Internship Report
on
THREE PHASE AUTHENTICATION

Submitted in partial fulfilment of the requirement for the award of the degree of

Internship

in

Computer Science and Engineering

By

Ruchi Sharma
(Uni Roll no: 2014447)

Under the supervision of
Dr Priya Matta
Associate Professor
Department of Computer Science & Engineering,
Graphic Era Deemed to be University

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GRAPHIC ERA DEEMED TO BE UNIVERSITY-248002
Jun-Jul 2021

ACKNOWLEDGEMENT

We are extremely thankful to our honourable President Sir, **Prof. (Dr.) Kamal Ghanshala** of **GRAPHIC ERA DEEMED TO BE UNIVERSITY** for providing all kind of educational and infrastructural support to work in this project, without which this project would not have been possible.

We hereby like to express our sincere gratitude and respect to our internship supervisor **Dr. Priya Matta** for her stimulating guidance and continuous supervision, monitoring, and constant encouragement throughout the project completion. The blessing, help, and guidance, given by him from time to time shall go a long way in the journey of life we are about to embark on.

We are obliged to our project team members for the valuable information provided by them in their respective fields. We are grateful for everyone's cooperation during the period of our project assignment.

Submitted By:

Ruchi Sharma

GraphicEra
Deemed to be University
Accredited by NAAC with Grade A
NBA Accredited Program in CSE, ECE & ME
Approved by AICTE, Ministry of HRD, Govt. of India

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the internship work entitled **THREE PHASE AUTHENTICATION** is a bonafide work carried out by Ruchi Sharma (Uni roll no:2014447) in partial fulfilment of the requirement for the award of summer internship of BTech IV Semester, Computer Science and Engineering, **Graphic Era Deemed to Be University**, Dehradun. This work is original work accomplished by the above-mentioned interns, and has been approved as it satisfies the academic requirements with respect to the work prescribed for the BTech IV Semester Internship.
The time duration for this internship was 15 June-31 July.

Sign of the Supervisor

Table of Figures

Table of Contents

1. INFORMATION SECURITY

Security basically means freedom from threats. Information Security is a set of processes that maintain the confidentiality, integrity and availability of data from malicious intentions. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, confidentiality, availability of information system resources (includes hardware, software, firmware, information/data and telecommunications).

Confidentiality, Integrity and Availability are sometimes referred to as the CIA Triad of Information Security.

1.1 Importance of Information Security

It is basically the practice to prevent unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be anything like your personal details, you profile on social media, your data in mobile phones or biometrics etc.

The most critical factor for protecting information assets and privacy is a great foundation for effective information security management.

Security management to meet these business requirements include:

The continued availability of their information system.

Preserve the confidentiality of sensitive data while stored.

Ensure the integrity of the information stored in the computer and in transit.

Ensure trust and obligation requirements in relation to any information relating to an identified or identifiable individual.

There is no doubt that a security violation can cost a lot to a company, whether in recovery from this event, or in the repair of public relations.

1.2 Some examples of Information Security

During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information.

With the beginning of Second World War formal alignment of Classification System was done.

Alan Turning was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

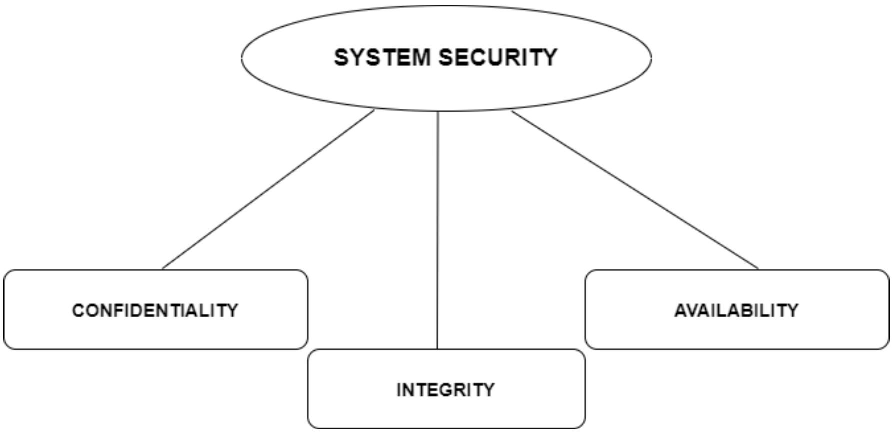


Figure 1. Triads of System Security

Confidentiality

When we say confidential, we mean that others should not understand except the parties involved in this transaction. If the third party sees our transaction or message the it means loss of privacy. So, we need to prevent unauthorized access and disclosure. Unauthorized access means nobody can access except the right entities who are involved in the transaction and disclosure means the message should not be open enough. In short, if the message is encrypted no one can see the message except the sender and the receiver. Therefore, confidentiality means we need to protect the data that is being transmitted. Encryption is one of the best way to protect to protect information as no one can see the data it is scrambled data that is seen which could not be understood by anyone except the person who has the key to decrypt the data. To, protect confidentiality, we need to define and enforce certain access levels for information. In some cases, separation of data was performed based on who can access the data and how important information is stored.

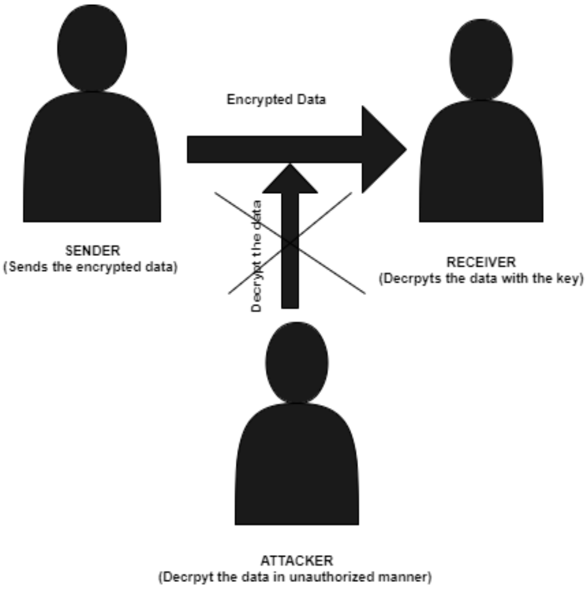

Encrypted Data
SENDER
(Sends the encrypted data)
Decrypt the data
RECEIVER
(Decrpyts the data with the key)
ATTACKER
(Decrpyt the data in unauthorized manner)

Figure 2. Process of confidentiality

Integrity

For understanding integrity we have a simple formula send=receive that is, whatever the sender is sending, the same message only the receiver should receive. For example, if you are performing a banking transaction of certain amount so the transaction should involve that particular amount you needed. What if the attacker modifies the amount thus increases it so not only the attacker modifies the amount but the destination address and the destination amount is given as the attacker's account, so this is the danger to the integrity. So, we don't want any modification messages by the unauthorized people. So, the transaction to the attacker's account should not be permitted by the system and the security system should be able to find out

that this is not the message that was sent by the sender. In other words, the security system should ensure that this is not transaction that was initiated by the sender.

So, integrity means we need to ensure that there is no modification of the message that is being transmitted. So, whatever the sender is sending that only the receiver should receive and if there is, any modifications that is been performed on the data, the system should find out that and it should discard that message. Integrity is one of the key terms of CIA triad.

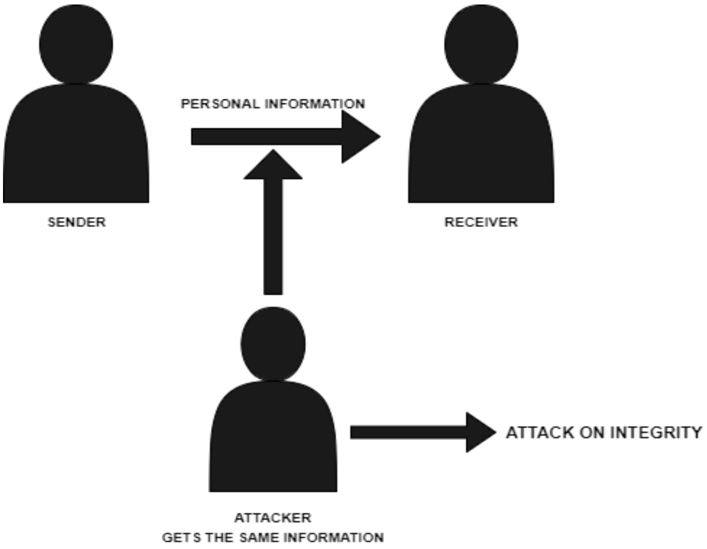


Figure 3. Process to maintain Integrity

Availability

It means we need to ensure the timely and reliable access to the system. For example, if you are hitting google.com, if you hit it at any time it will work because you trust that google server will always be available at the same time there will be many attacks that may be launched against google server but still google is very secured and it always provide its service to the customer or users who access it without any flaws so that's the power of a security system. Another example for understanding availability, imagine you have a bank account and you are expecting the banking server to respond you with the requested data. What if an attacker has launched an attack on the banking server and disrupted the service so when you access the banking server you are not getting the service that you are expecting and we do not want that because we except the service to provide service to us and this service should be timely and a reliable service. There will be attackers all over the internet and our security system is expected to provide security to the system and to the users and whenever any attack is launched on the server, we expect the server should withstand that attack and should still be able to provide access to the servers in the same way as it was in the perfect situation.

2. AUTHENTICATION

According to Authentication is the process or method in which the user is tested whether the user is the owner of that device or not. It is also the way of identifying or verifying the identity of the person. It involves validating the user using his/her credentials. It is an access control system means that user first has to authenticate or validate himself using his/her id, password to get access to the data or the system. Once the user is verified or authenticated, he/she has access to all the data or resource.

According to authentication is the process of validating the correct user whereas authorization is giving access to the validated user to use data or the resources. Authentication is the way of saving unethical access of any other user. It is a way of protecting the privacy of the user. Basically, authentication and privacy are dependent on each other more strong or accurate the authentication method is more the system or data is secured or privacy is protected.

Authentication is important because it helps an organisation or person to secure the data and it's resources from third party intrusion which is not authorized. Authentication is important to get access to computer systems, networks, databases, websites and other network-based applications or services. Authentication method needs to be efficient and secure so as to save the unauthorized access of any intruder.

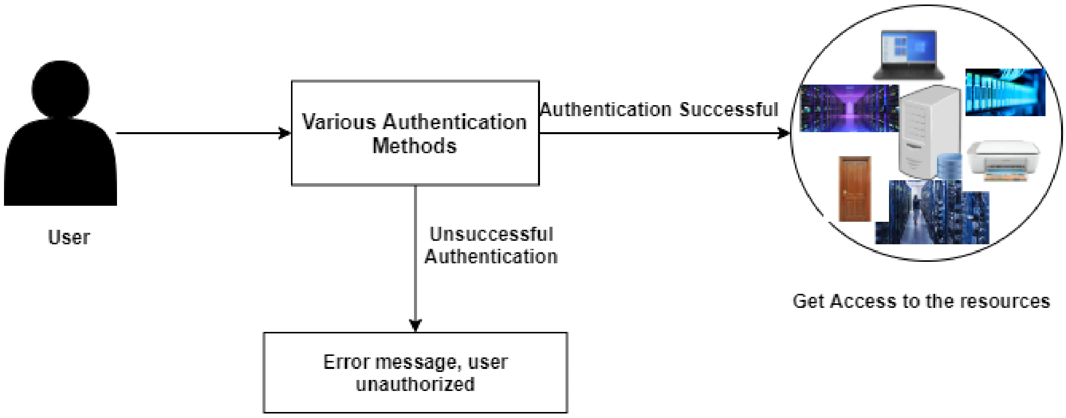

User
Various Authentication Methods
Authentication Successful
Unsuccessful Authentication
Error message, user unauthorized
Get Access to the resources

Figure 4. Importance of Authentication

2.1Types of Authentications:

➢ Biometric Based Authentication:

Biometric Authentication is the authentication method that relies on user unique biological characteristics. It includes Facial recognition, Fingerprint scanners, voice identification and eye scanners.

It includes measuring unique individual characteristics such as the retina, the iris fingerprints, face or even the voice. Biometric ease the way of authentication user need not to remember the password or the user need not to carry the card or any token with himself to get access to the data or the resource. Moreover, there are very less chance for anyone to replicate the unique individual characteristics such as retina, the iris or any other characteristics. Thus, we can say that biometric authentication is the most secure authentication method.

On the other side it is quite expensive as it includes scanning techniques. So, it might not be convenient and affordable to everyone and each company to adopt this method.

➢ Token Based Authentication:

[5] Token is a material chip which is used to get the access resources and the data. For example, it includes dongle, card or RFID chip. It is basically two factor authentication method as after using card we need to input pin or OTP to get access to the resource.

But it is tedious task to take that token everywhere to get access to the resources. If the token is lost, stolen or forgotten in any circumstance you won't be able to access the resource.

➢ Knowledge based Authentication (KBA):

It is also known as password authentication. It is the method that provides the authenticity to the user by using PIN (Personal Identification Number), password or any pattern. In this method the user needs to enter username and the password to get access. It is of two types: -

- Static KBA
- Dynamic KBA

Static KBA and Dynamic KBA:

Static KBA is a shared set of pre-determined questions and answers. In this category, the end user selects a set of questions and their appropriate answers prior to the authentication process. Alternatively, they conclude that it can be grounded on previously known answers to a set of correlated questions. The user is challenged with the inter-related questions for a given period of time. These questions of static KBA may be a very well-

known and easy to acquire fact, like user's first mobile number, mother's maiden name, pet's name etc. Static KBA may also include a strong password, PIN, or some confidential information as an answer to these questions.

Although it is very easy to implement to Static KBA, but the answers to the questions are easily available on the internet via the social network.

Dynamic KBA, takes the question-and-answer scheme one step further. In this category, questions are not selected in advance but generated dynamically consuming the information from different data sources. Dynamic KBA is a tougher scheme to implement, and it is also a time-consuming task. But the appealing fact with dynamic KBA is that it is difficult to

break and therefore more fraud resistant.

i. Single Factor Authentication:

It basically includes the one-way authentication. For example, user can authenticate using PIN, password, OTP or any of the method. It is not much secured because hacker can easily guess or hack the password and can get authorized to the data and the resources.

ii. Multiple Factor Authentication:

It includes more than one step to get access to the system. In this the user has to undergo multiple authentication major to get access to the data. [5] Suppose we have entered the password to get access than we have to get the Pin or OTP to get access to the device else the user will not be authenticated. It is useful for banking and email purpose. It is the secured way to access. It is affordable as it includes no scannable devices. So, it can be easily implemented. It has some drawbacks such has if the phone got lost than it will be difficult for the user to authenticate.

Token Based Authentication is less useful as its whole process depends only on the token if the token is damage, misplaced or stolen, then the person has to register once again because he won't be able to authorize without using the token. Biometric Based Authentication is although the most secured method but it is quite expensive. Every organisation or a person may not be able to afford the devices used for biometric authentication. Password are easy to guess or hack by the hacker.

Hence, Knowledge Based Authentication is the best authentication method on which work can be done so as to improve the security. Knowledge Based Authentication includes the password, PIN, pattern used to authorize. Knowledge Based Authentication with Two Factor Authentication can be a secured way for authentication.

3. PUBLISHED SCHEMES

3.1 The Enhanced Graphic Pattern Authentication Scheme

This paper proposes a new graphic pattern authentication mechanism to enhance the strength of that in the keypad lock screen Apps. It integrates random digital graphics and handwriting graphic input track recognition technologies to provide better and more diverse privacy protection and reduce the risk of vulnerability. The proposed mechanism is based on two factor identification schemes. First of all, it randomly changes digital graphic position based on unique passwords every time to increase the difficulty of the stealer's recording. Second, the input track of handwriting graphics is another identification factor for enhancing the complex strength of user authentication as well. This paper proposes a new graphic pattern authentication mechanism to enhance the strength of authentication in the keypad lock screen Apps. For validating the proposal, it also provides a proof software App implementation.

Such user identification technology is vulnerable to piracy, which leads to the outflow of personal information. The common methods of preventing crimes are to increase the length and complexity of digital passwords or to change passwords or password graphics regularly to prevent crimes. However, in essence, the problem has not been completely solved. To increase security, the biometric authentication mechanism such as fingerprint or face recognition on the mobile phone is used as the identification input data, which is safer than the password input method. However, the input of these mechanisms is not impossible to copy. Therefore, the security of a fingerprint or face as a password input still has challenges. If it can be combined with other security mechanisms, it will enhance the privacy protection of users.

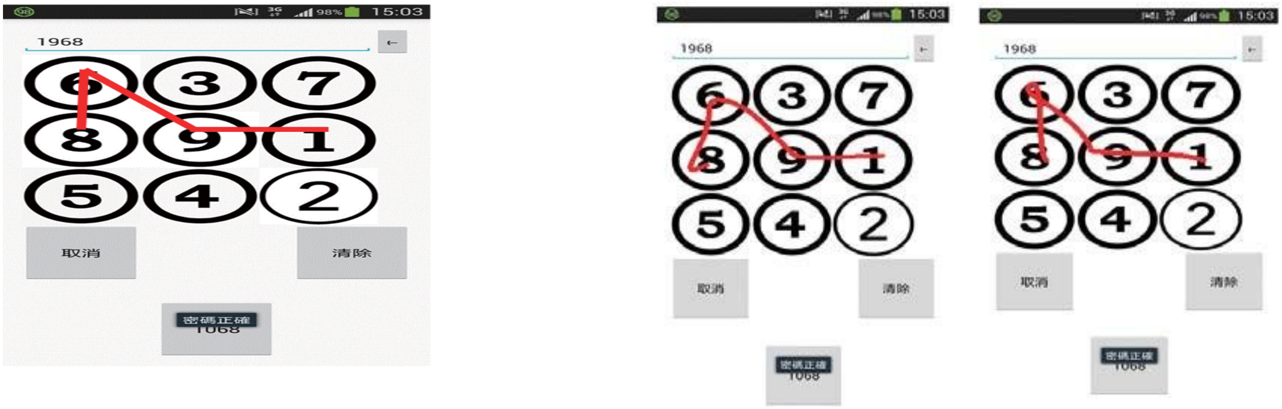


Figure 5. Enhanced Graphic Pattern scheme

3.2 Graphical Password Authentication Using Cued Click Point Technique

Cued Click Point (CCP) is a method under cued recall-based. In this method, the user will click on any point of the image for each image that chose and then capture the specific part pixel's value will bring to point x and y. A click point is used on five different images. The user could fast create and re-enter their watchword and very precise when entering their click point on the image and hard to guess by an attacker due to having a large set of images. This project proposed to implement the CCP technique in graphical password authentication to overcome the user's problems and thus increase the data security of the user's password. Therefore, a password will be more protected with the increasing number of the image where give workloads to attacker especially shoulder surfing. The implementation of Cued Click Point technique in graphical password based will be effective in making user use more friendly and the data user is more secure instead of only using the text base form.

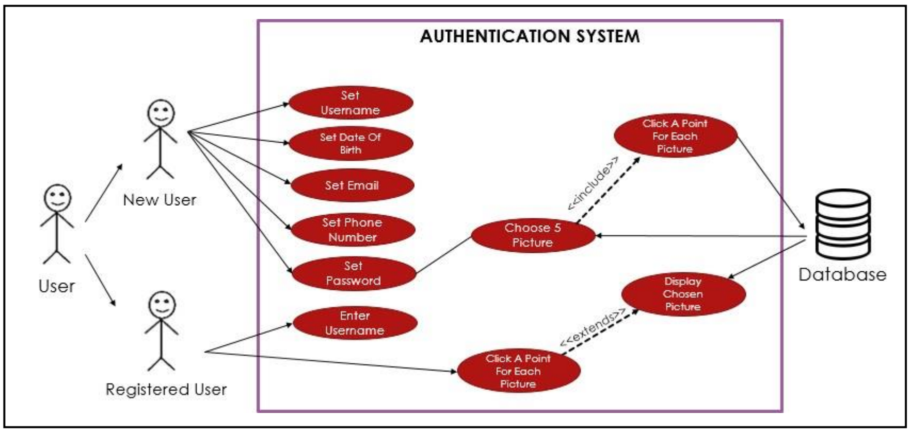


Figure 6. Cued Click Point Authentication

3.3 Implementation of Captcha as Graphical Passwords for Multi Security

Using hard Artificial Intelligence is a problem for security, Captcha, creates a new paradigm which differentiates human users from computers (bots) (von Ahm, Blum, Hopper, & Langford, 2003) i.e., through the use of a puzzle, which bots cannot identify but a human user can. This Captcha is mainly used to provide internet security for email from bots. But this has not gotten much success with cryptographic primitives based on hard mathematical problems.

CaRP is a click-based graphical password, where a sequence of random clicks on an image is used to derive a password, and the images generated by CaRP are a challenge and a new image is generated for every login attempt. Users are asked to click on the image or any part of that image as a password and these points or images are then stored as a graphical password. These images are different for every user. The newly generated graphical password is used along with the regular user password. CaRP can be used to prevent relay attacks where Captcha challenges were meant to be solved by humans. CaRP also can prevent shoulder surfing attacks if it is combined with dual- view technologies.

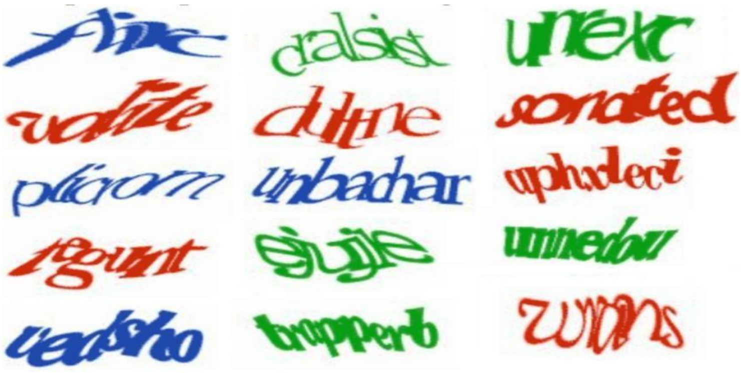


Figure 7. Captcha as graphical password

3.4 THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN- Based IoT Network

In this article, new graphical authentication scheme, which can prevent a variety of attacks, while ensuring the usability (i.e., users are not required to remember a complicated password and there is no need for extra devices for their authentication). The solution consists of two phases: 1) the registration phase and 2) the authentication phase. In the first phase, the user should choose the pattern, including his login password (a graph) and the image area. In the authentication phase, the user will obtain a 2-digit challenge value through the pattern. The authentication can be obtained if and only if the challenge value is correctly matched with the image area. This method prevents many types of attacks, including shoulder-surfing, smudge, and recording screen, since the system passes the challenge value implicitly and randomly.

Furthermore, it conducts three experiments, i.e., security experiment, usability experiment, and chronicity experiment to evaluate the performance of our proposed scheme.

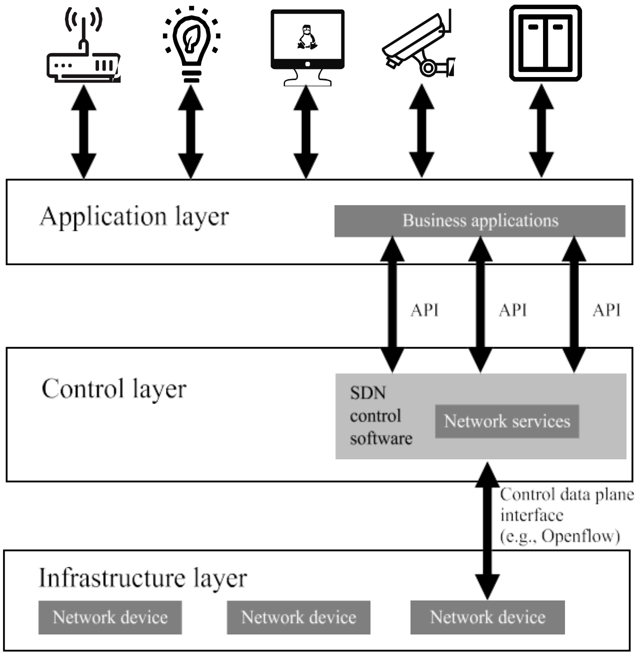


Figure 8. Structure of SDN Network

3.5 Video Captcha as a Graphical Password

Video CAPTCHAs are one more technique within the CAPTCHA system. Here during this methodology, a video is Provided to the user throughout linguistic communication up method. There will be few queries displayed for user to answer based on the video. If the answers match to the answers holds on within the

info user signs up successfully. This paper explains construct of victimization CAPTCHA as graphical passwords. Security primitives because of that it becomes necessary to develop systems like graphical passwords which square measure exhausting to crack and square measure safer than the traditional passwords. However, this technique prevents attacks made by bots. CAPTCHA plays vital role in World Wide net security wherever it prevents larva programs and Hackers from abusing on-line services. This paper has conferred ideas and history of CAPTCHAs, and mentioned their applications. Hence, we have gotintroduced Associate in Nursing new click based mostly video captcha that resolves all the weakness of the opposite existing captcha and makes the system or net world free from larva attack.

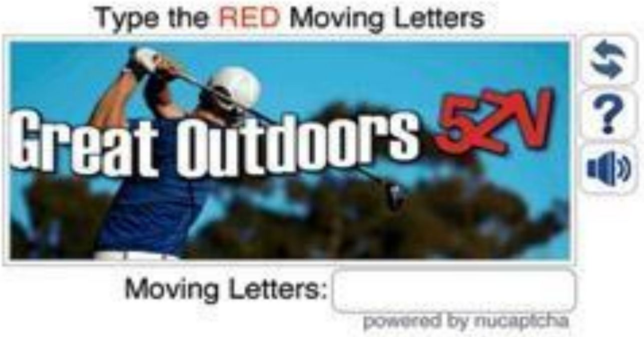


Figure 9. Video Captcha

3.6 A Graphic-based Cryptographic Model for Authentication

The password for each login session changes, thereby, enhancing the security of GBCM, which consequently make it resistant to all possible attacks on graphical password schemes. It was observed that the login time of the users that register with GBCM reduced at their second login session, which infers that with continuous use, users become more acquainted with the log in technique. The results produced from the comparative analysis done with an existing model show that GBCM is more user-friendly and secure.

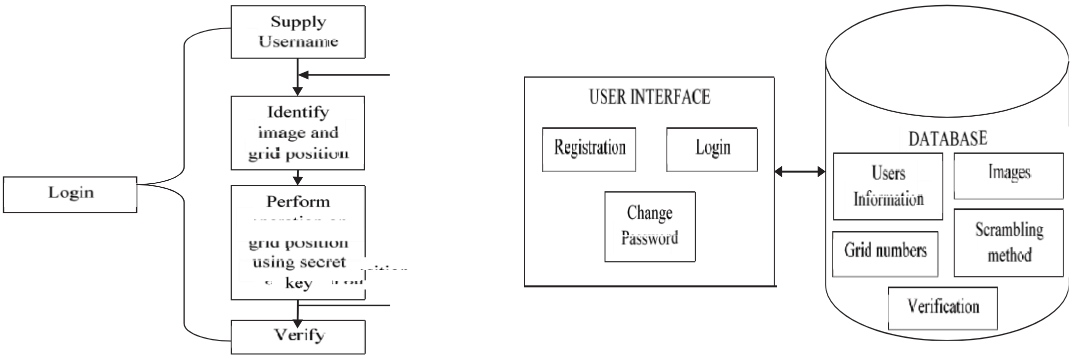
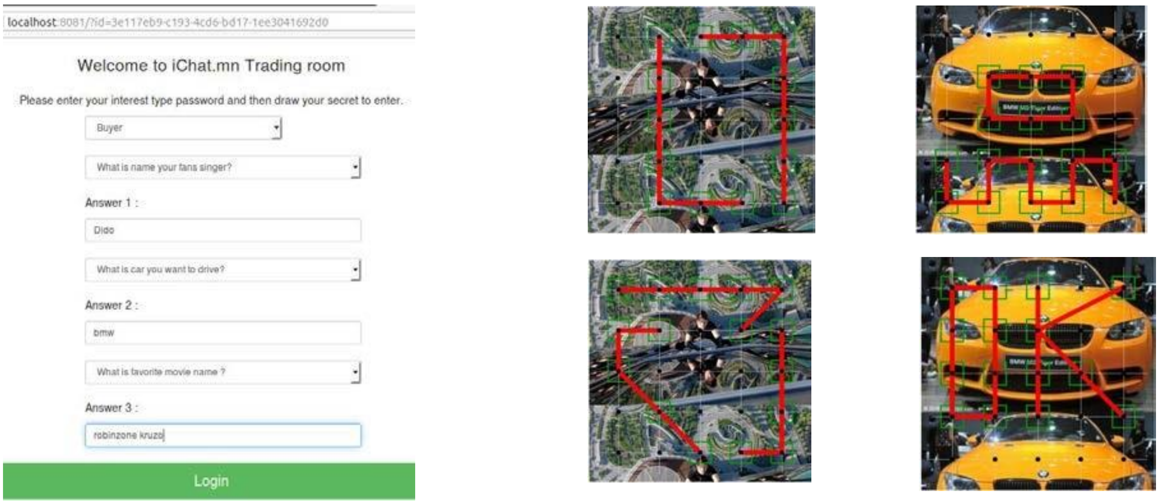


Figure 10. Architecture of Graphic based cryptographic model

3.7 New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation

QBP scheme can be protected from various attacks since there is no any personal information about the users on the website. While (designing and generating) the scheme, we established a new graphical password scheme, which is easy to use, interesting and strong, integrated by adding both BDAS based on recall and Pass-Go graphical password scheme to password like traditional text-based having secret questions and answers. For QBP scheme, there are 25 points on the 5x5 board and user connects points and draws optional image on free position using straight line. It is possible to mark 8 directions freely by striking at least more than 4 points. Draw path from start point to end point will be numbered 1 to 25. When reproduce, user need to select point drawn in previous step correctly and draw to end point by recall previous imagination.



localhost:8081/?id=3e117eb9-c193-4cd6-bd17-1ee3041692d0

Welcome to iChat.mn Trading room

Please enter your interest type password and then draw your secret to enter.

Buyer

What is name your fans singer?

Answer 1 :

Dido

What is car you want to drive?

Answer 2 :

bmw

What is favorite movie name ?

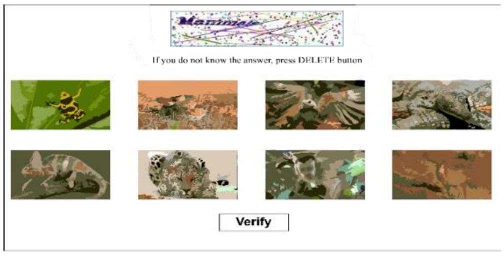
Answer 3 :

robinzone kruzo

Figure 11. Password Scheme containing Questions Background pattern

3.8 A Cued-Recall and Emotion Classification Graphical Password Authentication Scheme

This is a two-layer graphical password scheme. This method employs a Captcha and Recognition-Based Image Layer, and an Emotional and Cued-Recall Image Layer. These layers rely on the user's natural cognitive abilities. As user gets different independent challenge images for the first and second authentication layers, this scheme is robust to dictionary, rely and brute-force attacks. The cracking probability is lower for a larger number of possible showed images on layer 1, and for images with larger amount of sub rectangles and required clicks on layer 2. The system also counts with bot prevention using the shutdown event for more than one authentication failure attempt on layer 1 and 2.



If you do not know the answer, press DELETE button

Figure 12. Authentication layer with images of animals as subject.

3.9 Captcha as Graphical Passwords—A New Security Primitive Based On Hard AI Problems

In this scheme a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which is known as Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-
view technologies, shoulder-surfing attacks.
CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
CaRP also offers protection against relay attacks, an increasing threat to bypass Captcha's protection.

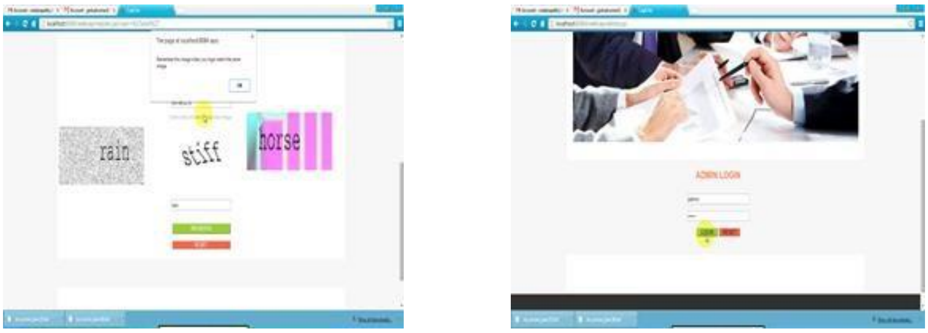
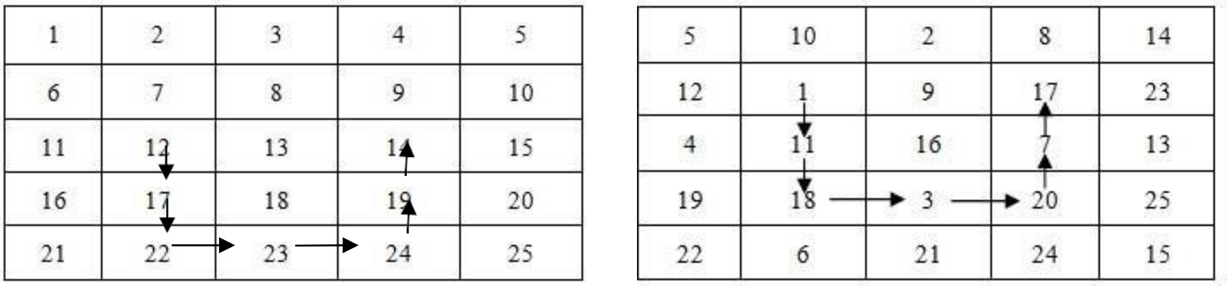


Figure 13. Captcha as graphical password

3.10 Secure Pattern-Key Based Password Authentication Scheme

The proposed pattern-key based password authentication scheme provides high level of security, as mention above the complexity of guessing only key is very high inspite of the inclusion of pattern and dummy complexities. Due to high complexity, it minimizes the brute-force attack, shoulder surfing attack etc. This scheme does not overload human memory. It provides more usability in many webs application and provides security against anonymous users. The advantage of this scheme is that user just needs to remember key values same as he remembers its password and also recognize the pattern during registration phase. During login phase, user needs to recall the pattern and map the key values. It is found that the proposed scheme is more secure than the existing similar schemes as the complexity of the proposed scheme is very high and thus it is resistant to all types of possible attacks.



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

5	10	2	8	14
12	1	9	17	23
4	11	16	7	13
19	18	3	20	25
22	6	21	24	15

Figure 14. Key based authentication

Table I: Brief about proposed Schemes

Name	By Whom	When	About Scheme	Pros	Cons
Secure Pattern-Key Based Password Authentication Scheme	M Hamza Zaki, Adil Husain, M Sarosh Umar, Muneeb H Khan	2017	In this scheme, user will not draw a pattern on screen instead he enters the location number of pattern and recognizes the pattern.	It is the highly secured as it is contain key value of every character.	It is complex for the user to guess and remember the key value.
New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation	Bulganmaa Togookhuu and Junxing Zhang	2017	In thus authentication method first it consist of some general question and the we have to draw pattern joining some points to get access.	It is easy to use and created password consisted of strong entropy bit.	After some attempts the hacker can easily guess the password.
A Cued-Recall and Emotion Classification Graphical Password Authentication Scheme	Danilo E. Vieira, Tonny L. Mesquita Abreu, Max E. Vizcarra Melgar, Luz A. M. Santander	2017	It is a two-layer graphical password scheme. This method employs a Captcha and an Emotional and Cued-Recall Image Layer.	Consumes less time for authentication.	First phase of authentication that is captcha is easy to guess it means it is not 100% secure as it's first phase can be passed easily.
Captcha As Graphical Passwords—A New Security Primitive Based On Hard AI	Silla Nirosha and Mr. Urlam Sridhar	2017	In this scheme a new security primitive based on hard AI problems. CaRP is both a Captcha and a graphical password scheme.	CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks.	It is not convenient way because it is not user friendly, hard to understand.
Implementation of Captcha as Graphical Passwords for Milti Security	Babu Rajeev Maddipati	2018	Mainly to provide internet security for email from bots using CaRP which is a click based graphical password.	The ease of CaRP by utilizing images of various levels therefore	Confusing for user with numerous authentication process.

				easy to remember.	
Video Captcha as Graphical password	Pooja Kute, Tejaswini Lokhande, Manasi Kanadi, Sayali Kashid, Rushira Deshmukh	2018	Proposed a graphical Captcha where a vidio is displayed and few questions related to it is answered by the user.	Avoid OCR attacks and prevent system from bots.	User Complexity.
A Graphic-based Cryptographic Model for Authentication	Boniface K. Alese, Abimbola Akindele, Folasade M.Dahunsi, Aderonke F. Thompson, Tosin Adesuyi	2019	It is an authentication method which has three phase for authentication and every time when user log out the order or password shuffle.	GBCM is more user-friendly and secure.	Initially is time consuming.
The Enhanced Graphic Pattern Authentication Scheme	Sung Shiou Shen, Che-Tzu Change, Shen-Ho Lin, Wei Chien	2019	Screen Unlock map input track	Focuses on trajectory identification.	Other user can easily recognize the password as numbers are not shuffled when second time you enter password.
THP: A novel Authentication Scheme to prevent multiple attacks in SDN- Based IoT network	Liming Fang, Yang Li, Xinyu Yun, Zhenyu Wen, Shouling Ji	2020	New security login authentication based on both graphical password and text. Challenge value for an SDN-based IoT network.	Prevent multiple attacks.	Difficult for user to remember
Graphical Password Authentication using Cued Click point technique	Nor Azida Binti Mohd Fazli	2021	Creating password with use of both pictures and text by cued click point technique on pictures.	A secured way and difficult to crack.	Difficult for user to remember the points on pictures where he clicked.

4. PROPOSED SCHEME: THREE PHASE AUTHENTICATION

Authentication is important topic nowadays. Threats to privacy are increasing day by day. So, we decided to make authentication method more secure. Three phase authentications will have the highest security.

We have read about many research papers and were able to know that authentication needs to be more secured and different authentication method.

Our Scheme has three phase authentication which is the most secure way of authentication. In this user need to enter password based on mouse click. Reducing key tracking attack. At first user need to enter password by clicking Devanagari letters. After that there will be shuffled alphabetical password which shuffle on each click which make it hard for the third person to know. Hacker will not be able to guess the password because in second phase the alphabet shuffle on every click. Our third phase will be OTP that will be sent on user mail ID set at the time of registration.

These three phases make our authentication more secure. Our authentication method reduces the chances of key tracking and various unauthorised access. Our code work for multi user login. If the user is new, he/she needs to enter his/her details to register. His/her data will be stored in database so that they can login to the site.

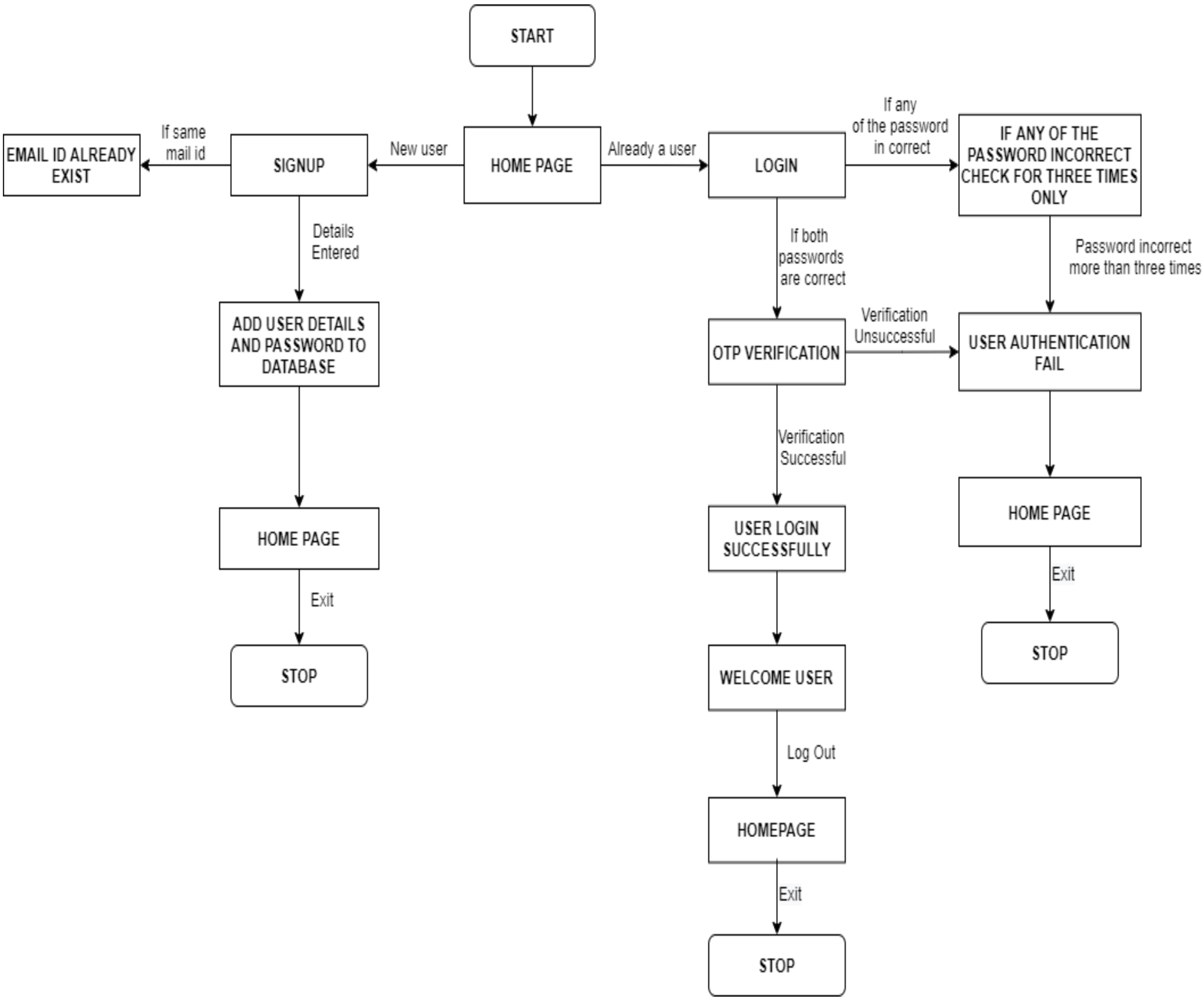
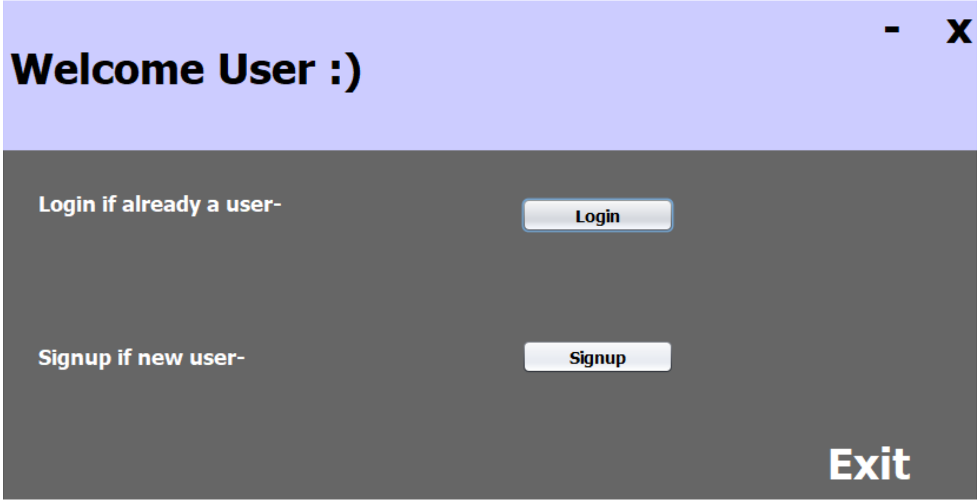


Figure 15. Brief of our Scheme through flowchart

Figure 15 gives us the brief about the working of our scheme.
Starts with the home page. If already a user, then go for login if not a user goes for sign up. For login successfully user need to enter both passwords correctly that is Devanagari and the English password. If entered correctly go for OTP verification step and after verifying OTP we successfully login into the page. Welcome user page opens. Then if he/she log out they reach to the home page.
If user enter any of the one password wrong, they get three chances to enter password and if still the password is wrong then their authentication is failed. Home page will open of login signup.
If the user is new, he/she will go for signing up and enter his/her details with two passwords.
If while sign up we enter any username or Gmail id which has been already used then it will display the message that username or mail id already exists.

5. PROPOSED DESIGN

This is first is the home page of our three-phase authentication system.
User will be given two choices- if the user has already signed up before he/she will login now and the person who is visiting the page for the first time has to sign up by entering his/her details and password.



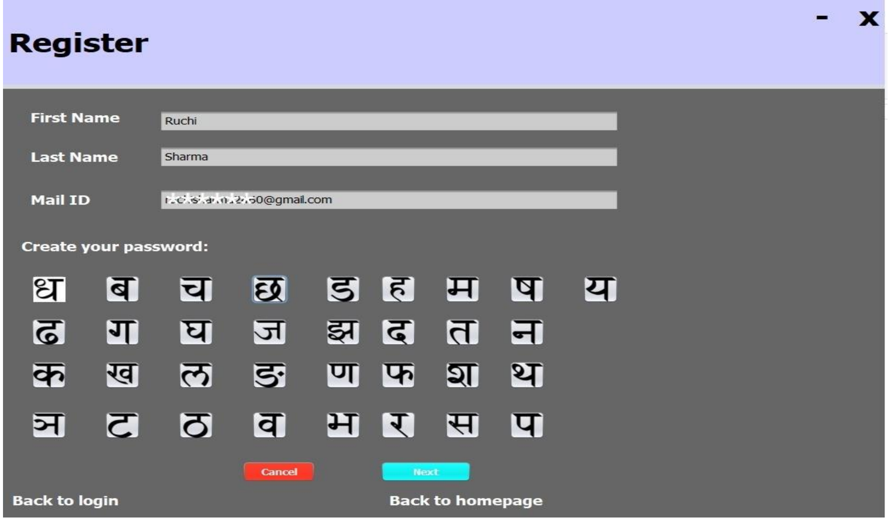
Welcome User :)

Login if already a user-

Signup if new user-

Figure 16. Home Page

The picture below shows the registration form which appears after the home page. While singing up this is the first phase of our three-phase authentication system. For signing up user need to enter his first name, then his last name, then his mail id where he or she will receive the OTP in the third face of authentication.
The first time the user enters the password is in Devanagari form, that means for sign up the first password will be the Hindi password entered by the user by clicking the Hindi letter and it could be of any length. After entering the password and details we click on next.



Register

First Name: Ruchi

Last Name: Sharma

Mail ID: [redacted]0@gmail.com

Create your password:

Figure 17. Registration form with first password

The second phase of the authentication is shown below. The user after saving his/her Devanagari (Hindi) password now enters a password in English. When the user clicks on one letter all the alphabets get shuffled, the password entered could be of any length. After every click all the letters get shuffled. It will be very difficult for the attacker to recognize the password in shuffled letters.

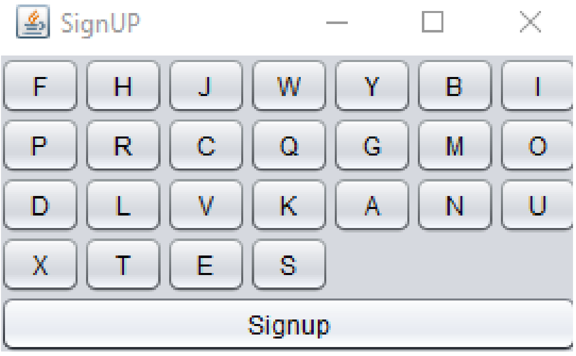
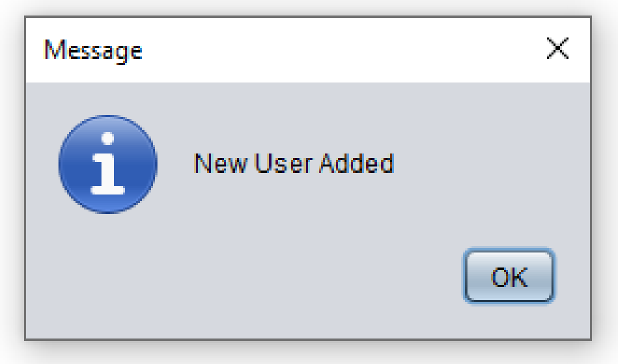


Figure 18. The Second password

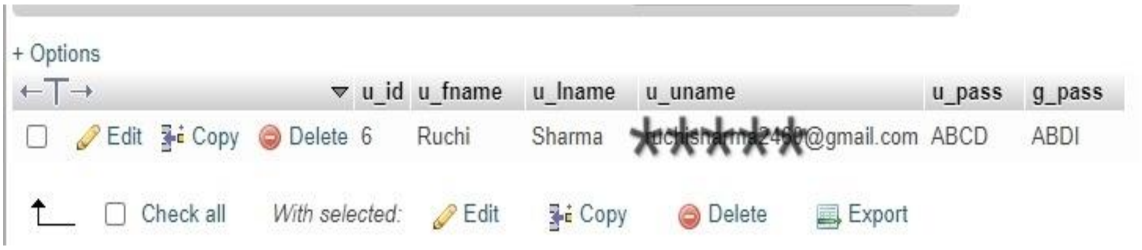
As soon as the second phase of authentication is completed and user enters the two passwords successfully the user's name will be added. And after the second password entered successfully this message will be displayed which shows new user added.



Message

New User Added

Figure 19. New User Added to the list of users

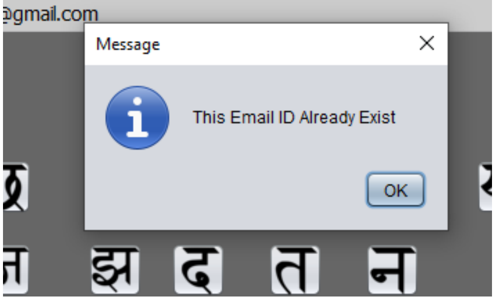


+ Options

	u_id	u_fname	u_lname	u_uname	u_pass	g_pass
☐ Edit Copy Delete	6	Ruchi	Sharma	[redacted]@gmail.com	ABCD	ABDI

Figure 20. Database

While signing up user needs to enter unique email id if Email ID already exist error message will be popup on the window.



Message

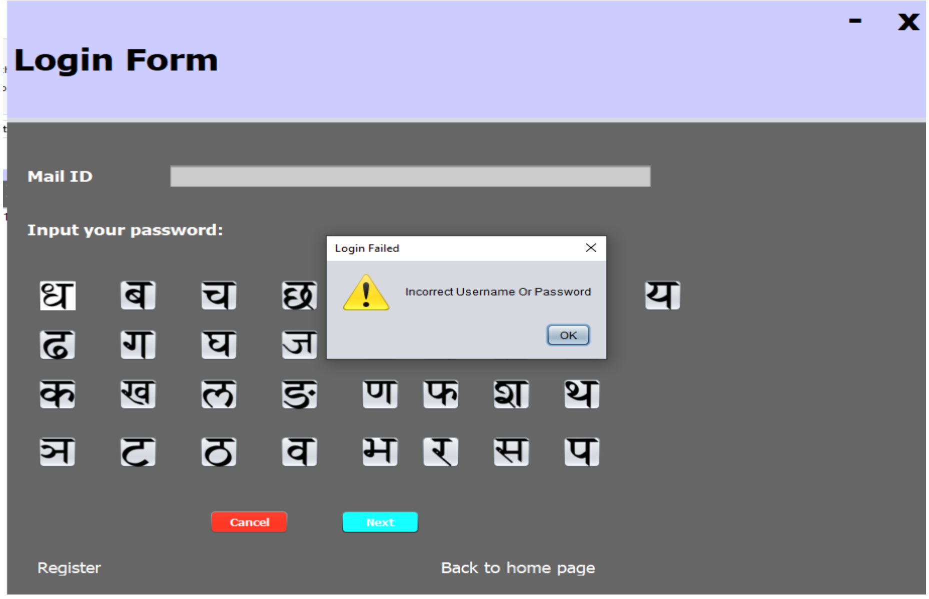
This Email ID Already Exist

Figure 21. Message Popped

Now, again user open form to login in the form as the user has already signed up as a new user. So, now user click on login instead of signup and then our three-phase authentication starts.

The first phase, enter the Devanagari password user has setup while signing up. Firstly, enter your mail id which you have used while signing up.

For a while if you forget the password and you enter the wrong password this will be the message displayed on the screen which says incorrect username or password.



Login Form

Mail ID

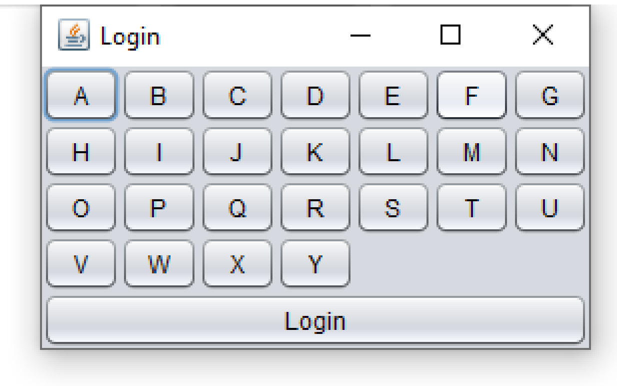
Input your password:

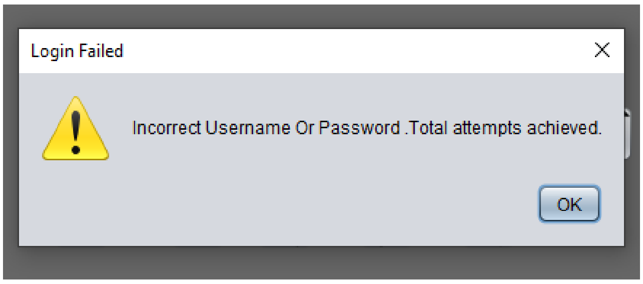
Login Failed

Incorrect Username Or Password

Figure 22. Login Form

If user enter correct password and user name, he/she enters second phase of authentication that is alphabetical password. It will be most secured way of authentication as alphabet shuffle on each click.
If the user enter password wrong more than three times error message will be shown up. And then home page will open.

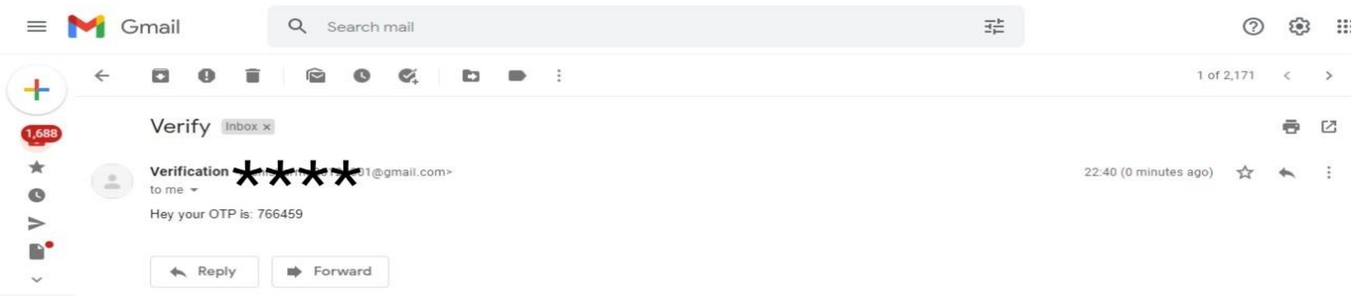



Login Failed

Incorrect Username Or Password .Total attempts achieved.

Figure 23. Alphabetical Password **Figure 24. Error Message**

After successful login. This is the third verification phase, OTP Verification.
In this we are checking if the person who logged in is a genuine user or not.
When user reach this phase of authentication user will receive an OTP in his/her mail id which he/she has to enter here to successfully login to the page.



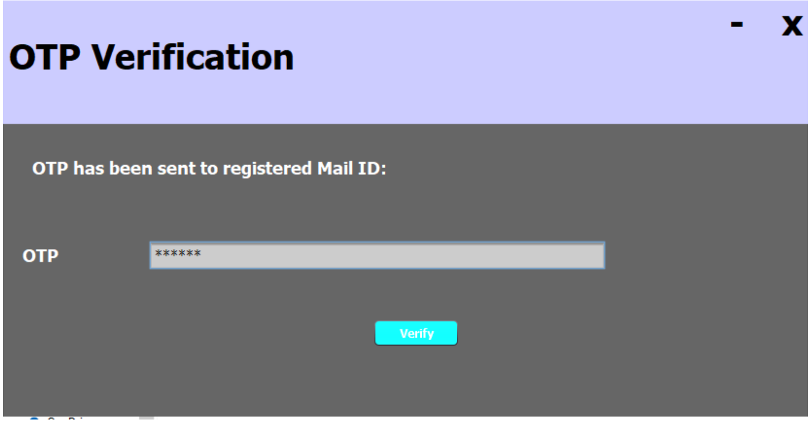
Verify Inbox ×

Verification [redacted]
to me

22:40 (0 minutes ago)

Hey your OTP is: 766459

Figure 25. OTP sent on Email ID

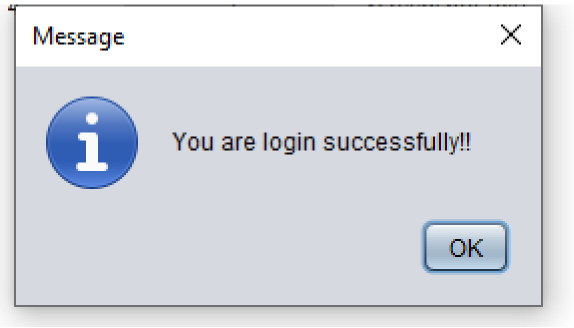

OTP Verification

OTP has been sent to registered Mail ID:

OTP ******

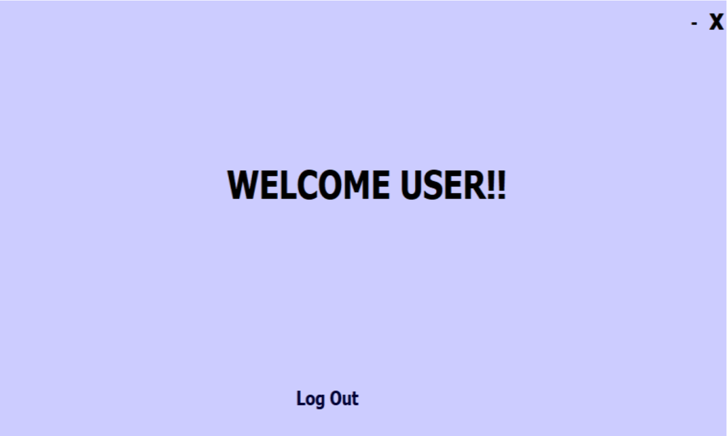
Figure 26. OTP Verification

If user verified successfully welcome user page opens and after logging out home page opens.



You are login successfully!!

Figure 27. Login Successful



WELCOME USER!!

Figure 28. Welcome User Page

6. REFERENCES

1. Wikipedia online https://en.wikipedia.org/wiki/Authentication

2. TechTaget online https://searchsecurity.techtarget.com/definition/authentication

3. Okta Authentication vs Authorization https://www.okta.com/identity-101/authentication-vs-authorization/

4. ID R&D Authentication methods https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/

5.Alliance Technology Partners Authentication Methods https://www.alliancetechpartners.com/network-security-authentication/

6. A review of Authentication INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH by Nilesh A. Lal, Salendra Prasad, Mohammed Farik

7. TCpC: a graphical password scheme ensuring authentication for IoT resources by Priya Matta and Bhasker Pant

8. Okta Different methods of authentication https://www.okta.com/blog/2019/02/the-ultimate-authentication-playbook/

9. The Enhanced Graphic Pattern Authentication Scheme Via Handwriting identification by Sung-Shiou Shen, Che-Tzu Chang, Shen-Ho Lin, Wei Chien

10. Graphical Password Authentication Using Cued Click Point Technique by Nor Azida Binti Mohd Fazli

11. Implementation of Captcha as Graphical Passwords For Multi Security by Babu Rajeev Maddipati

12. A New Security Captcha As Graphical Passwords On Hard AI Problems by M.Sneha Divya, Mr.P.Joshua Raju

13. Video Captcha as a Graphical Password by Pooja Kute, Tejaswini Lokhande, Manasi Kanadi, Sayali Kashid, Ruchira Deshmukh

14. A Graphic-based Cryptographic Model for Authentication by Boniface K. Alese, Abimbola Akindele, Folasade M.Dahunsi, Aderonke F. Thompson, Tosin Adesuyi

15. New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation by Bulganmaa Togookhuu and Junxing Zhang

16. A Cued-Recall and Emotion Classification Graphical Password Authentication Scheme by Danilo E. Vieira, Tonny L. Mesquita Abreu, Max E. Vizcarra Melgar, Luz A. M. Santander

17. Captcha As Graphical Passwords—A New Security Primitive Based On Hard AI Problems Silla Nirosha and Mr. Urlam Sridhar

18. Secure Pattern-Key Based Password Authentication Scheme by M Hamza Zaki, Adil Husain, M Sarosh Umar, Muneeb H Khan

7. APPENDICES

Java Code for shuffling buttons in second step of authentication

```
public void SetPassword() {
        if (buttons != null) {
            Collections.shuffle(Arrays.asList(buttons));
            layoutButtons();
        }
    }
 public void layoutButtons() {
        gridPanel.removeAll();
        for (JButton button : buttons) {
            gridPanel.add(button);
        }
        gridPanel.revalidate();
        gridPanel.repaint();
    }
 private JButton[] getButtons(int size) {
        JButton[] buttons = new JButton[size];
        for (int i = 0; i < size; i++) {
            int z=i+65;
            char j=(char)z;
            final JButton button = new JButton(""+j+"");
            button.addActionListener(new ActionListener(){
                public void actionPerformed(ActionEvent e) {
                    SetPassword();
                    pass=pass+button.getText();
                    System.out.println("Button " + button.getText() + " pressed");
                }
            });
            buttons[i] = button;
        }
        return buttons;
    }
```

Java code for generation of OTP through mail in third step of authentication

```
String smtp_host = "smtp.gmail.com";
              String from_userName = "abcdef @gmail.com";
              String from_passWord = "rama4776";
              String show_name = "Verification";
          String recipients=uname;
```

```
 String sendSubject="Verify";
  Random rand = new Random();
   OTP=rand.nextInt(999999);

   String sendText = "Hey your OTP is: "+OTP;

try {
                        Properties props = System.getProperties();
                        props.put("mail.smtp.starttls.enable", "true");
                        props.put("mail.smtp.host", smtp_host);
                        props.put("mail.smtp.user", from_userName);
                        props.put("mail.smtp.password", from_passWord);
                        props.setProperty("mail.smtp.socketFactory.class", "javax.net.ssl.SSLSocketFactory");
                        props.setProperty("mail.smtp.socketFactory.fallback", "false");
                        props.setProperty("mail.smtp.port", "465");
                        props.setProperty("mail.smtp.socketFactory.port", "465");
                        props.put("mail.smtp.auth", "true");
                        Session session = Session.getDefaultInstance(props, null);
                        session.setDebug(false);
                        MimeMessage message = new MimeMessage(session);
                        message.setFrom(new InternetAddress(from_userName));
                        message.addRecipient(Message.RecipientType.TO, new InternetAddress(recipients));
                        message.setFrom(new InternetAddress(show_name + "<" + from_userName + ">"));
                        message.setSubject(sendSubject);
                        message.setContent(sendText, "text/html;charset=utf-8");
                        Transport transport = session.getTransport("smtp");
                        transport.connect(smtp_host, from_userName, from_passWord);
                        transport.sendMessage(message, message.getAllRecipients());
                        transport.close();
           new OTPForm(OTP).setVisible(true);
           OTPForm otp  = new OTPForm(OTP);

otp.pack();
otp.setLocationRelativeTo(null);
otp.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
frame.dispose();
              }
catch (Exception ex) {
                        ex.printStackTrace();
                        System.out.println("failure! ");
           frame.dispose();
```