ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Secure Authentication with 3D Password

Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod
Department of Computer Engineering, Amrutvahini Collage of Engineering, Sangamner

Abstract*—Providing Authentication to any system leads to provide more security to that system. There are many authentication techniques are available, Such as textual password, Graphical password, etc. but each of this individually having some limitations & drawbacks. To overcome the Drawbacks of previously existing authentication technique. A new improved authentication technique is used, This authentication Scheme is called as 3D password. The 3D password is multi-password & multi-factor authentication system as it uses a various authentication techniques such As textual password, Graphical password etc. Most important part of 3d password scheme is inclusion of 3d virtual environment. 3d virtual environment is virtual environment which is consisting of real time object scenarios. It is not actual real time environment, it is just user interface provided to scheme which looks like same as real environment. 3d password is more secure authentication scheme than any other authentication techniques. Because this authentication scheme is more advanced than any other schemes. Also this scheme is hard to break & easy to use. In this paper we have introduced our contribution towards 3D Password to become more secure & more user friendly to users of all categories. This paper also explaining about what is 3D password?, working of 3D password scheme, some mathematical concept related to 3D password, applications of scheme etc. all these concepts are briefly introduced & explained in this paper as per section wise.

***Index Terms*–Authentication, Multi-password, Quick Hull algorithm, Textual Passwords, 3-D Password, 3-D Virtual Environment.**

I. INTRODUCTION

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].

Ideally there are two types of Authentication schemes are available according to nature of scheme & techniques used, those types are

1) Recall based:

In this authentication tech. user need to recall or remember his/her password which is created before [1]. Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

2) Recognition based:

In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used.

Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time. To overcome these drawbacks & limitations of previously existing authentication schemes. We have introduced a new authentication scheme which is based on previously existing schemes. This authentication scheme is based on combination of passwords called as *"3D Password"*. Which is a multifactor scheme uses combination of above discussed scheme as well as biometric & many other schemes [1]. All these schemes are implemented in virtual 3D environment while creating 3d Password. Where this environment contain various virtual objects through which user interacts with. The interaction with 3D environment changes as per user changes. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions [2][3][5].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

II. PROPOSED SYSTEM

Proposed authentication scheme is combination of many other authentication schemes together. 3D password is combination of both recall-based (i.e. textual password, etc) & recognition based (i.e. graphical password, biometrics, etc). so that 3D password is multifactor & multi password authentication scheme. Refer fig.1

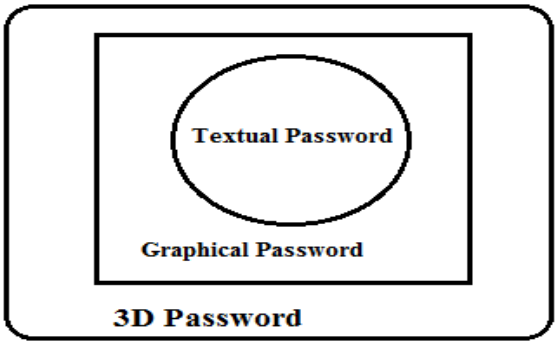
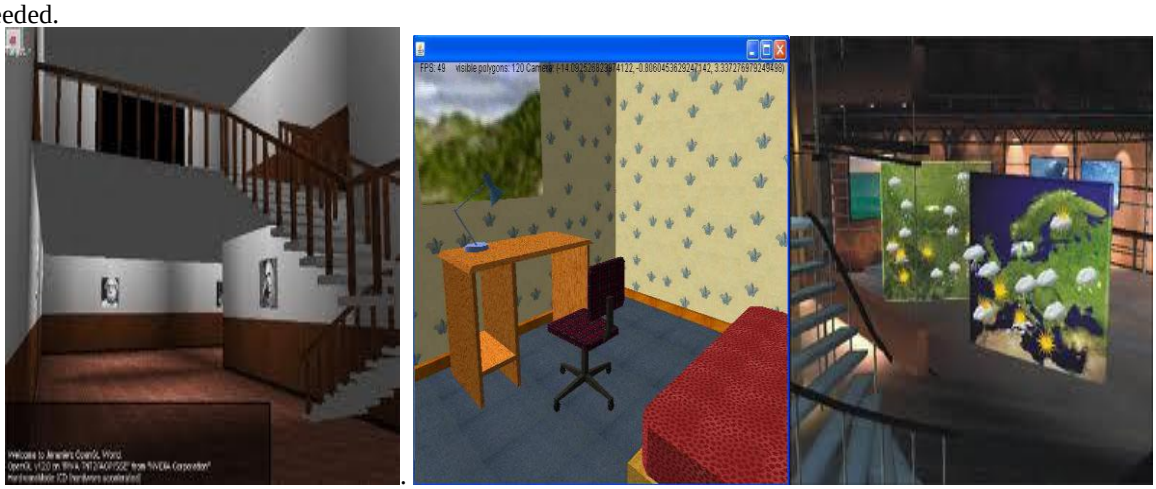


Fig. 3D password as Multi-factor & Multi-password Authentication scheme.

Fig. 1 Multifactor authentication scheme

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) (c)

Fig 2 (a) snapshot of Art Gallery, (b) snapshot of study room, (c) snapshot of weather forecasting office

Fig. 2 shows some snapshots of 3D Virtual Environment of different real time scenarios created in virtual environment like art gallery, office, and study room, 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 proposed system

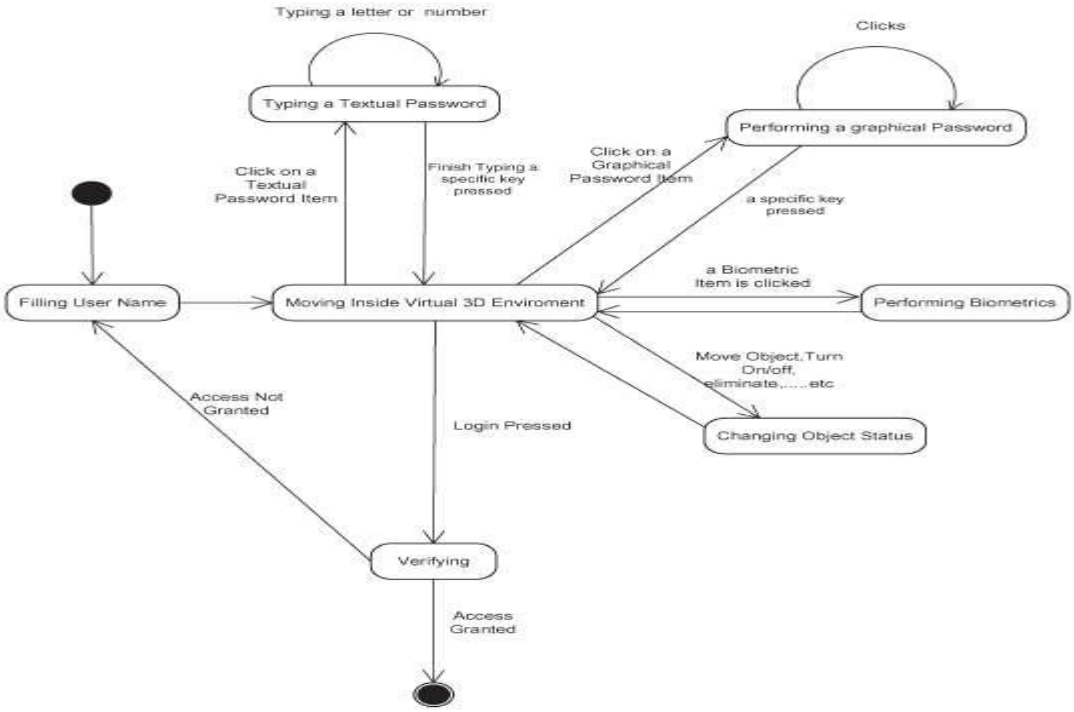
- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems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

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

III. 3D PASSWORD

A. *Architectural study*

This section tell about that how to create 3D password & what are different schemes used to form a complete 3d password.. 3D password is multi-factor & multi password authentication scheme. So that many password schemes like textual password, graphical password, biometric, etc. password schemes can be used as a part of 3D password. Choosing of different schemes are
based on category of user who are going to use this scheme to there system. Fig.3 shows state diagram of 3D password creation.



.Fig.3 state diagram of creating 3D password [1] [6] [7].

B. *Working of 3D password scheme*

In 3D password user have to First Authenticate with simple textual password(I.e. user need to provide user name & password) Once authentication successful then user moves in 3D virtual environment, Thereafter a computer with keyboard will be seen on screen. On that screen user have to enter password (textual).which is stored in a simple text file in the form of encrypted co-ordinates(x1, y1, z1). After successfully completion of this authentication, Then user automatically enter into an art gallery, where he/she has to select multiple point in that gallery or he can do some action in that environment like switching button on/off or perform action associated with any object like opening door, etc[1]. The sequence in which user has clicked (i.e. selecting objects) that sequence of points are stored in text file in the encrypted form. In this way the password is set for that particular user. For selection of points we have used 3d Quick hull algorithm which is based on convex hull algorithm from design & analysis of algorithms. Next time when user want to access his account then he has to select all the object which he has selected at the time of creating password with proper sequence .This sequence is then compared with coordinates which are stored in file. If authentication successful thereafter access is given to authorized user. 3D password working algorithm is shown in fig.4. Which will give the flowchart for 3D password creation & authentication process.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

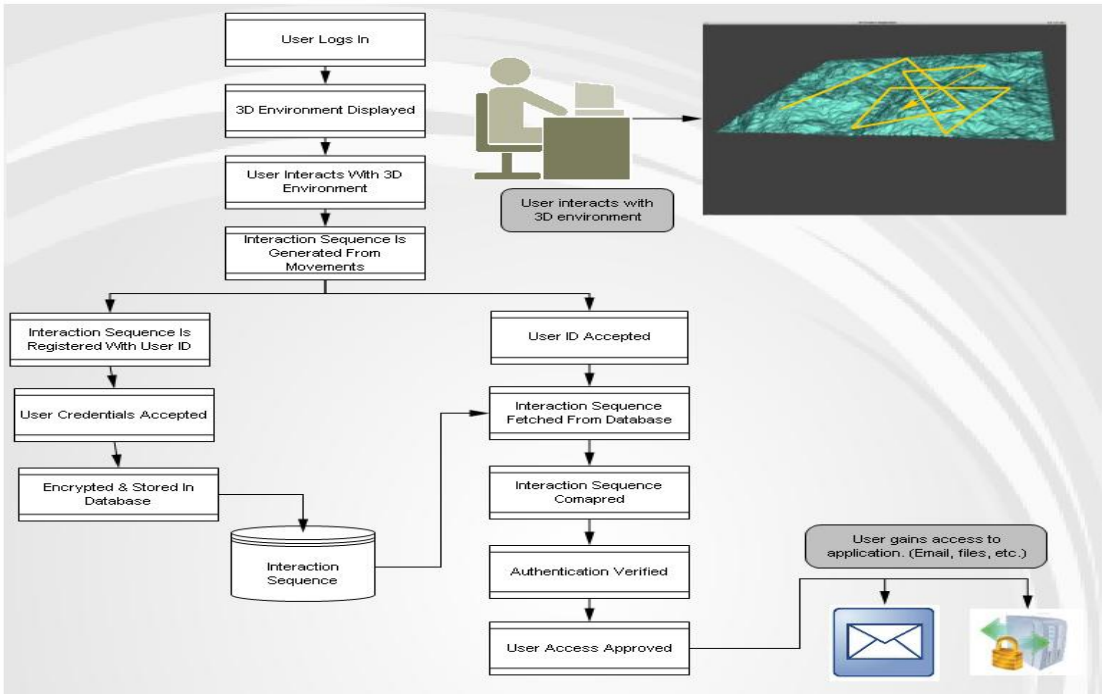


Fig.4 working of 3d password scheme [5]

C. *3D virtual environment*

In this multi-factor authentication scheme the basic building block used is 3D virtual environment. 3D virtual environment is created inside a 2D screen, refer fig.5. 3D environment is a real time scenario seen by peoples in day to day life which is created virtually in 3d virtual environment. We can use any real time object as a environment like any room or village but for simplicity we suggest to use small environment like room.

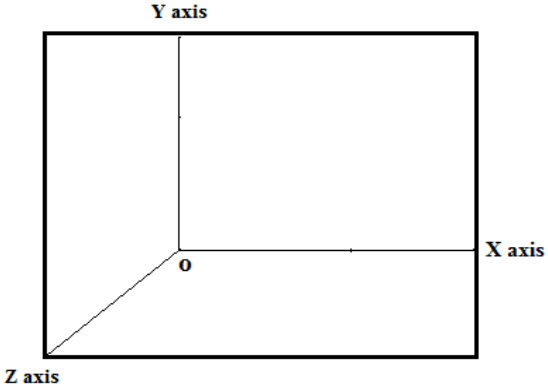


fig. 3D Virtual Environment under 2D screen

Fig. 5 3D environment under 2D screen

For selecting the sequence of objects (i.e. points) we have used a very simple, easy & efficient algorithm called as convex hull algorithm. The 3d quick hull algorithm is used. & also the points selected are stored in the form of 3d co-ordinate(x, y, z) in a simple text file. Some design guidelines related to 3d environment such

- Virtual environment selected in such a way so that it is similar to real life object.
- Every object is unique & distinct from other.
- Virtual environment size should be considered [1].

IV. MATHEMATICAL CONCEPTS RELATED TO 3D PASSWORD SCHEME

3D password is a authentication technique which can be implemented in 3D virtual environment. As every project having problem statement which is relation with mathematical concepts like feasibility study,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

complexities, set theory etc. this section of paper will explain almost all the mathematical concepts applied while creating 3D password schemes.

A. Time Complexity

For calculating the time complexity of 3D password scheme let's assume A be the virtual 3d environment plotting, & B is algorithmic processing. From this data available we have come to time complexity of system. Equation (1) gives the time complexity of proposed system.

Time Complexity=$A^m + B^n$ (1).

Where m is time required to communicate with system, & n is time required to process each algorithm in 3d environment.

B. Space Complexity

This system include 3D virtual environment, so that each point in this environment will having 3 co-ordinate values. Any point from 3D virtual environment is represented in the form of (X, Y, Z).Where X, Y & Z are the coordinate values stored for particular point. We are storing three co-ordinate values of each point such as (x1, y1, z1). There for space complexity of proposed system is n^3.

C. Class of problem

When solving problems we have to decide the difficulty level of our problem. There are three types of classes provided for that. These are as follows:

1) P Class
2) NP-hard Class
3) NP-Complete Class

A decision problem is in P if there is a known polynomial-time algorithm to get that answer. A decision problem is in NP if there is a known polynomial-time algorithm for a non-deterministic machine to get the answer. Problems known to be in P are trivially in NP — the nondeterministic machine just never troubles itself to fork another process, and acts just like a deterministic one.

But there are some problems which are known to be in NP for which no poly-time deterministic algorithm is known; in other words, we know they're in NP, but don't know if they're in P.A problem is NP-complete if you can prove that (1) it's in NP, and (2) show that it's poly-time reducible to a problem already known to be NP-complete. A problem is NP-hard if and only if it's "at least as" hard as an NP-complete problem. The more conventional Traveling Salesman Problem of finding the shortest route is NP-hard, not strictly NP-complete. We know that time complexity & space complexity of this system. So that 3D password produces feasible solution, hence this system is feasible & is in NP-Complete type.

V. 3D PASSWORD SECURE AUTHENTICATION SCHEME

A. Attacks & countermeasures:[1]

As mentioned earlier 3D password is most secure authentication. We will see different kinds of attacks & how 3D password scheme is more secure against different attacks.

1) Timing Attacks

This attack is based on how much time required completing successful sign-in using 3D password scheme. Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our 3D password scheme is designed more securely, these kinds of attacks are not easily possible on 3D Password & also not much effective as well.

2) Brute force Attacks

In This kind of attacks the attacker has to try n number of possibilities of 3D Password. As these attacks considers following two points.

- Required time to login: as in 3d password time required for successful login varies & is depend on number of actions & interactions, the size of 3d virtual environment.
- Cost required to attack: as 3d password scheme requires 3D virtual environment & cost of creating such a environment is very high.

3) Well-studied attacks

In this attack attacker has to study whole password scheme. After studied about scheme the attacker tries combination of different attacks on scheme. As 3d password scheme is multi-factor & multi-password authentication scheme, attacker fail to studied whole scheme. this attacks also not much effective against 3D password scheme[2].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

4) Key logger

In this attack attacker install as software called key logger on system where authentication scheme is used [7]. This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password, but as 3D password is multi password authentication scheme. So that this kind of attacks are not much effective in this case [5].

5) Shoulder Surfing attacks

Attacker uses camera for capturing & recording of 3D password. This attack is more effective than any other attacks on 3D password. So that 3D password must be performed in a secure place where this attack can't be performed. Shoulder surfing attacks is still effective & easily possible against 3D password [1].

B. Advantages

- 3D Password scheme is combination of re-call based, recognized based, Biometrics .etc into single authentication technique [1].
- Due to use of multiple schemes into one scheme password space is increased to great extend.
- More secure authentication scheme over currently available schemes.

C. Disadvantages

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

D. *Applications*

As 3D password authentication scheme is more useful & more secure than any other authentication schemas, 3D password can be used in wide area where more security is needed to system. Some of areas are as follows:

1) Networking*:*

Networking involves many areas of computer networks like client-server architecture, critical servers, etc. To provide more security to server of this architecture 3D password can be used. It very efficient & more secure way to keep data or important information secure from unauthorized people. For email applications 3D password is most secure & easier scheme to used.

2) Nuclear & military areas

Nuclear & military area of a country are most important area where more security is needed we can use 3D password scheme in this area for more providing more secure authentication**.** 3D password scheme can protect data or secrete information about these areas very securely.

3) Airplane & jetfighters

There is possibility of misuse of airplanes and jetfighters for religion-political agendas. Such airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems. In addition, 3-D passwords can be used in less critical systems [1] [4] [6].

4) Other areas

we can use 3d password authentication scheme to areas such as ATM, Cyber cafes, Industries (for data security), Laptop's or PC's, critical servers, web services, etc & many more[1]-[4],[6][7].

VI. CONCLUSION AND FUTURE WORK

Currently available schemes include textual password and graphical password .But both are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use [1]. The 3-D password is a multifactor & multi password authentication scheme that combines these various authentication schemes. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes. Due to which passwords space increases. It is the user's choice and decision to construct the desired and preferred 3-D password. The 3D password is still new & in its early stages [1]. Designing various kinds of 3-D virtual environments, deciding on password spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password. Gathering attackers from different background and attack made by them and how to overcome them is main future work. Shoulder surfing attacks are still possible so how to overcome that is a field of research & development [1]. Inclusion of biometrics leads to increasing cost & hardware in scheme, to reduce this is still field of research. So that 3D password can be used in many application areas as discussed earlier & also many more area other than those. Thus this paper tells about our study about 3D password, still it is in early stage. Future work is needed in 3d password scheme to develop this scheme up to more secure level. Implementing 3D password for mobile handset is the another important future work of this paper & also our project too.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

ACKNOWLEDGEMENT

We are thankful to our project guide & H.O.D of computer department **Prof. R.L Paikrao**. He had motivated & guides us for creating this review paper on 3D password which is more secure scheme than existing one.

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] Vidya Mhaske et al, Int.J.Computer Technology & Applications, Vol 3 (2), ISSN: 2229-6093, 510-519.

[3] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, "3D password", International Journal of Computer Applications (IJCA), 2012.

[4] A.B.Gadicha , V.B.Gadicha , "Virtual Realization using 3D Password", in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.

[5] 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.

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

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

AUTHOR BIOGRAPHY

Gunjal Vipul Suresh is currently pursuing degree in Bachelor of Engineering in the field of Computer Engineering, From Amruitvahini College of Engineering, and Sangamner. Currently working on Final Year project with subject '3D Password for more secure authentication'. Interested in security, animation, software testing etc.

Kolhe Vishal Nivrutti is currently pursuing degree in Bachelor of Engineering in the field of Computer Engineering, From Amruitvahini College of Engineering, Sangamner. Currently working on Final Year project with subject '3D Password for more secure authentication'.

Kalaskar Sayali is currently pursuing degree in Bachelor of Engineering in the field of Computer Engineering, From Amruitvahini College of Engineering, and Sangamner. Currently working on Final Year project with subject '3D Password for more secure authentication'.

Rathod Pranjal is currently pursuing degree in Bachelor of Engineering in the field of Computer Engineering, From Amruitvahini College of Engineering, and Sangamner. Currently working on Final Year project with subject '3D Password for more secure authentication' and he is the owner and founder of Ensemble solutions, which is the leading software and web hosting company.