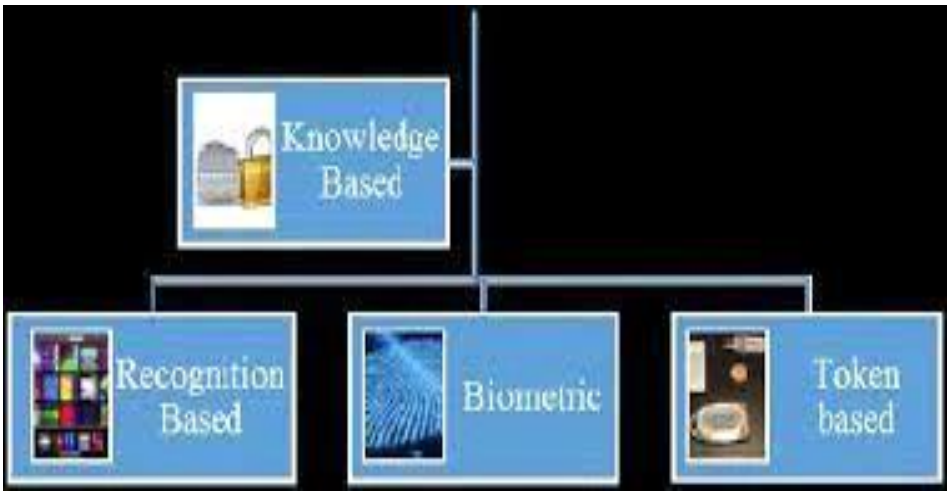

Fig 2: Human Authentication Technique

- **Computer Authentication Techniques** are as follows:

- Textual Passwords (Recall Based)-Recall what you have created before.
- Recognition Based: means what you recognize. Includes graphical passwords, iris recognition, face recognition, etc.

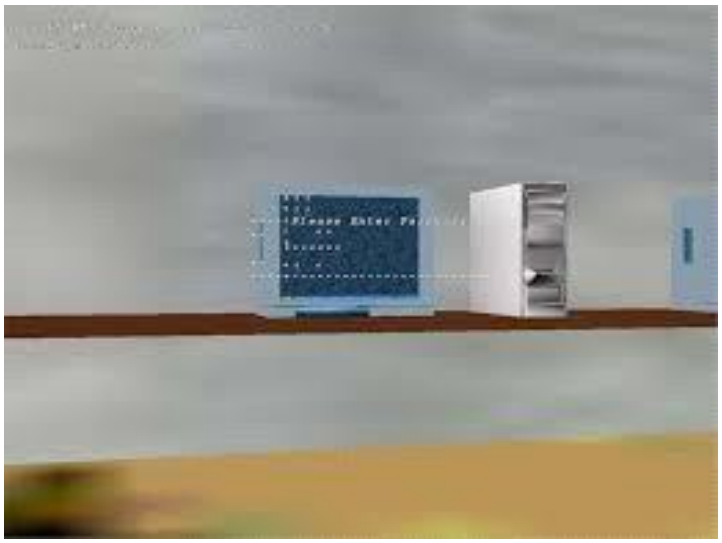
Fig 3: Computer Authentication Technique

## II. LITERATURE SURVEY

The existing authentication techniques include textual passwords, token-based passwords, and biometrics and recognition-based passwords.

**Textual passwords**: Textual passwords, or those that take the form of text and have comprehensive definitions obtained from dictionaries, user names, etc., are the most often used passwords nowadays. On the other side, a password that is difficult to guess is frequently also difficult to remember. Long and random-looking passwords are hard for users to remember. As a result, people come up with weak passwords that are brief and easy to guess. It makes text-based passwords simple to crack, easy for hackers to copy, and susceptible to brute-force attacks. The shortcomings of text-based passwords gave rise to a new type of authentication known as token-based passwords.

- **Token-based passwords:** These are the passwords that appear as tokens, such as jumbled letters, symbols, combinations of numbers, etc. Token-based passwords are used as a form of authentication at the gates to laboratories, ATMs, and swipe cards. Smart cards or tokens, on the other hand, are susceptible to theft and must be carried at all times when access is needed. Moreover, there is a danger that users will forget or lose their tokens. The shortcomings of text-based passwords and token-based passwords have given rise to a new type of authentication known as graphical passwords.

- **Graphical passwords:** These are the passwords that result from people's propensity for recalling and understanding images over words. The majority of graphical passwords are susceptible to shoulder surfing assaults, in which a perpetrator uses a camera to watch or record the legitimate user's graphical password. The shortcomings of graphical passwords, token-based passwords, and textual passwords give rise to a new kind of authentication known as biometrics.

- **Biometrics:** What you are is what biometrics signify. These are the passwords that can be identified by things like thumbprints and natural signatures. Your "natural" signature is captured by biometrics, and cards or tokens serve as identification documents. Hackers may employ chemicals, and they may simply alter a user's thumbprint. Also, some people detest carrying around their cards and some object to having their retinas exposed to intense Infrared light during biometric scanning. As people age, biometrics may also somewhat change.

## III. METHODOLOGY

- PROPOSED SCHEME
- Goal

The main objective of the suggested system is to develop a multi-feature, multi-password secure authentication scheme that combines all available authentication methods into a single, virtual, three-dimensional environment, resulting in a bigger and more secure password space.
The following are the objectives of the proposed scheme:

- The new scheme must offer more secure authentication when compared to the existing authentication scheme.
- The new scheme must be built in such a way that it is a combination of Recall, Recognition, and Token-based authentication techniques.
- The new scheme must be built in such a way that it is easy to understand and provides a user-friendly authentication technique.
- The new schemes provide secrets that are not easy to write down on paper. Moreover, the scheme's secrets shouldbe difficult to share with others.
- The new scheme must provide secrets that are easy to recall or memorize and at the same time hard to guess forthe hackers.


Fig4: Multifactor authentication

The main objective of the suggested system is to develop a multi-feature, multi-password secure authentication scheme that combines all available authentication methods into a single, virtual, three-dimensional environment, resulting in a bigger and more secure password space. The 3D password combines

many authentication methods, including textual, graphical, and token passwords, into one 3D virtual environment. The two steps of a 3D password are called the registration phase and the login phase. If a user is already registered, he can use the login phase to unlock his password; if he is a new user, he can register using the registration phase.

- **System Architecture**

The two steps of a 3D password are registration (Fig. 3) and the login phase (Fig 7). A new user registers a 3D password by providing the required information, such as an email address and a password, during the registration phase. After successful registration, a 3D environment (Fig. 4) is displayed, and the user interacts with it. The interactions are registered with the user's user-id and stored in the database as evidence of the registration's success. After completing the registration process successfully, the user logs in to the login phase, where they enter a one-step authentication process to gain access to a 3D environment. After this authentication, the 3D environment is displayed, and the user interacts with it. Additionally, the new interaction sequences are verified against the existing interactions stored in the database, and after the successful interaction, authentication is verified, indicating a successful login (Fig. 8).

- Authentication Method

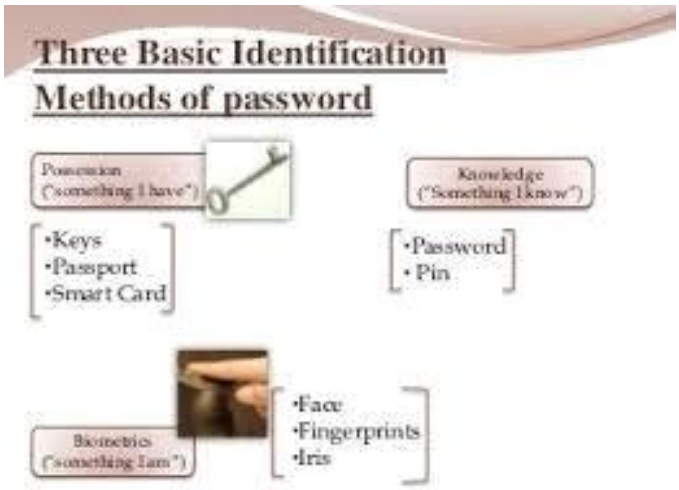


Fig5: base identification method

Establishing or confirming something's authenticity, or the veracity of claims made by or about it, is the act of authentication. This could entail verifying a person's identification, tracking an artifact's history, making sure a product is what it says it is on the packing and labeling, or making sure a computer software is reliable. For instance, you are requesting authorization to act on behalf of the account holder when you present correct identifying credentials to a bank teller. If your authentication request is granted, you are then permitted access to that account holder's accounts.

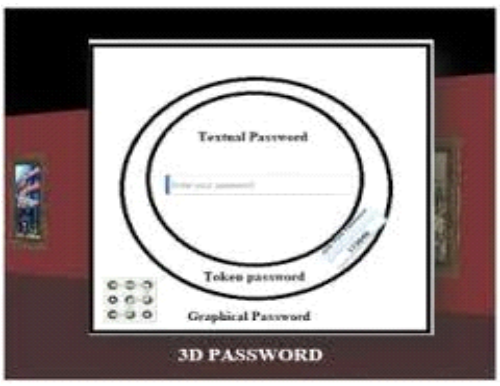


Fig 6: 3D Authentication Method

The first step is to compare the object's characteristics to what is known about items with a similar origin. An art specialist might, for instance, analyze the location and form of a signature, seek for similarities in the painting's style, or compare the piece to an old photograph. An archaeologist may use carbon dating to

confirm an artifact's age, perform a chemical study of the materials employed, or assess the artifact's construction or adornment in comparison to others of comparable age or origin. The veracity of audio recordings, pictures, or videos can be checked using the physics of sound and light in comparison to a known physical environment. The second type is dependent on proof or other outside affirmations.

For instance, establishing the chain of custody of provided evidence is frequently required by the rules of evidence in criminal courts. This can be done using a written log of the evidence or by having the police detectives and forensics team testify. Some antiques come with certifications stating that they are real. External records are separated from the item, as well as to forgery and perjury concerns of their own.

The first kind of authentication technique is frequently used with money and other financial items. Receivers can easily verify the authenticity of bills, coins, and checks because they have physical characteristics that are difficult to copy, like fine printing or engraving, a distinct feel, watermarks, and holographic images. Both types of authentication techniques can be used on consumer items like medications, perfume, and apparel to stop fake products from profiting from a well-known brand's reputation and harming that brand owner's sales and reputation.

**STATE DIAGRAM**

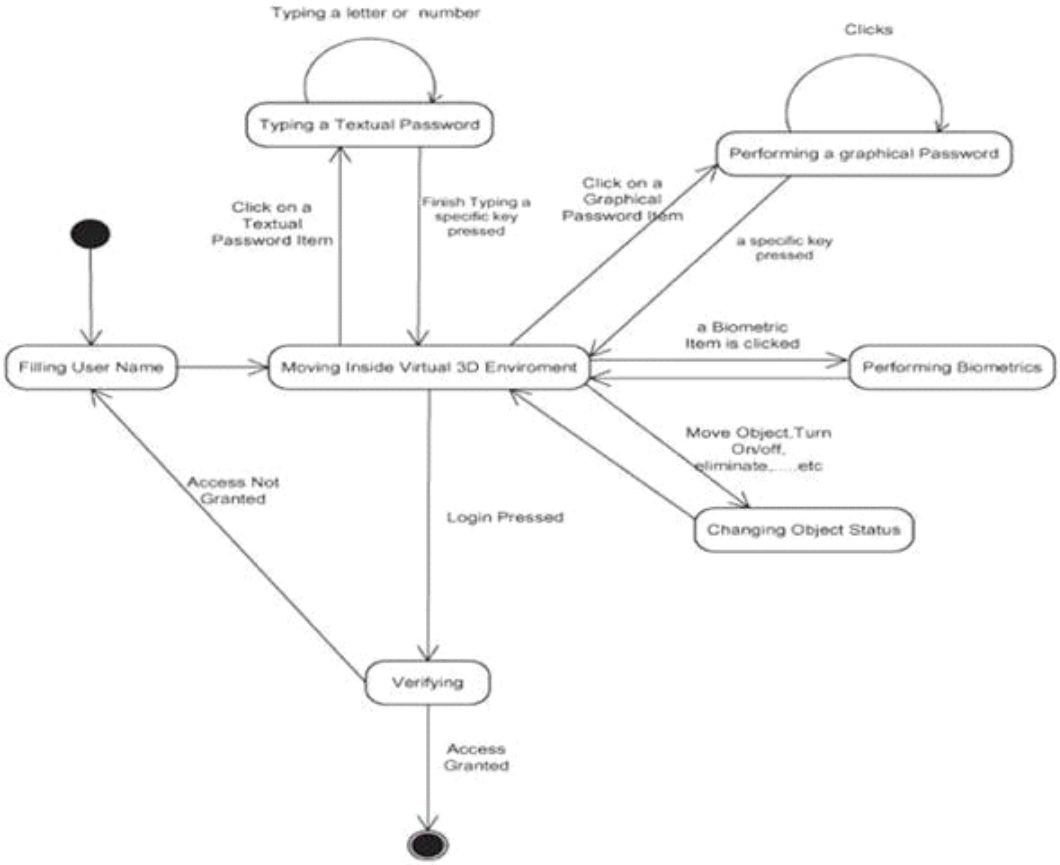


Fig 7: State diagram for 3D Password

## IV. SYSTEM IMPLEMENTATION

A multi-factor authentication system is a 3D password. The 3D password displays a 3D virtual setting with a variety of virtual objects. The user moves around this setting and engages with the objects.


Fig 8: Virtual Environment Example

The user activities that take place in the 3D virtual world are what make up the 3D password. The 3Dpassword enables the integration of token, biometric, recognition, recall, and recall-based systems into a single authentication process. This can be achieved by creating a 3D virtual environment with items that ask for the presentation of tokens, the recollection of information, the recognition of information, and the verification of biometric data. Picture of a proof-of-concept 3-D virtual environment in which the user is entering a text password on a computer simulation as part of their 3-D password.

For instance, the user might log into the virtual setting and type a text password. The user must then choose a picture frame on a computer that is in the position (x1, y1, z1), click on the third window of the building in that frame that is in the position (x2, y2, z2), and then enter a room with a thumbprint recognition device that is in the position (x3, y3, z3) and give his or her impression. The user's 3D password is created from the combination and sequencing of earlier actions taken toward particular items.

VIRTUAL OBJECT

- A computer with which the user can type;
- A fingerprint reader that requires the user’s fingerprint;
- A biometric recognition device;
- A paper or a whiteboard that a user can write, sign or draw on;
- An automated teller machine (ATM) that requires a token;
- A light that can be switched on/off;
- A television or radio where channels can be selected;
- A staple that can be driven;
- A car that can be driven;
- A book that can be moved from one place to another;
- Any graphical password scheme;
- Any real-life object;
- Any upcoming authentication scheme

3D VIRTUAL ENVIRONMENT DESIGN

The design of 3-D virtual environments affects the usability, effectiveness, and acceptability of 3D passwords. The first step in building a 3D password system is to design a 3D environment that reflects the administration's needs and security requirements.

Fig 9: Virtual Environment Design

The design of 3D virtual environments should follow these guidelines.

- Object Uniqueness and Distinction

In the 3D virtual environment, every virtual object or thing is distinct from every other virtual thing. Every virtual object has distinctive characteristics, such as position, which contribute to its individuality. As a result, the potential interaction with object 1 is different from the interaction with object 2. However, the user could become confused if there are 20 PCs or other similar objects all in one location. Because of this, it is important to take into account how each object can be distinguished from others while designing the 3D virtual world. Similar to this, it should be simple for users to move around and recognize different items in a 3D virtual environment. The user can recognize objects more easily thanks to the differentiating trait. As a result, the system's usability is enhanced.

- Three-Dimensional Virtual Environment Size

A city or the entire world can be portrayed in a 3D virtual environment. Yet, it can also represent a space that is narrowly concentrated, such as a single room or office. A big 3D virtual environment will make it take the user longer to use a 3D password. A sizable 3D virtual world can also include a lot of virtual objects. Thus, the potential 3D password space grows. Yet, a small 3D virtual world typically only has a few things, making a 3D password easier to complete.

- Number of Objects and Their Types

Determining the kinds of objects and how many should be placed in the area is a part of developing a 3D virtual environment. The categories of things determine the reactions the object will elicit. Requesting a text password or a fingerprint can be thought of as an objective answer type for the sake of simplicity. The likely password space of a 3D password is influenced by the number of objects and the appropriate object response kinds.

- System Importance

The systems that will be secured by a 3D password should be considered in the 3D virtual environment. The quantity and variety of objects utilized in the 3D virtual environment should be indicative of the value of the protected system.

## V.RESULT ANALYSIS

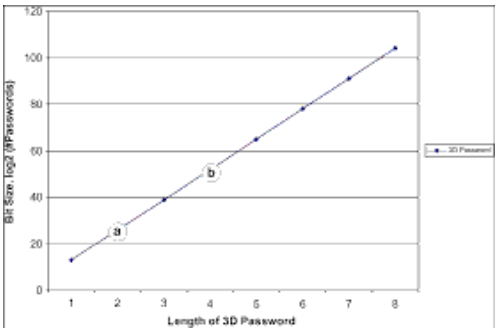


Fig 10: 3D Password space

To determine the password space, we have to count all possible 3D passwords that have a certain number of actions,interactions, and inputs toward all objects that exist in the 3D virtual environment.

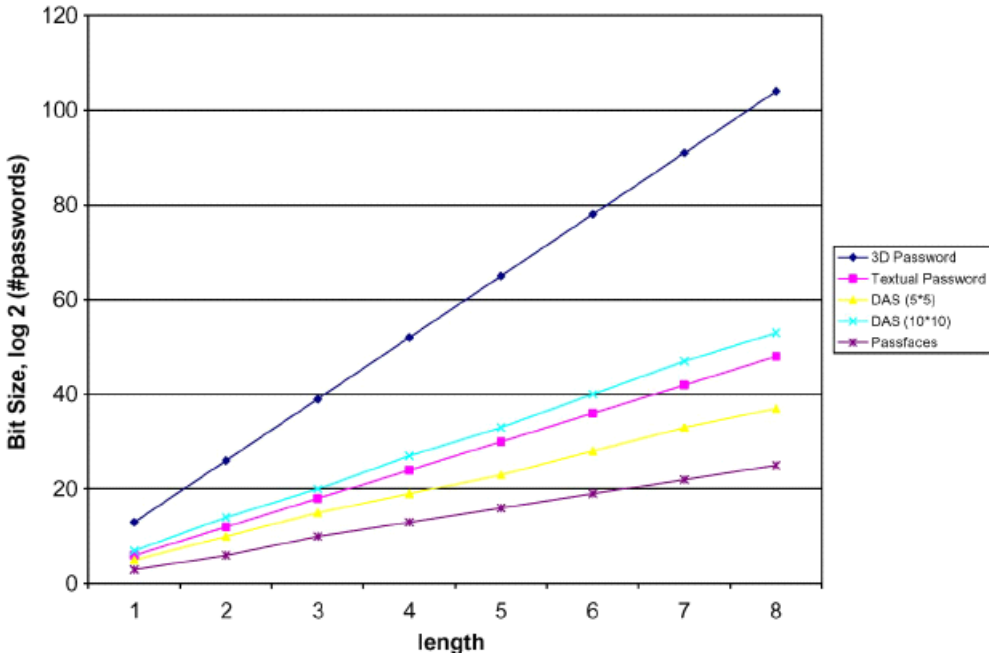


Fig11: Password space of the 3-D password, textual password, Pass faces, and DAS with grid sizes of 5 × 5 and 10 ×10

Length is measured in terms of 3-D password activities and interactions, textual password characters, Pass faces' selections, and the number of points that correspond to DAS strokes.
There is a maximum of eight. Fig: Comparing the two crucial Points of textual passwords to the number of actions and interactions that a 3-D password could take while operating in the 3-D environment described in Section V-A. The bit size of the Klein [2] (3 106) dictionary of eight-character textual passwords is shown by point "a." The entire password area for eight-character text passwords is represented by point "b."

## VI. ADVANTAGES AND DISADVANTAGES

**ADVANTAGES**

A 3D password can be memorized by users as a "little story," which makes the password simple to remember.

- **Flexibility**: Three-factor authentication is supported by a 3D password. Alpha-numeric passwords, smart cards, and biometrics can all be integrated with 3D password technology.

- **Strength**: A 3D world provides practically infinite combinations of choices for a scenario. Because such systems might have unique 3D worlds, hacking them is very challenging.

The 3D password allows customers the option to choose the kind of authentication methods they want to utilize.
- Secrets that are difficult to put on writing.
- It should be challenging to divulge the scheme's secrets to others.
- Provide secrets that can be quickly amended or canceled

**DISADVANTAGES**

- Difficult for blind people to use this technology
- Requires sophisticated computers technology expensive.
- A lot of program coding is required.

## VII. APPLICATIONS

In comparison to other authentication techniques, the 3D password can have a very wide password space, making the protection of vital systems and resources one of its key application fields.

- Critical Servers

There are important servers in many large firms, and they are typically secured by a text password. A text-based password can be effectively replaced with a 3D password.
- Nuclear and Military Facilities

The strongest authentication techniques should be used to safeguard these facilities. The 3D password is a wise choice for high-level security settings since it has a very large probable password space and can integrate token, biometric, recognition, and knowledge-based authentications into a single authentication system.
- Airplanes and Jet Fighters

The use of such aircraft should be safeguarded by a robust identification mechanism due to the potential hazard of exploiting planes and jet fighters for religiopolitical purposes. Additionally, because the 3D virtual environment can be customized to meet the needs of each system, 3D passwords can be utilized in less important systems. The following systems, for example, can make use of a small virtual environment.
- Some other applications are:

- ATM
- Desktop Computers & laptop logins
- Web Authentication

## VIII. SECURITY ANALYSIS

The following factors must be taken into account to evaluate and analyze how secure a system is: Based on the information contained in a password space, a measurement may be possible. Although the textual password space may be vast, it has been shown that it only takes a small portion of the total password space to successfully compromise such an authentication system. It is crucial to establish a scheme with a very broad range of potential passwords since this makes it harder for an attacker to compromise the authentication system. Look for a technique that is completely unaware of the most likely user password choice.
Typical rules for selecting strong passwords are made to make them more difficult to guess by computer programs:

- If the system permits, use upper- and lowercase letters, digits, and symbols in your passwords. Passwords should be between 12 and 14 characters long, and longer if you can make them memorable.
- Use capital and lower-case letters if the system considers the case to be important.
- Avoid using passwords that are based on dictionary words, repetition, letter or number sequences, usernames, pet or family names, romantic connections (past or present), or biographical details (e.g., dates, ID numbers, ancestor's names or dates, ...)
- Passwords should be simple for users to remember and shouldn't compel them to take unsecured insecure behaviors (e.g., the very bad and insecure practice of writing the password down on a Post-It note stuck to the monitor)

- Brute Force Attack

The potential 3D passwords must all be tried by the attacker. For the following reasons, this form of attack is exceedingly challenging. the time needed to log in Depending on the volume of interactions and activities, the size of the 3D virtual environment, and the nature of the interactions and actions, the total time required for a valid user to log in may change. Consequently, a 3D password brute force attack is exceedingly challenging and time-consuming. The cost of an attack Both token-based objects and biometric recognition objects are present in the 3D virtual world. The attacker must fabricate all biometric data that is conceivable, as well as all necessary tokens. Because it is exceedingly expensive to fake such data, it is harder to break the 3D password. Due to a large amount of potential 3D password spaces, the attacker has very little probability of successfully cracking the 3D password.

- Well Studied Attack

The assailant searches for the most likely distribution of 3D passwords. The attacker must have information about the most likely distributions of 3D passwords to start such an attack. Because the attacker must research every authentication method currently in use in the 3D environment, this is quite challenging. It necessitates research on the objects that the user chose for the 3D password. A well-studied attack is also highly challenging to execute because it must be specifically tailored for each unique 3D virtual world design. Unlike any other 3D virtual environment, this one contains a variety of objects and object response types. Consequently, to launch a successful attack, a properly crafted study is necessary.

- Shoulder Surfing Attack

An attacker watches the authorized user while they execute the 3D password or employs a camera to record the user's 3D password. The most effective method of attack against 3D passwords and several other graphical passwords is this one. The user's 3D password might, however, include text passwords or biometric information that cannot be seen from behind. As a result, we consider that using the 3D password should be done in a safe location where shoulder surfing attacks are impossible.

- Timing Attack

In this technique, the attacker watches the amount of time it takes the authorized user to successfully sign in using the 3D password. The attacker can determine the length of the 3D password from this observation. However, since it only provides the attacker with suggestions, this form of attack cannot be extremely effective on its own. It would therefore likely be launched as a part of a planned or brute-force attack. The inefficient design of the 3D virtual world can make timing attacks particularly effective.

## IX. FUTURE WORK

The most popular user authentication methods are text-based passwords and token-based passwords. However, numerous other plans have been applied in particular fields. Although they haven't been used in the real world, more strategies are being researched. The goal of this effort is to create a system with a large password space that combines all current and future authentication schemes into one scheme.

A 3D password allows the user the option to model his 3D password to include any preferred authentication scheme. Users are not required to submit their fingerprints if they want not to. The system administrator's design of the three-dimensional virtual environment can represent the likely password space for a 3D password. The administrator may decide to include any things in the three-dimensional virtual world that they believe the users are familiar with. For instance, football players can use a three-dimensional virtual stadium where they can move about and interact with recognizable elements. Critical systems and resources make up the majority of 3D Password's application domains.

A 3D Password system with a huge three-dimensional virtual environment can safeguard vital systems like military bases, critical servers, and highly classified regions. Moreover, less important systems like handheld devices, ATMs, and operating system logins can be protected using a modest three-dimensional virtual world. The practical strength of a 3D password may be demonstrated by learning the likely distribution of a user's 3D password. Additionally, research is being done to establish a defense against attacks using shoulder surfing on 3D passwords and other authentication methods.

## X. CONCLUSION

Currently, there are numerous authentication methods available. Some of them are based on the user's physical and behavioral characteristics, while other authentication strategies, like textual and graphical passwords, are based on the user's knowledge. Additionally, some other significant authentication methods depend on your possessions, including smart cards. Textual passwords and token-based systems, or a combination of both, are frequently used among the many authentication strategies. A multifactor authentication

method known as the 3-D password integrates these numerous authentication methods into a single 3-D virtual environment.By adding it as a reaction to activities taken on an item, the virtual environment can incorporate any current authentication scheme or even any upcoming authentication schemes. As a result, the generated password space grows far larger than any of the existing authentication systems. The 3-D virtual environment's layout, the choices made for the things inside of it, and the nature of the objects themselves all represent the final password space. The system administrator's job is to plan the environment and choose the right object to reflect the needs of the protected system. Furthermore, creating a straightforward and user-friendly 3-D virtual environment is a component that increases the user acceptability of a 3-D password system.The user's tastes and needs are reflected in the selection of the authentication mechanisms that will be included in their 3-D password. In addition to their 3-D password, a user who likes to memorize and recall their password may choose textual and graphical passwords. However, users who have a harder time remembering or recalling things may want to employ smart cards or biometrics as part of their 3-D password.

## REFERENCES

[1]. Tejal Kognule, Yugandhara Thumbre, Snehal Kognule, 2012, "3D PASSWORD" International Conference on Advances in Communication and Computing Technologies (ICACACT).
[2]. Ganesh Jairam Raj Guru, "Secure Authentication with 3D Password", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 68-75.
[3]. Nayana S, Dr. Niranjanamurthy M, Dr. Dharmendra Chahar, October 2016," Study on Three Dimensional (3D) Password Authentication system," International Journal of Advanced Research in Computer and Communication Engineering.
[4]. Prof. Dr.G.M.Bhandari, Naikwadi Shradha, Deshpande Gandhali, Tapkire Priya, Nawale Sanchita, September 2016, " A Survey on 3D Password," International Journal of Innovative Research in Computer and Communication Engineering.
[5]. https://www.uniassignment.com/essay-samples/information-technology/secured-authentication-3d-password-information technology-essay.php