ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

3D Login
For More Secure Authentication

Ashwini A. Khatpe[1], Sheetal T. Patil[2], Amruta D. More[3], Dipak V. Waghmare[4], Ajit S. Shitole[5]

Student, Dept. of Compute Engineering, Sinhgad Academy of Engineering, Pune, India[1]

Student, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[2]

Student, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[3]

Student, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[4]

Assistant Professor, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[5]

ABSTRACT: 3D password is nothing but a multifactor authentication scheme. Authentication is a necessary element need to provide to any system as it leads to provide more security to that system. But current authentication techniques have some limitations and weaknesses. They are textual passwords, biometric authentications, graphical passwords, etc. These techniques do not satisfy the security concern regarding authentication scheme completely. A new improved authentication technique is used to overcome the drawbacks of previously existing techniques, which is called as 3D password. In this technique, 3D password is created with help of 3D virtual environment. 3D virtual environment is just a user interface provided to the scheme which looks like same as real environment. 3D virtual environment is consisting of real time object scenarios. User navigates inside the 3D virtual environment and user's interactions towards the objects construct the user's 3D password. This scheme is hard to break and easy to use and also for user, it is easy to remember the 3D password. As 3D password is advanced authentication scheme, it is more secure authentication scheme than any other authentication techniques. In this paper, we present and evaluate our contribution towards 3D Login to the E-mail client system with the help of 3D password to become more secure and more user-friendly to the users. This paper also explains the concept about what is the 3D password, how the Working of 3D password scheme is done, some concepts related to 3D password, applications of the scheme.

Keywords: 3D password, 3D virtual environment, 3D password space, working of 3D password, applications.

I. INTRODUCTION

A. BACKGROUND of AUTHENTICATION TECHNIQUES

Now-a-days, usage of computer system has been increased much and it has given rise to many security concerns. One major concern is authentication which is process of validation. There are many authentication techniques were introduced previously. Generally authentication techniques can be divided into three main areas:

- Token based authentication techniques
- Biometric based authentication techniques

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

- Knowledge based authentication techniques

Token based means what you have. This includes credit cards, ATM cards, key cards, smart cards, etc. To enhance security many token based authentication systems also use knowledge based techniques. Most token based systems require personal identification number (PIN) for authentication, as token based systems are vulnerable to theft and loss. **Biometric based** means what you are. It includes techniques such as fingerprints, palm prints, iris scan, face recognition, voice recognition, etc. This system can be expensive and identification process can be slow and often unreliable, is the major drawback of this technique. **Knowledge based means** what you know. It is the most widely used authentication technique and include both text based (textual) and picture based (graphical) passwords. This technique is further divided into recall based and recognition based techniques. In **recall based** password scheme user repeat or reproduce the secret that the user created before during registration or earlier stage, e.g. textual password. In **recognition based** password scheme user identify and recognize the secret or part of it that the user selected before during registration stage, e.g. graphical password [1]. Textual password is most common method used for authentication. Eves dropping, dictionary attack, social engineering, shoulder surfing are the vulnerabilities of this method. Textual passwords are easy to break. Graphical password is based on the idea that users can remember images better than words. Some graphical password schemes require long time to be performed. Most of the graphical passwords can be easily observed or recorded while legitimate user is performing a graphical password [2].

B. 3D PASSWORD AUTHENTICATION SCHEME

As we have seen all available authentication techniques have some limitations and drawbacks. We have introduced a new authentication scheme which is based on previously existing authentication techniques to overcome their issues. Combination of passwords is known as 3D password which is also called as multifactor scheme. It is called so because it uses combination of above discussed authentication schemes. To create a 3D password all these schemes are implemented in a 3D virtual environment. 3 D virtual environment contains several virtual objects or items with which user can interact. In 3D virtual environment, 3D password is constructed by observing the actions and interactions of the user with the virtual objects and by observing the sequences of such actions. The number of possible 3D passwords will increase, as large number of objects and items are given in 3D virtual environment. Therefore, it becomes much more difficult to guess the user's 3D password for the attacker. 3D password authentication scheme provides the secrets that are easy to remember and also that can be easily revoked or changed.

II. RELATED WORK

Current Era is an electronic world, where all their needs are met through internet. Different authentication mechanisms have emerged and came into existence. In this situation people having choice of one of the human authentication methods for their secure web services. These authentication methods are based on what you know, what you have and finally what you are (textual password, token based, and biometrics respectively).

3D password scheme combines many authentication schemes such as token based, knowledge based and biometrics based. Knowledge based technique has two schemes 1) Textual and 2) Graphical. Many graphical password schemes have been proposed. Blonder introduces graphical password scheme. Blonder's idea of graphical passwords is that by having predetermined images the user can select touch regions of the image causing the sequence and the location of the touches to construct the user's graphical password. After Blonder the notation of graphical password was developed. Many graphical schemes have been proposed. Recognition graphical password scheme that authenticates user choosing the portfolios among decoy portfolios. In token based technique, as a security to system tokens are provided like ATM cards, etc. But it may get lost.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Biometrics scheme is more powerful than these technique but injuries can deny access to authenticated person. Introduction of 3D authentication overcome the drawbacks of knowledge based, token based and biometrics based techniques .With help of 3D environment we can create not easily breakable password for number of application e.g. 3D login for e-mail client. In mobile technology area, the operating system likes Android providing facility of 3D login. Currently 3D login authentication is also used in financial organization to increase security layers for money.

III. PROPOSED AUTHENTICATION SYSTEM

The 3D password authentication scheme can combine all existing authentication schemes into a single 3D virtual environment which is consists of different virtual objects or items. Which type of authentication techniques will be part of their 3D password is the user's choice to select it. User interacts with these objects or items in 3D virtual environment and the type of interaction varies from one item to another. The choice of authentication type can be achieved through interacting only with the objects that acquire information that the user is comfortable in providing, so that by ignoring the objects that request information with which user is not comfortable, user prefers not to provide. Moreover, giving user the freedom of choice as to what type of authentication schemes will be part of their 3D password enhances the usability of the system.

3D password technique is combination of both recall based (i.e. textual password, etc.) and recognition based (i.e. graphical password, etc.), so that multifactor and multi password are the another names for 3D password authentication scheme. In our proposed 3D password authentication system, we don't use token and biometric authentication schemes. Because these schemes are having some major drawbacks, thus we haven't included token based and biometric based authentication schemes in our proposed authentication system. Token based schemes are vulnerable to theft and loss as well as to some other attacks if it uses knowledge based scheme. Biometric scheme is efficient over shoulder surfing attack but other attacks are easy on it. And another thing is, inclusion of token based and biometric based schemes may leads to increase of cost of the system and more hardware parts also needed.

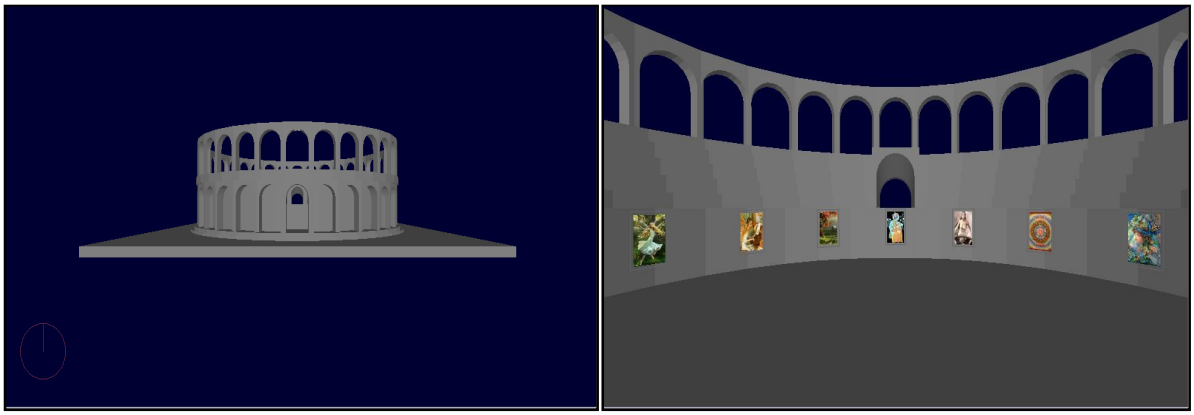
We are implementing the 3D password authentication scheme with the help of email client system. We are creating the email client system with the strong security by providing 3D password authentication scheme to it. The user creates an account to use the email client system for mailing purpose by providing his profile information and by creating the 3D password in 3D virtual environment. After that user gets access to the email client system by providing his or her correct or same 3D password which was created at the time of account creation. Creation of account using 3D password enhances the security of the user's account. User accesses email account by following sequences of the actions done in 3D virtual environment while creating a 3D password. 3D virtual environment plays an important role in the creation of 3D password. User navigates inside the 3D virtual environment and clicks on the virtual objects in a significant sequence. Thus, it is very difficult for the intruders to guess the 3D password and also even it is difficult to observe password while user providing it, as user moves in virtual environment and clicks on some objects in a definite sequence. So it is not easy for observer who wants to hack the user's account to observe whole sequence of 3D password. If we assume that observer gets known about some clicks of the password still he or she can't get access to user's account. Because as soon as when he or she attempts wrong clicks after giving sequence of right clicks which he or she knows, system gets alert that user is not entering the password and it shows different sequence of objects which is not the part of user's 3D password. So that intruders can't access the user's account in any way.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014



(a) (b)

Figure 1 (a) Snapshot of 3D virtual environment entry, (b) Snapshot of an art gallery

Fig. 1 shows some snapshots of different real time scenarios created in 3D virtual environment like art gallery. User can interact with virtual objects in 3D virtual environment and creates the 3D password.

A. Objective of Proposed System

- To provide more secure authentication scheme to the system than the existing one.
- To give user the freedom of selecting more than one password scheme as single system.
- To design and develop more user friendly and easier authentication scheme.
- To generate 3D virtual environment in such a way that it is similar to real life objects and every object is unique and distinct from other.
- To overcome the weaknesses and issues of the previously existing authentication techniques.

IV. 3D PASSWORD IMPLEMENTATION

A. ARCHITECTURAL STUDY of 3D PASSWORD

In this section, we will see how to create 3D password and what are different schemes used to form a complete 3D password. As we know, 3D password is multifactor and multi password authentication scheme, thus many password schemes like textual password, graphical password can be used as a part of 3D password. Choosing one of the schemes from different authentication schemes is based on category of user who is going to use this scheme to the system. 3D password presents a 3D virtual environment which is nothing but the conversion of real life scenarios into the virtual objects. For creation of 3D password user moves inside this environment and interacts with the virtual objects. The interaction with virtual objects inside 3D virtual environment differs as per the different users. In 3D password system, the first step is to design a 3D virtual environment that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

reflects the administration needs and the security requirements. 3D virtual environment is a basic building block of the 3D password authentication system. Designing a well studied 3D virtual environment enhances the usability, effectiveness and acceptability of a 3D password authentication system. Fig. 2 shows the state diagram of creation of 3D password.

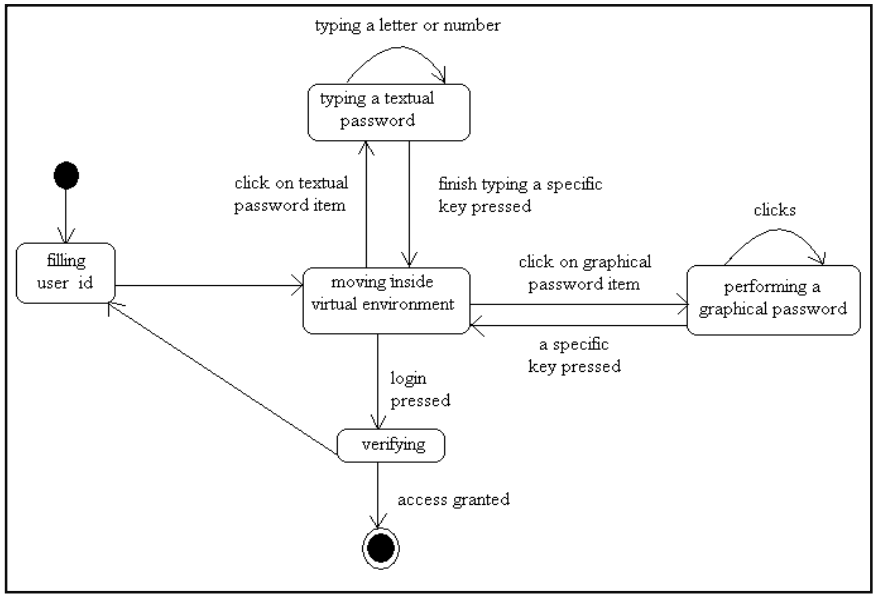


Figure 2 State diagram of 3D password creation

B. WORKING of 3D PASSWORD

3D password key space is determined by the design of the 3D virtual environment and type of object selected. Let us consider G x G x G be the size of 3D virtual environment space. The objects are distributed with the unique (x, y, z) coordinates in the 3D virtual environment [4]. We are implementing 3D password scheme to provide the security to the email client system. To access mailing services user need to create the account. To create his or her account user has to feel up his or her profile details like user id, etc. and has to provide password which is nothing but 3D password. After giving profile information in 3D password scheme, user moves in 3D virtual environment. We assume that the user can navigate inside 3D virtual environment and interact with the virtual objects using any input device such as mouse, keyboard. In 3D virtual environment, user enters into an art gallery. Art gallery is consists of many images in it. User has to select multiple point or images in that art gallery. The sequence in which user has clicked or select the objects that sequence of points are stored in text file in the encrypted form. In this way the 3D password is set or created for the particular user. We have used Centered Descretization method and Secure Hash Algorithm for the selection of the points and to manage database. Next time when user wants to access his or her account, he has to select all objects which he has entered at the time of creating password with correct sequence. This sequence then compared with the coordinates which are stored in file. Access is thus given to the authorized user if authentication gets

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

successful. Working of 3D password is shown in fig. 3 which depicts the flowchart for 3D password creation and authentication process.

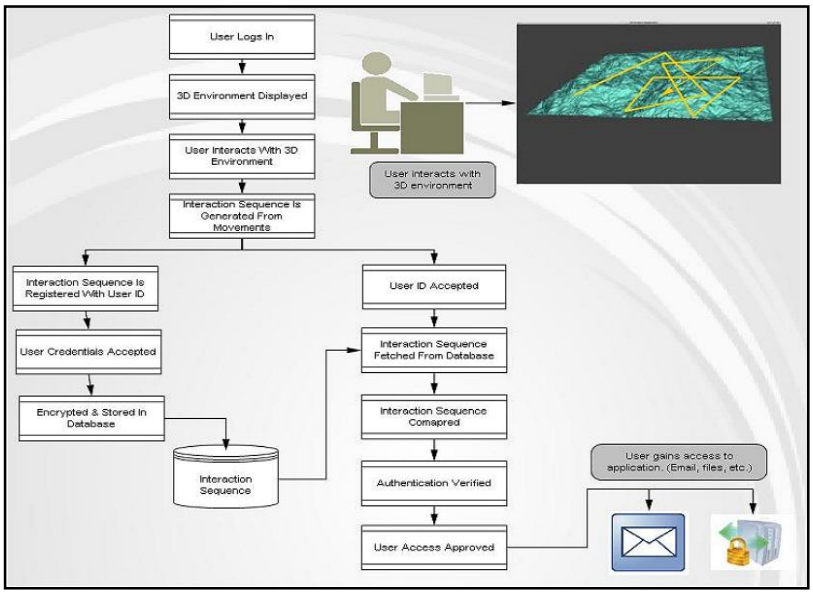


Figure 3 Flowchart for 3D password authentication process

V. 3D PASSWORD APPLICATIONS

3D password can be used in wide areas where more security needed to the system, as 3D password authentication scheme is more useful and more secure than any other existing authentication schemes. 3D password's main application domains are protecting critical systems and resources, because 3D password can have a password space which is very large as compared to the other authentication schemes.

A. *NETWORKING:* Networking involves many areas of computer networks like client-server architecture, critical servers, etc. 3D password can be used to provide more security to the server of this architecture. To keep data or important information secure from unauthorized people, it is very efficient and more secure way. For email application 3D password is most secure and easier scheme to use.

B. *CRITICAL SERVERS:* Critical servers are usually protected by a textual password, many large organizations have it. 3D password authentication scheme proposes a sound replacement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes by PIN numbers. Henceforth, 3D password can be used to protect the entrance to such locations and protect the usage of such servers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

C. *AIRPLANES and JETFIGHTERS:* For religion as well as political agendas, there is possibility of misuse of airplanes and jetfighters. By using powerful authentication system such airplanes should get protected. The 3D password authentication scheme is recommended for these kinds of the systems [1] [4].

D. *NUCLEAR and MILITARY AREAS:* We can use 3D password scheme in this area for providing more secure authentication as nuclear and military areas of a country are most important area where more security is needed. 3D password scheme can protect data or secrete information very securely about these areas. 3D password authentication scheme is a sound choice for high level security locations [1] [4].

E. *OTHER AREAS:* The 3D password authentication scheme has wide areas of application. We can use 3D password authentication scheme to areas like ATMs, cyber cafes, in industries for data security, to laptops or PCs, web services and much more.

VI. SECURITY ANALYSIS of 3D PASSWORD SCHEME

To analyze and study how secure a system is, we need to consider how hard it is for the attacker to break the system. On the basis of the information content of a password space, a possible measurement can be done. As mentioned earlier 3D password is most secure authentication, in this section we will see different analysis methods and how 3D password authentication scheme is more secure than other authentication schemes.

A. *ATTACKS and COUNTERMEASURES*

We have to consider all possible attack methods to realize and understand how far an authentication scheme is secure. We need to find whether the authentication scheme proposed is immune against such attacks or not. In this section, we try to cover most possible attacks and whether the attacks are valid or not. Moreover, we try to propose countermeasures for such attacks that prevent such attacks.

1) *BRUTE FORCE ATTACK:* The attacker has to try n number of possibilities of 3D passwords in this kind of attacks. This attack is considered as very difficult for the following reasons:
   - Required login time: The total time needed by a legitimate user for successful login may varies, depending on the number of actions and interactions as well as their type, the size of 3D virtual environment.
   - Cost required to attack: As for creation of 3D password, 3D password scheme requires a 3D virtual environment and cost of creating such environment is very high.

2) *WELL STUDIED ATTACK:* The attacker has to study whole password scheme in this kind of attack. The attacker tries combination of different attacks on scheme after studied about scheme. As 3D password is authentication scheme is multifactor and multi password scheme, so attacker fails to studied whole scheme. In addition, it requires a study of the user's selection of objects, or a combination of objects, that the user used as a 3D password. This attack is also not much effective against 3D password scheme [3].

3) *SHOULDER SURFING ATTACK:* The attacker uses camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed in this kind of attack. Shoulder surfing attack is more effective

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

than any other attacks on 3D password. Thus we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed [2] [3].

4) *TIMING ATTACK:* The attacker observes how much time required for completion of successful login by the legitimate user using 3D password scheme in this kind of attack. Timing attacks can be effective if authentication scheme is poorly designed. These kinds of attacks are not easily possible on 3D password scheme, because our 3D password scheme is designed more securely and also not much effective as well [2] [3].

5) *KEY LOGGER:* In this kind of attack, attacker install software called key logger on the system where authentication scheme is used. This software stores text entered through keyboard and those text are stored in text file. This attack is more effective only for textual password scheme. Thus this attack is not much effective in this case because 3D password is a multi password authentication scheme.

VII. CONCLUSION AND FUTURE WORK

In current state, many authentication schemes available there are. But as we discussed before, these existing authentication techniques are vulnerable to certain attacks. Moreover, there are numerous authentication schemes that are currently under study and they may require additional time and effort to be use to provide required security to the system. The 3D password is a multifactor authentication scheme that combines benefits of various authentication schemes into a single 3D virtual environment by which usability of the system enhances. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. The simple and easy design of 3D virtual environment leads to higher user acceptability of the 3D password authentication system.

The 3D password is still in its early stages. Designing different kinds of 3D virtual environments, deciding on password spaces and understanding user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3D password. Gathering attackers from different background and attack made by them and how to overcome them is a main future work. Shoulder surfing attack is still possible so how to overcome that is field of research and development. Inclusion of token based and biometric based schemes leads to increasing cost and hardware of the system; to reduce this is still field of research. 3D password is used in many areas of application as mentioned earlier and also it has wide area of application other than those. Hence this paper tells about our study of 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 authentication scheme for email application is another important future work of this paper and also of our project too.

ACKNOWLEDGMENT

We take this opportunity to express our profound gratitude and deep regards to our internal guide A. S. Shitole Sir for his exemplary guidance and monitoring throughout. The valuable information given by him helped us while doing this project. Also we would like to take this opportunity to express a deep sense of gratitude to our HOD Prof. B. B. Gite for his cordial support and guidance.

Lately we thank to our friends for their constant encouragement throughout.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

REFERENCES

1. Alsulaiman, F. A.; EI Saddik, A., 'Three- for Secure', IEEE Transactions on Instrumentations and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
2. A. B. Gadicha, V. B. Gadicha, 'Virtual Realization using 3D password', International journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.
3. Chippy. T, R. Nagendran, 'defenses against large scale online password guessing attacks by using persuasive click points', International Journals of Communication and Engineering, vol. 03 no. 3, issue no. 1, March 2012.
4. Alsulaiman, F. A.; EI Saddik, A., 'A Novel 3D Graphical Password Schema', IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.
5. Birget, J. C., Hong, D., and Menon N., 'Graphical Passwords Based on Robust Discretization', IEEE Transactions on Information Forensics and Security, vol. 1, n0. 3, September 2006.
6. G. E. Blonder, 'Graphical Password', U.S. Patent 5 559961, Sep. 24, 1996.

BIOGRAPHY

Ashwini Atmaram Khatpe

Currently pursuing degree in Bachelor of Computer Engineering in the field of Computer Engineering from Sinhgad Academy of Engineering, Kondhawa (Bk.), Pune- 48. Currently working on Final Year Project which is 3D password for more secure authentication.

Sheetal Tatyasaheb Patil

Currently pursuing degree in Bachelor of Computer Engineering in the field of Computer Engineering from Sinhgad Academy of Engineering, Kondhwa (BK.) and Pune- 48. Currently working on Final Year Project which is 3D password for more secure authentication.

Amruta Dnyandeo More

Currently pursuing degree in Bachelor of Computer Engineering in the field of Computer Engineering from Sinhgad Academy of Engineering, Kondhwa (BK.) and Pune- 48. Currently working on Final Year Project which is 3D password for more secure authentication.

Dipak Vishwanath Waghmare

Currently pursuing degree in Bachelor of Computer Engineering in the field of Computer Engineering from Sinhgad Academy of Engineering, Kondhwa (BK.) and Pune- 48. Currently working on Final Year Project which is 3D password for more secure authentication.