A project report on

"Authentication Schemes for Session Password using Four levels"

submitted in partial fulfillment of the requirement for the award of

DIPLOMA IN
COMPUTER ENGINEERING

by

Suchita Kudke

Sharayu Mane

Harshada Jadhav

Bhagyashri Patil

Under the guidance of

Prof. Rushali Navale

DEPARTMENT OF COMPUTER ENGINEERING

DR. D. Y. PATIL POLYTECHNIC

Dr. D. Y. Patil Vidyanagar, Sector-7, Nerul, Navi Mumbai – 400706

Academic Year 2019– 2020

CERTIFICATE

This is to certify that the report on project entitled

"Authentication Schemes for Session Password using Four levels"

has been successfully completed and submitted by

NAME	ROLL NO	SEATNO
Suchita Kudke	03	
Sharayu Mane	08	
Harshada Jadhav	14	
Bhagyashri Patil	27	

for the partial fulfillment of the requirement for the award of Diploma Course in Information Technology as laid down by **Maharashtra State Board of Technical Education** for the academic year **2019 – 2020.**

During the project they have maintained regular attendance and have worked sincerely.

(_____)	(_____)	(_____)
(Prof.Rushali.Navale)	**(Prof.Umesh.Patil)**	**(Prof. N.P.Vetale)**
PROJECT GUIDE	**HOD**	**PRINCIPAL**

(_____)	(_____)
INTERNAL EXAMINER	**EXTERNAL EXAMINER**

CERTIFICATE

This is to certify that Mr./Ms……

From……Institute having Enrollment No.:……

has completed project of final year having title……

….……during the academic year 20__-20__. The project completed by group consisting of……persons under the guidance of the Faculty guide

……

…….

Name & Signature of Guide:……..

Telephone:……

ACKNOWLEDGEMENT

After the completion of this work, words are not enough to express feelings about all those who helped us to reach goals.

It's a great pleasure and moment of immense satisfaction for us to express our profound gratitude to our guide **Prof.Rushali Navale ,** whose constant encouragement enabled us to work enthusiastically. His perpetual motivation, patience and excellent expertise in the discussion during progress of the project work have benefited us to an extent, which is beyond expression.

We would also like to give my sincere thanks to **Prof. Umesh Patil**, **Head of Department,** from Department Information Technology**,** Dr . D.Y. Patil Polytechnic, Nerul, Navi Mumbai for his guidance, encouragement and support during the seminar.

We are also thankful to **Prof. N. P. Vetale , Principal**, Dr . D.Y. Patil Polytechnic, Nerul, Navi Mumbai for providing an outstanding academic environment, also for providing the adequate facilities.

Last but not the least; I would also like to thank all those who directly or indirectly helped us in completion of our work.

ABSTRACT

Authentication plays an important role in protecting resources against unauthorized and illicit use. Authentication processes might vary from easy secret based mostly authentication system to expensive and computation intense authentication systems. Passwords are a unit over
simply a key. They're used for many functions .They guarantee our privacy, keeping our sensitive info secure. For authentication we generally use textual password. Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eyes dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Session password can be used only once and every time a new password is generated .In this project we generated four level of security .They are :

- Textual Password
- Image Based Password Authentication
- Captcha based otherization
- OTP Authentication

INDEX

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

Authentication is the process of determining whether a user is authenticated to access a system. Text-based password is the most often used authentication system. A text password is nothing but a jumble of characters with strong encryption and decryption algorithm. But nowadays user can't remember strong password easily they create text passwords with pet names, phone number, etc. which is easy to remember and easy to guess. But password created must be easy to remember but hard to guess. Our human brain is better at remembering images than text. Our username identifies the user and therefore the secret validates user. However, the passwords have some weaknesses: over one person will possess its data at just once. Moreover, there's a continuing threat of losing your secret to any other person with venomous intent. There is a unit many various techniques like graphical passwords and bioscience. Biometrics, like fingerprints, iris scan or face recognition has been introduced, however, These builds systems to expensive and hard to adopt. The most disadvantage of this approach is that such a system will be high-ticket and therefore the identification method will be slow. Numerous graphical positive identification schemes are used as alternatives to alphanumerical positive identification.

Image passwords are meant for reducing the memory saddle on users. Image passwords may offer better security than text-based passwords because most of the people, in an attempt to memorize text-based passwords, use simple words. In this project, we propose an image based password authentication. A password consists of one click-point per image for a sequence of images. The image may be predefined or user defined. Image based password offers both improved usability and security. We are presenting three level authentication and one level of otherization. Text based password, Image base password, Captcha, and OTP. This four way authentication and otherization will help to improve security policy of the application.

CHAPTER 2

LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

Authentication based password is largely used in the computer security and privacy. Most of the traditional passwords are numbers and alphabets character. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known .The unauthorized people can easily identify the password. Random and lengthy passwords can make the system secure.However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked.

Lack of security has become a major concern, given the prevalence of attackers, hackers, crackers, scammers and spammers. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access a given system or resource. Adequate authentication is the first line of defense for protecting resources. Existing authentication processes are usually accomplished by user ID and password, with the authentication schemes alphanumeric-based, biometric-based or increasingly graphical-based. Alphanumeric passwords are no doubt the most commonly used method by far for user authentication, but the "password problem" arises .

To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user friendly passwords, while increasing the level of security.As we know graphical images are more easily recalled then text. In this selection so graphical password system based on recognition and recall based are discussed.

1)Recognition-Based Technique: In this type of technique, users will select pictures, logos or any symbols from prestored image. For authentication process user need to recognize the image, which he choose as a password.

2)Recall-Based Technique: Again recall-based password authentication are categorize in two parts

i) Pure Recall Based Technique

ii) Cued Recall Based Technique

CHAPTER 3

SCOPE OF THE PROJECT

CHAPTER 3

SCOPE OF THE PROJECT

Textual password are very much vulnerable. Various attack are possible on them. System using session password provide much security. Authentication using image based password can be used where security is very significant such as bank, army sector etc. we can use such system to protect the significant data.

The aim of this project is that the various techniques used by an imposter to get access to the system fail. We are presenting three level authentication and one level of otherization. Text based password, Image base password, Captcha, and OTP. This three way authentication and otherization will help to improve security policy of the application.

- To develop secure system
- To avoid eves dropping
- To avoid shoulder surfing
- To avoid dictionary attack

CHAPTER 4

METHODOLOGY

CHAPTER 4

METHODOLOGY

Generally textual passwords are used for authentication, but textual passwords are vulnerable to many attacks such as dictionary attack, eves dropping, shoulder surfing and social engineering. Graphical passwords are introduced to overcome the disadvantages of textual password but many of the graphical passwords are vulnerable to shoulder surfing. To overcome this problem session passwords are created. A session password is a password uniquely generated for every session. The scheme allows the system to automatically generate a session password each time the user logs in. The session password is generated randomly based on the randomly generated grid. The grid is used as a medium for password generation. While registration the user must normally enter his username and password while registering into the system. Now the system stores this password and uses it to generate a unique session password while user logs in the next time. During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters.

- **Password**

A password is a string of characters used for authenticating a user on a computer system. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. While usernames are generally public information, passwords are private to each user.

- **Image Based Authentication scheme:-**

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters.
Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed.
There are two set of 3 x 3 grid and it consist alphanumeric images and images. These are randomly placed on the grid and the interface changes every time.
In our case, we are going to use the image sequencing password to enhance the security. In this system, the user selects a four number of images from each set of random pictures during registration. Later, during login the user has to identify the preselected images for authentication from a set of images

- **Captcha based otherization:-**

Captcha depends on the gap of capabilities between humans and robots in determination sure arduous AI issues .There are a unit 2 types of visual Captcha that is text Captcha and Image- recognition Captcha (IRC). The previous depends on character recognition while the latter depends on recognition of non-character objects.

- **Login with OTP Authentication**

Login with an OTP code is a secure method for the user authentication process.
In this method, a one-time password is generated dynamically and sent to the user who attempts login. OTP can be sent to the user's email or his mobile phone. When the user enters the OTP code then the application will authenticate the user via this code.

CHAPTER 5

DETAILS PF DESIGNS . WORKING AND PROCESSES

CHAPTER 5

DETAILS OF DESIGNS , WORKING AND PROCESSES

Flow of Project

Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed.

There are two set of 3 x 3 grid and it consist alphanumeric and images. These are randomly placed on the grid and the interface changes every time.

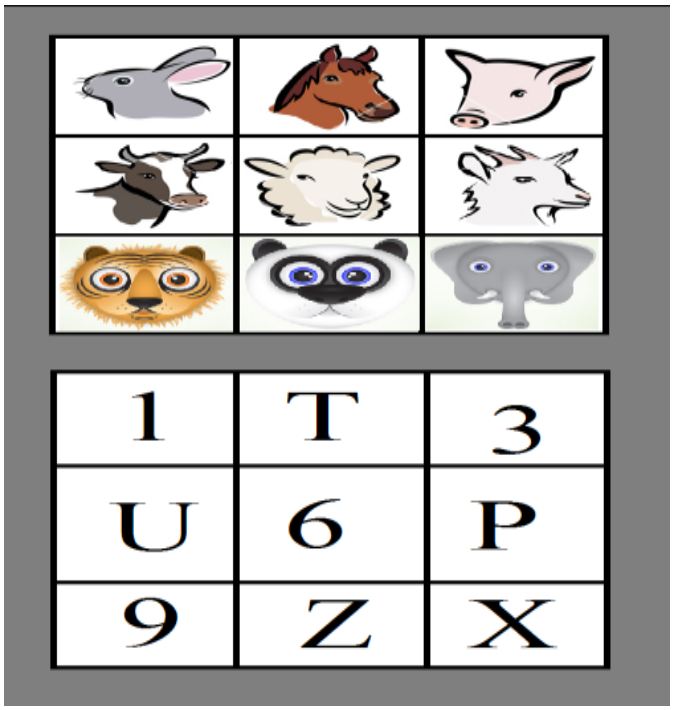
In our case, we are going to use the image sequencing password to enhance the security. In this system, the user selects a four number of images from each set of random pictures during registration. Later, during login the user has to identify the preselected images for authentication from a set of images

It is efficient to use both CAPTCHA and text password in a user authentication to create an additional layer of security over the passwords. Captcha and password work side by side and independently in such captcha-assisted systems. Captcha filters out the suspicious programs from the human beings and password recognizes the legitimate user among the human beings.

An OTP is more secure than a static password, especially a user-created password, which can be weak and/or reused across multiple accounts. OTPs may replace authentication login information or may be used in addition to it in order to add another layer of security.

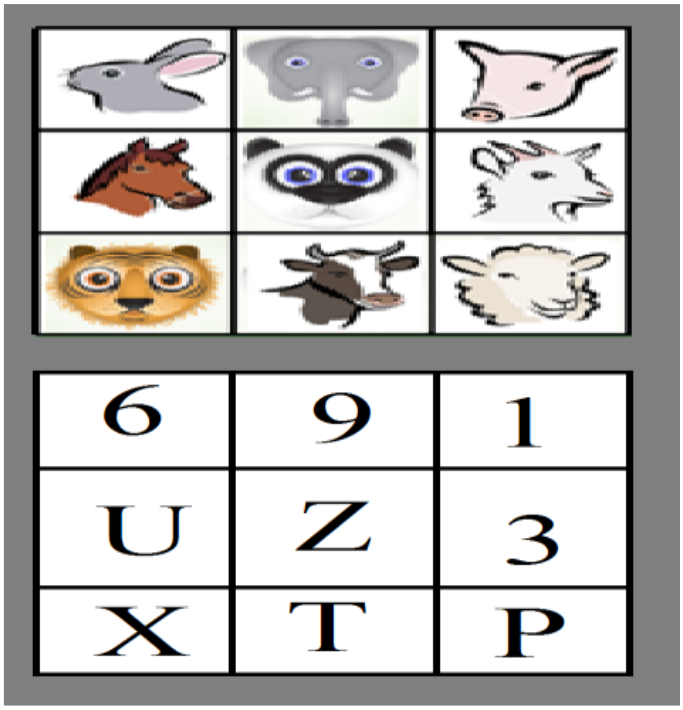
Modules :-

1. User Registration Module :- User register into the application by filling Personal information, text base password, Image base Password.
2. Image base password will be work as follows: In our case, we are going to use the image sequencing password to enhance the security. Suppose in this we have a sequence of horse-cow-goat-panda-1-6-U-Z. The sequence number of them is 24681548. So when we enter the sequence number we are enter to the database. Here we are going to use two set of images for image sequencing and each image contains 9 sequence. First diagram contain animals and second contains numeric and alphabets.



Here in the figure, when you again get on this page or refresh the page your sequence will be changed and according to sequence your password is also changed.

The position of the animals are shuffle, hence our password is also change. Now our password becomes 48653145 according to the position of horse-cow-goat-panda.



We are also use the RSA algorithm as:

1. Choose two large prime numbers P and Q

2. Calculate N = P x Q

3. Select the public key (i.e., Encryption Key) E such that

it is not a factor of (P-1) and (Q-1)

4. Select the Private key (i.e., Decryption Key) D such that

the following equation is true:

(D X E) mod (P-1) X (Q-1) = 1

5. For encryption, Calculate the cipher text CT from the

plain text PT as follows:

CT = PT^E mod N

6. Send CT as the cipher text to the receiver

7. For Decryption, Calculate the plain Text PT from the

cipher text CT as follows:

PT = CT^D modN

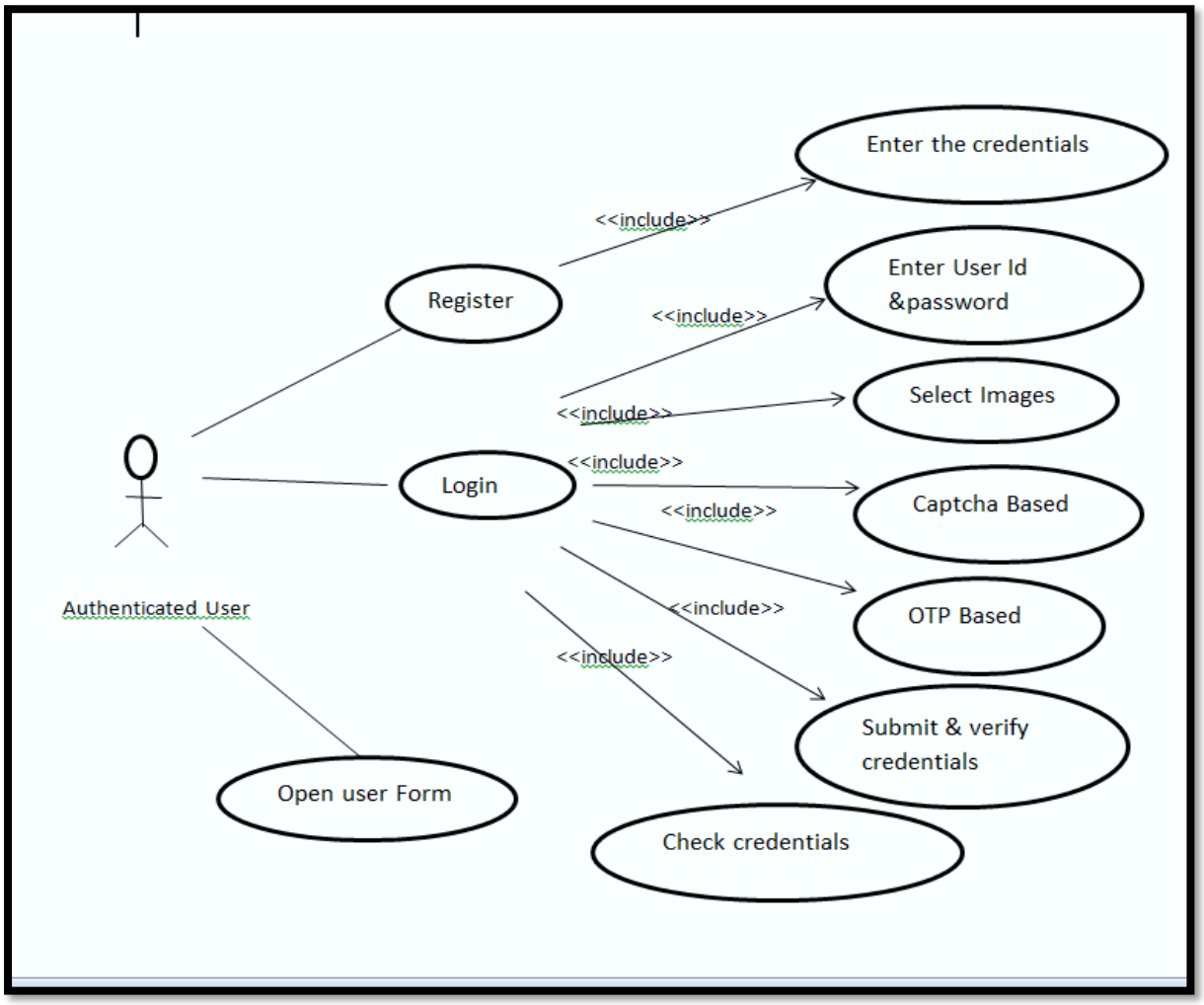
2. User Login:- while login into the system user have to follow a procedure.

First user will enter his Username and Password, then user select the image sequence which was specify during registration. Then user have to solve Captcha and user will get one OTP for OTP Verification process.

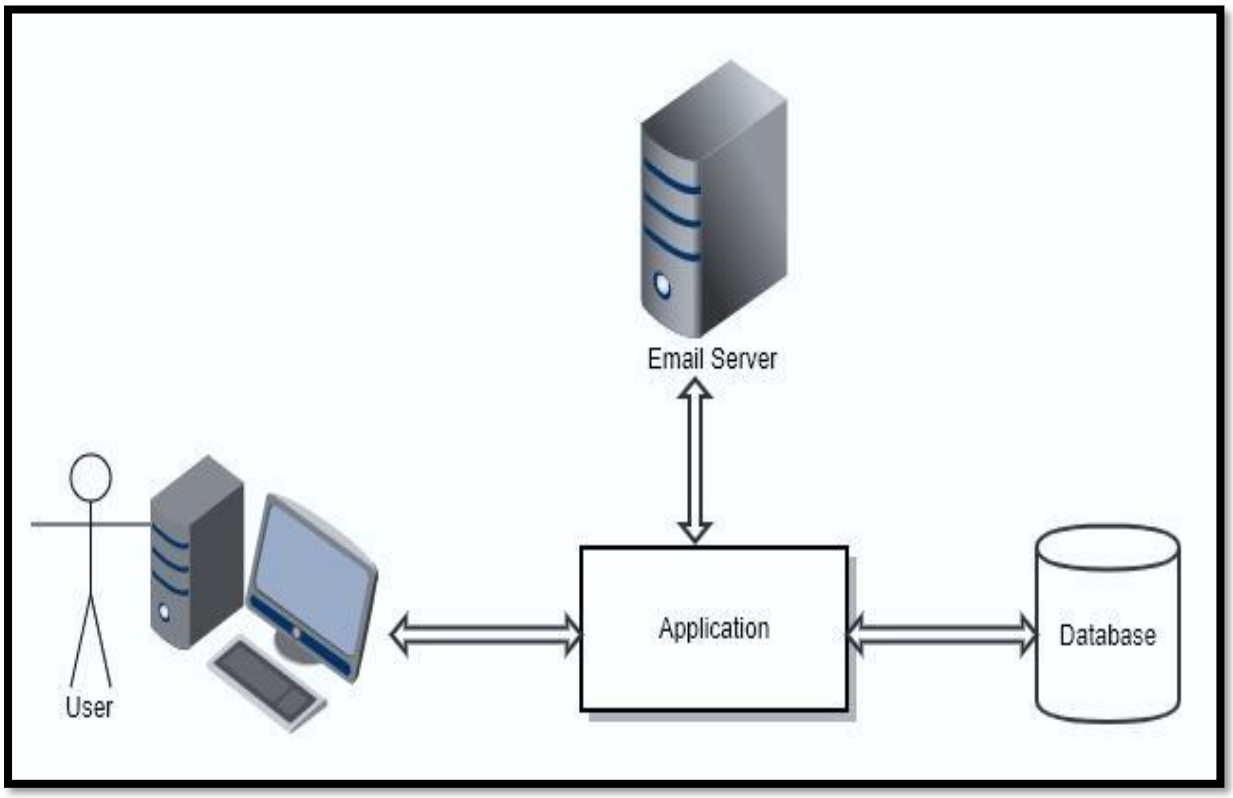
If all the Authentication will get right then user will get the access of the application.

UML Diagrams

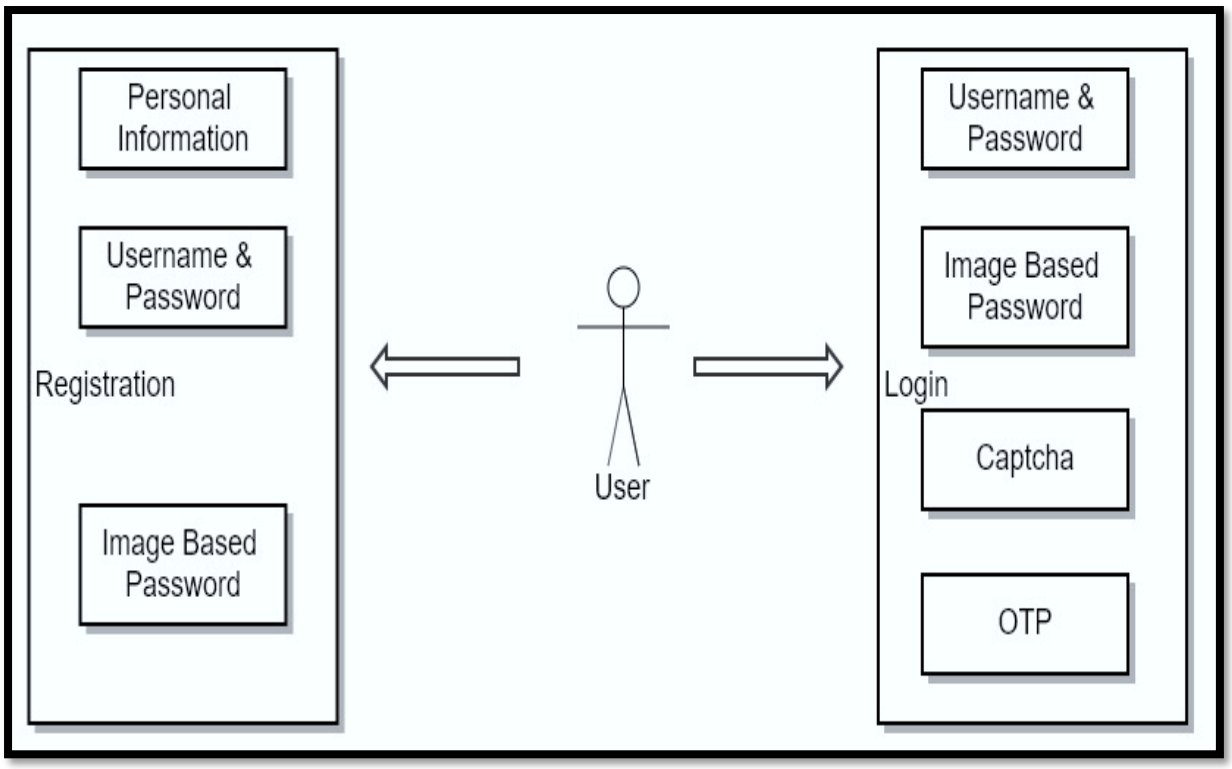
USE CASE MODEL:-



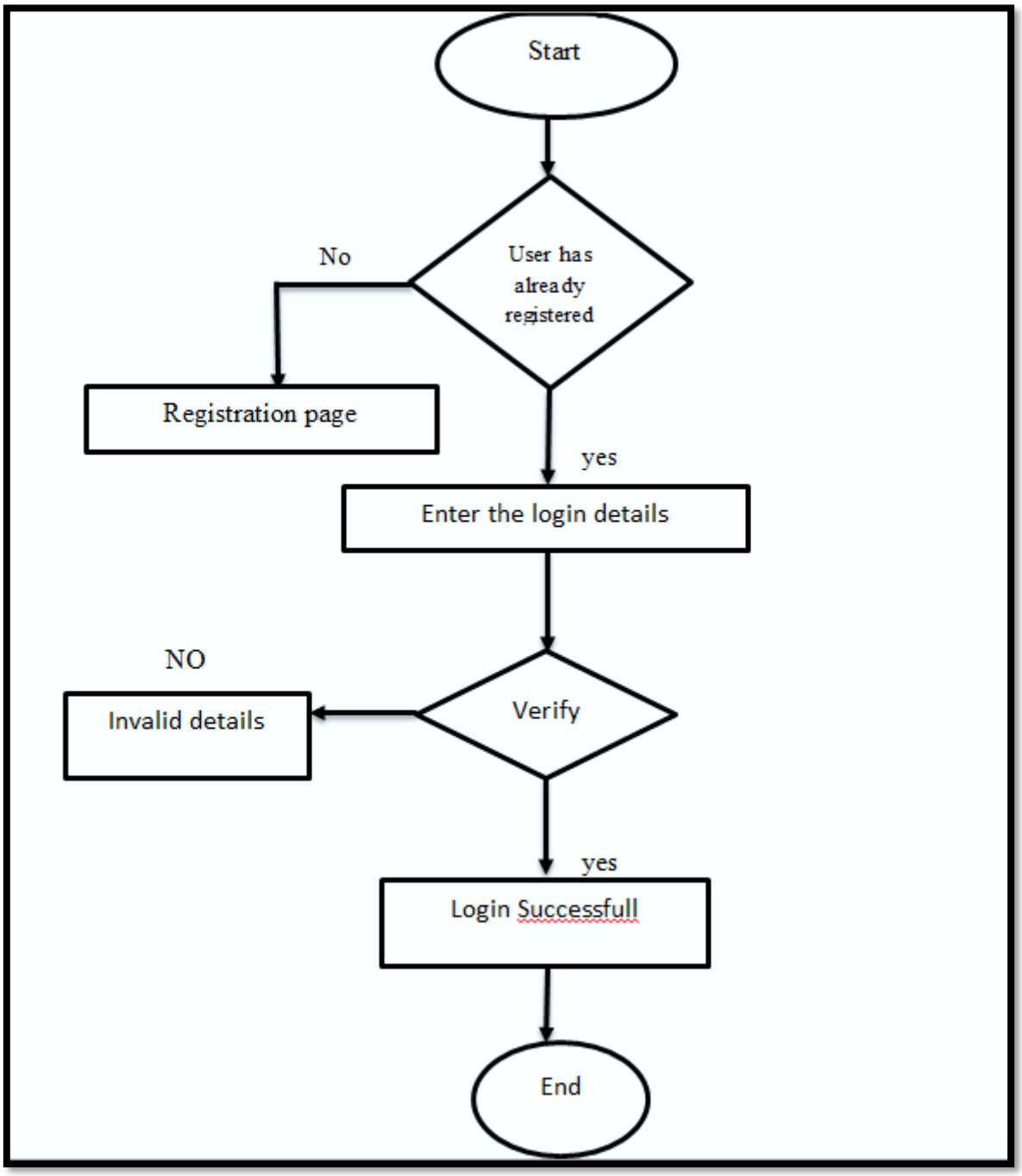
Architecture diagram:-



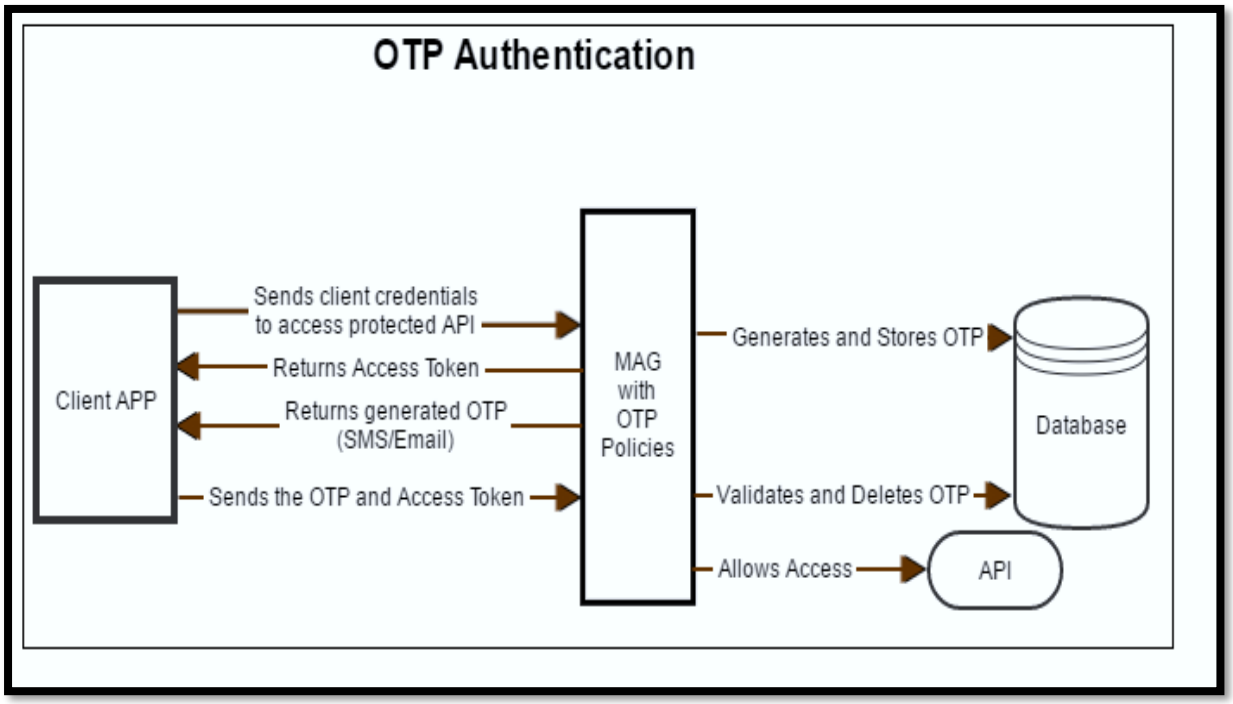
Functional Diagram:-



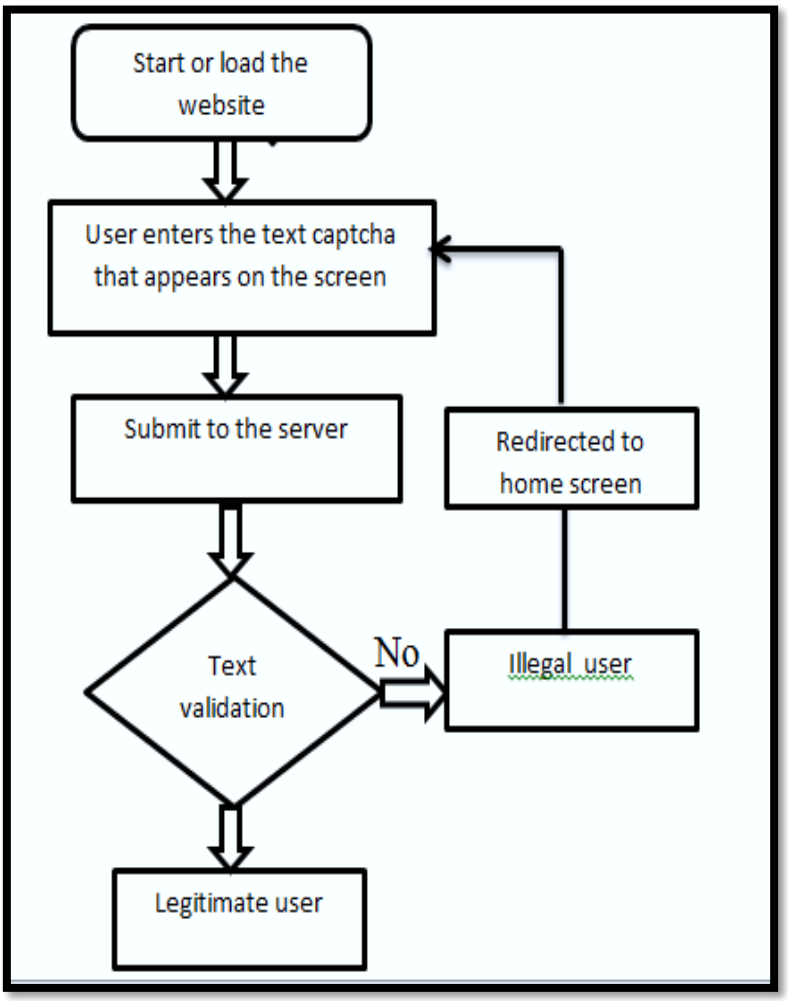
FlowChart


Start
User has already registered
No
Registration page
yes
Enter the login details
NO
Invalid details
Verify
yes
Login Successfull
End

OTP Authentication



Captcha


Start or load the website
User enters the text captcha that appears on the screen
Submit to the server
Redirected to home screen
Text validation
No
Illegal user
Legitimate user

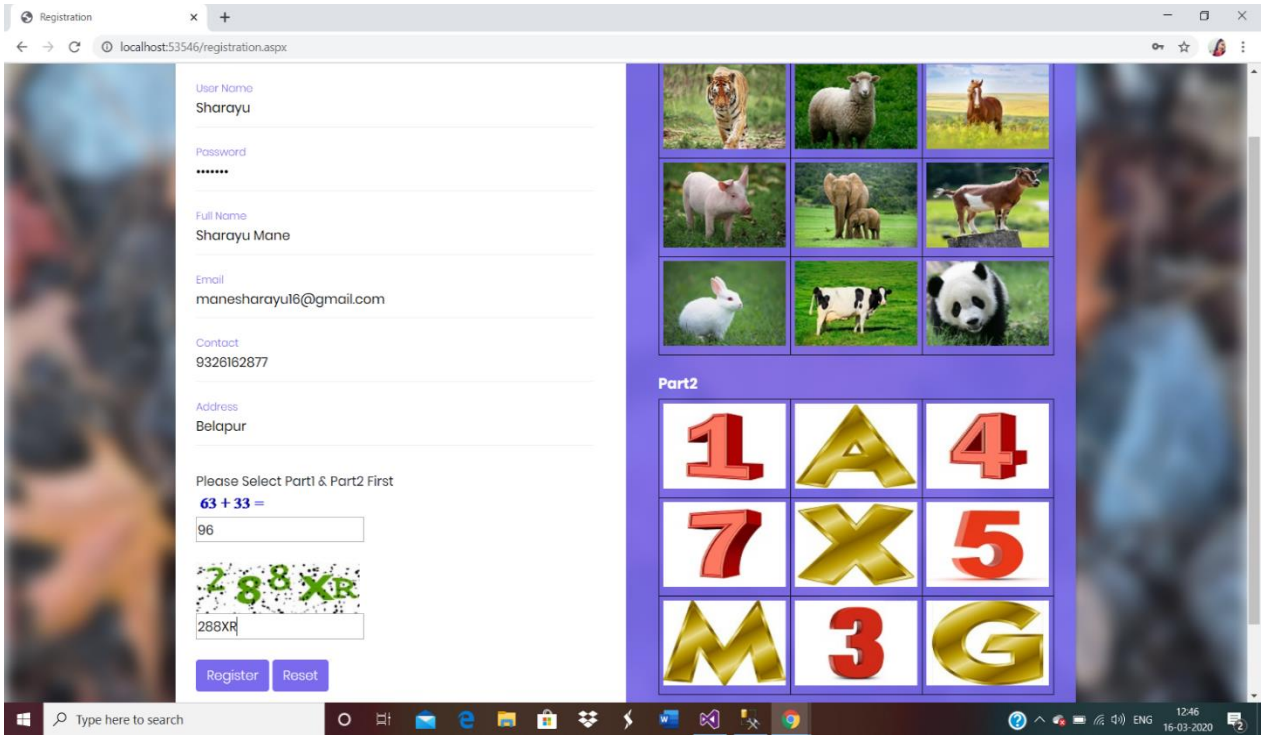
CHAPTER 6

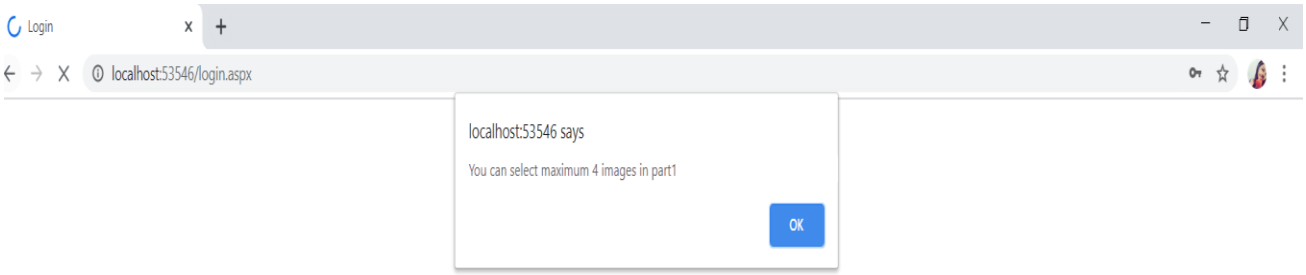
RESULTS AND APPLICATIONS

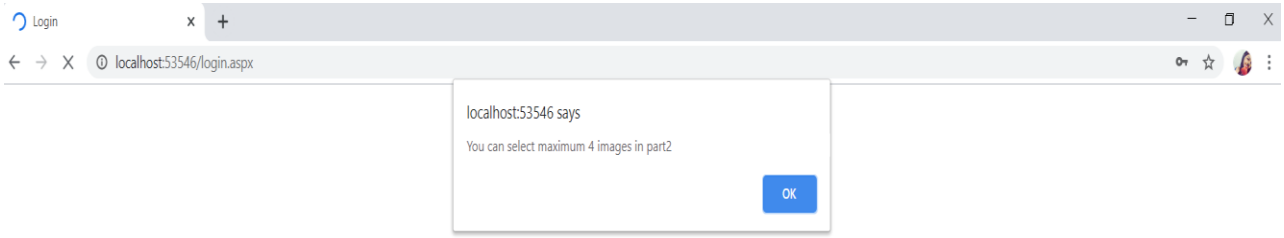
CHAPTER 6

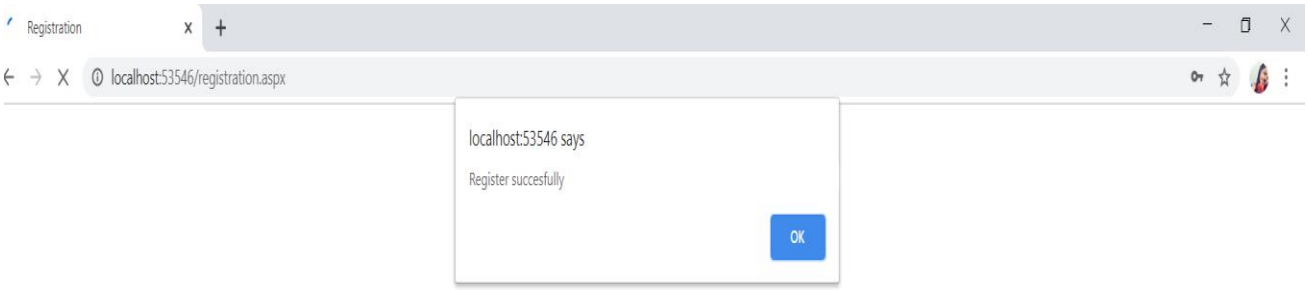
RESULTS AND APPLICATIONS

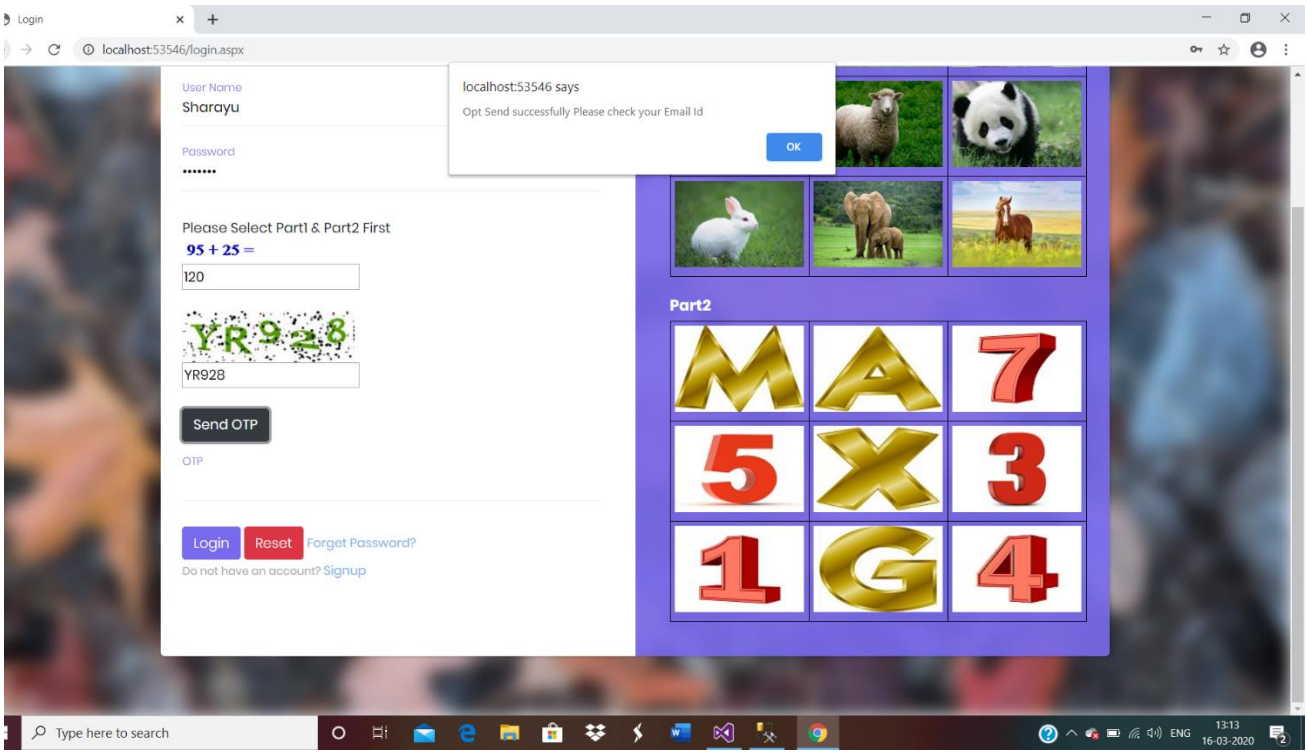
RESULTS

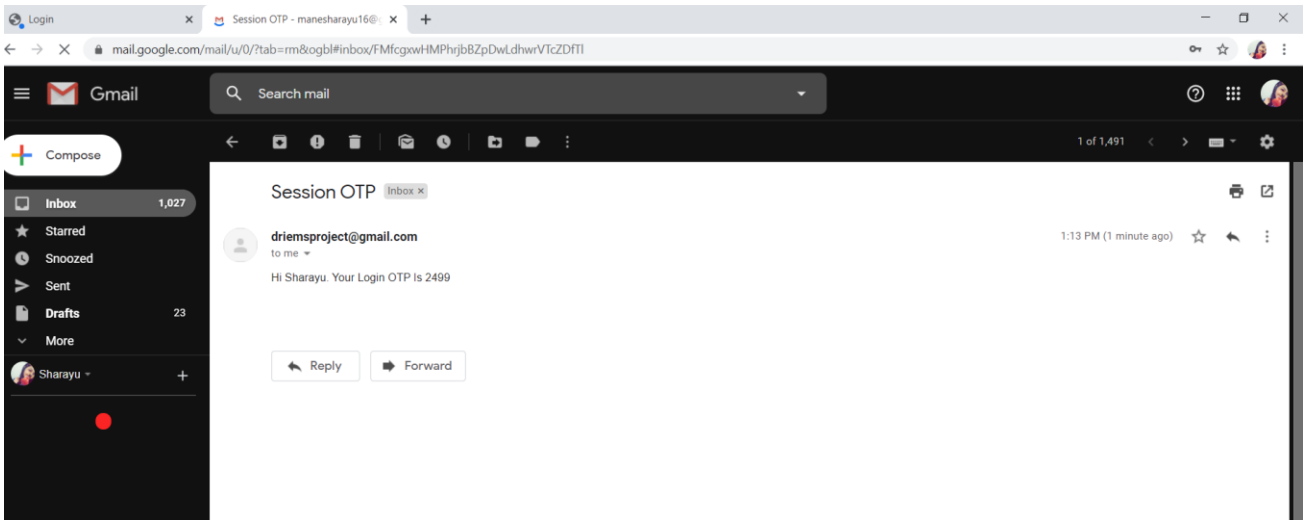


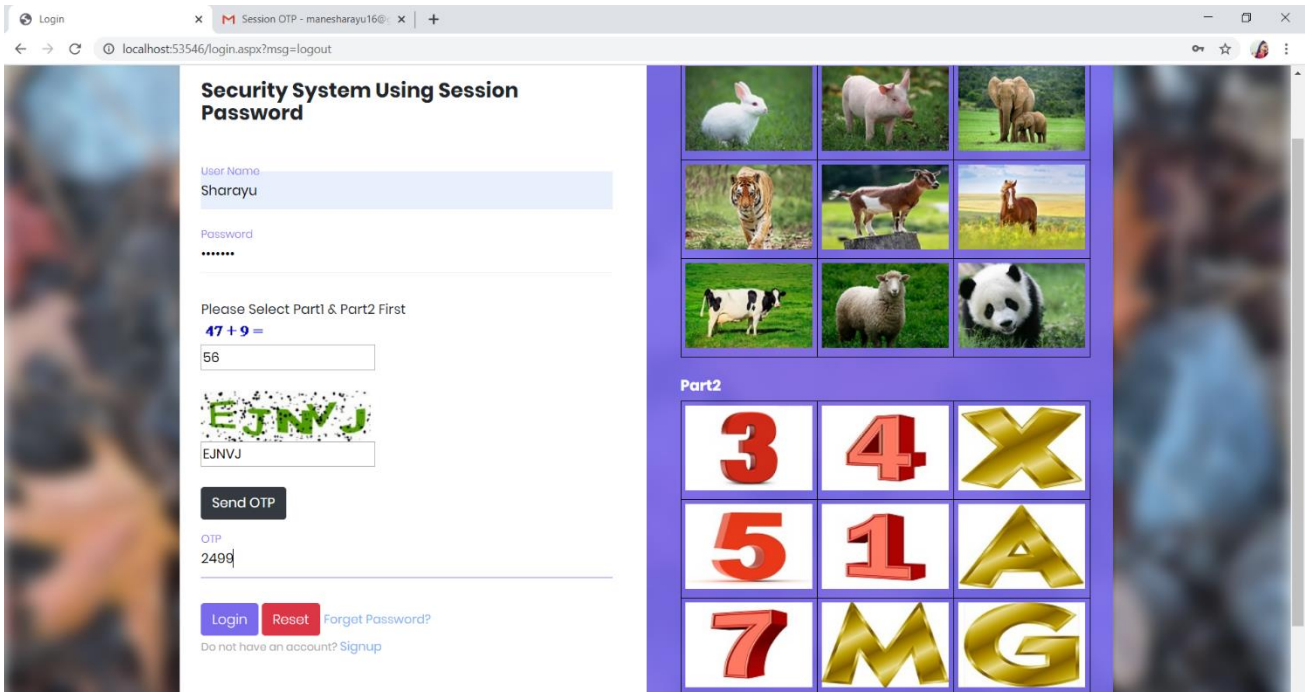

Login
localhost:53546/login.aspx
localhost:53546 says
You can select maximum 4 images in part1
OK

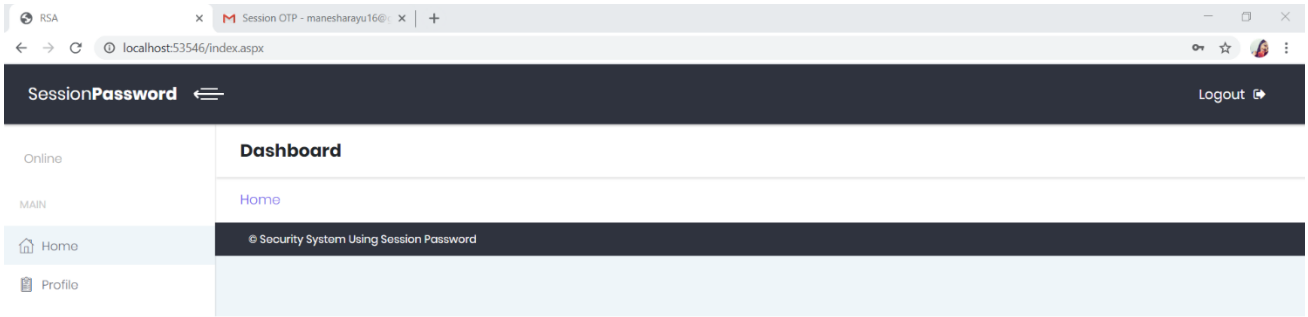

Login
localhost:53546/login.aspx
localhost:53546 says
You can select maximum 4 images in part2
OK

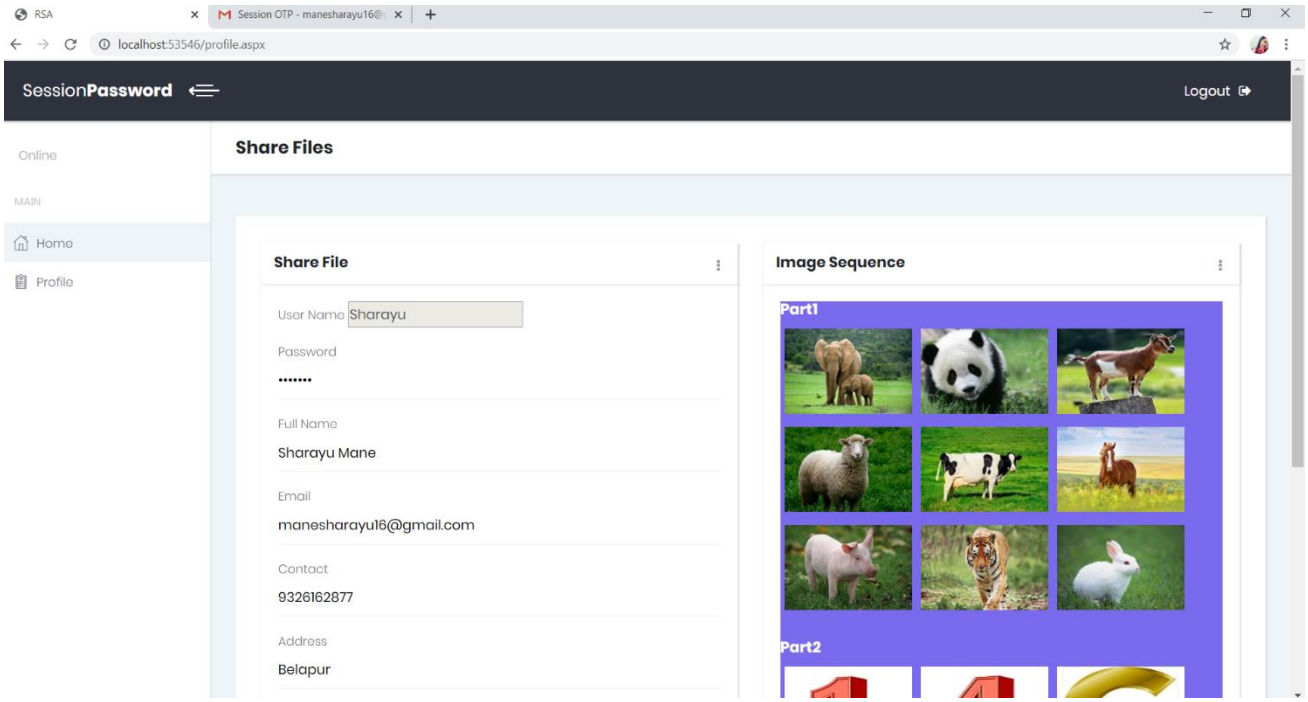

Registration
localhost:53546/registration.aspx
localhost:53546 says
Register succesfully
OK


Login
localhost:53546/login.aspx
User Name
Sharayu
Password
Please Select Part1 & Part2 First
95 + 25 =
120
YR928
Send OTP
OTP
Login
Reset
Forget Password?
Do not have an account? Signup
localhost:53546 says
Opt Send successfully Please check your Email Id
OK
Part2
Type here to search
ENG
13:13
16-03-2020


Login
Session OTP - manesharayu16@
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgxwHMPhrjbBZpDwLdhwrVTcZDfTl
Gmail
Search mail
Compose
Inbox 1,027
Starred
Snoozed
Sent
Drafts 23
More
Sharayu
1 of 1,491
Session OTP
Inbox ×
driemsproject@gmail.com
to me
1:13 PM (1 minute ago)
Hi Sharayu. Your Login OTP Is 2499
Reply
Forward


Login
Session OTP - manesharayu16@
localhost:53546/login.aspx?msg=logout
Security System Using Session Password
User Name
Sharayu
Password
Please Select Part1 & Part2 First
47 + 9 =
56
EJNVJ
Send OTP
OTP
2499
Login
Reset
Forget Password?
Do not have an account? Signup
Part2
3
4
X
5
1
A
7
M
G





APPLICATIONS : -

1. In corporate companies where user authentication is the main concern.
2. In Banks
3. In ATM Machine
4. In customised Software’s

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

Conclusion :

The existing techniques does not have that much capability to secure password from hackers or third party location .because in this techniques only one password is used for each and every session and password is transfer for authentications of users. So these passwords are easily hacked by hackers. We proposed a system called Session password ,in this it provides a new password for each session and need not to transfer password form server each time for authentication purpose that's why Session password scheme provides more security than the other existed systems.

Future scope:

Future scope of this technique is that , as it provides more security than the others existed systems more secure login of users is possible .so this technique is not just limited for PDA i.e. personal digital Assistant but also it is very useful for providing protection against Hacking, Dictionary attacks ,etc. In future it will be used for Banking Applications, Mobile phones applications where the security is more important. It also use with the 3D password technique for providing more and more security.

CHAPTER 8

REFERENCES AND BIBLIOGGRAPHY

CHAPTER 8

REFERENCES AND BIBLIOGRAPHY

.

[1] Imamah. "One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congruential Generator (LCG)." *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*. IEEE, 2018.

[2] Barkadehi, Mohammadreza Hazhirpasand, et al. "Authentication systems: A literature review and classification." *Telematics and Informatics* 35.5 (2018): 1491-1511.

[3] Venkatesh, Gotimukul, et al. "Application of session login and one time password in fund transfer system using RSA algorithm." *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*. Vol. 2. IEEE, 2017.

[4] Srivastava, Shubham, and M. Sivasankar. "On the generation of alphanumeric one time passwords." *2016 International Conference on Inventive Computation Technologies (ICICT)*. Vol. 1. IEEE, 2016.

[5] Sreelatha, M., et al. "Authentication schemes for session passwords using color and images." *International Journal of Network Security & Its Applications* 3.3 (2011): 111-119.

`

Evaluation sheet for Internal Assessment

Name of Student:……..

Name of Programme:…… Semester: Sixth

Course Title: Capstone Project :Execution and Report Writing **Code:22060.**

Title of Capstone Project:……

….……

A. PO's addressed by the Capstole Project

a) **An ability to apply computer science and engineering knowledge.**
b) **An understanding of professional and ethical responsibilities.**
c) **An ability to function as individual or as a group in diverse environment.**
d) **A knowledge of contemporary issues in computer science & engineering.**

B. CO's addressed by the Capstole Project

a). Ensure quality in product.

b). Assess the impact on project in real life.

c).Communicate effectively and confidently as a concern member of the team

d).Take appropriate decisions based on the collected information.

C. OTHER LEARNING OUTCOMES ACHIEVED THROUGH THIS PROJECT

1. Unit Outcomes

a). ……

b). …….

c)…..……..

d)……..

`

2.Practical Outcomes

a). ……

b). …….

c). ……..

d)……..

3.Affective Domain Outcomes

a). ……

b). …….

c). ……..

d)……..