# Enhance Security for Authentication

**Ankush S, Vinayprasad M S**

***Abstract:*** ***An enhanced security for authentication is defined because it is vital that authentication is an extremely important crucial robust process for each user to access any of the applications. Magnificent growth and usage of the internet raise agitate about the way to communicate, protect data and sensitive information safely. In today's world hackers use differing types of attacks in order to acquire valuable information. Many of the attacks are primarily used to get into an application to steal the credentials followed by internal information of the users. The first thing of security is defined in three terms. i.e., confidentiality, integrity and availability. Confidentiality can protect information from unauthorized access and exploiting of sensitive data. Integrity measures protect information from unauthorized alteration. Whereas availability so as for a data system to be useful it must be available to authorized users. The most objective of this paper is to supply information about confidentiality in terms of multifactor authentication. Confidentiality plays a serious role in terms of authentication. Authentication is the process of proving or showing to be true. This includes confidentiality and integrity. The improved security for authentication is additionally known for multifactor authentication for the users. This multifactor authentication is implemented for an android application using a visual-picture login technique to access the an application.***

***Keywords:*** ***Multifactor authentication (MFA), One-time-password(OTP), Visual-picture login, Confidentiality, Integrity, Click-points, Coordinates.***

## I. INTRODUCTION

Security for the users to access any kind of application is becoming more popular than even before. This is due to recent technological advances in terms of authentications. The authentication is a process of proving or showing to be true and this includes confidentiality and integrity. The improved security of authentication is additionally known as multifactor authentication (MFA) for users. MFAs has intended to provide more security in terms of authentication and also has led to decrease in vulnerabilities. MFA is a security system that verifies a user's identity by requiring multiple process while logging in rather than just asking for username and password. MFAs requires other additional sources to identify if the users are authentic or not. The additional sources such as a one-time-password, the answer to a security question, biometric, facial recognition and so on [5]. There are several methods or techniques to identify whether the users are authentic or not. In every smartphone, there will be security source for the users to secure login. Nowadays, for each and every application has a secured login to prove the existence of confidentiality. For all these things, the primary focus must be confidentiality, i.e., the user's credentials must be strong and unique in order to safeguard an application. The authentication for the users are implemented in many areas like bank, online transaction, all social medias, and in fact to get into our own devices to access our own contents or details. There are many techniques or ways or types to implement to an application like, biometric, one-time-password, tokens, hard tokens, SMS tokens and one of the important unique technique is visual login.

There are different types of checks to implement in a multifactor authentication and the list of checks will be always growing day by day. Each of the checks will have the level of security and latest trends of technologies to be used. One of the greatest inventions in terms of authentication is biometric verification. Biometric verification is used to check to confirm their identity as part of MFA. Biometric ID verification will be easier than entering some random one-time-password (OTPs), so customers find it less aggravating to use it frequently. Next comes the phone call, where the identity of the user is verified via phone call from the third-party application or from the native application. This has so many disadvantages over biometric ID verification. OTP verification is the process of identifying the users by sending random OTP to registered mobile and will be asked to enter the same. This also has its own disadvantage like bypassing the OTP or bypassing the SMS/Call. The Email token technique is a kind of OTP verification process in which, the unique code will be sent to the users registered email [11]. The best robust technique which is implemented in this paper is visual picture login technique. In this technique, the user has to register to an application by choosing his/her own picture and need to select four random check points. And while logging in to an application, the user has to choose the same picture which was chose while registering. And also, he/she needs to select the same four check-points which is called coordinates in order to identify themselves to access into an application.

## II. MOTIVATION

In the networking system the flow of information is the most important service. It is clear that a simple authentication failure can lead to the failure to access any of the application. Most of the authentication failures occurs when the user gives poor password and when easily decode the password types. Day-by-day the attacks in terms of authentication growing in a faster rate, and not only to meet the purpose but to mask off the attacks in terms of authentication, the security analysis is very crucial to enhance the security system for an authentication. However, to avoid these kind of security breaches or attacks, the authentication must be very secured and robust. So, this requirement has motivated me to create a novel mechanism for multifactor authentication.

**Revised Manuscript Received on August 12, 2020.**

***** Correspondence Author

**Ankush S,** MTech, Networking and Internet Engineering from JSS Science and Technology University, Mysore. Email Address: anku.aradhya@gmail.com

**Vinayprasad M S,** Assistant Professor in the Department of Electronics and Communication Engineering, JSS Science and Technology, Mysuru. Email Address: vpms1408@sjce.ac.in

## III. PROBLEM STATEMENT

The authentication for any of the applications has become the most powerful technique to identify the users from any kind of falsification. Falsification has become a severe threat to security. The falsification in terms of authentication is nothing but the attacks being attacked by some third-party by bypassing the identification of the users. Most of the application needs a login. For that, the user will give the credentials which include username and password. This shows single-factor authentication. To bypass the single-factor authentication, there are many methods or attacks and it is very easy. That is why the multifactor authentication techniques are used to provide more security in terms of authentication and maintain confidentiality. equations objective of this paper is as follows:

- Designed an android application for the users.
- The main objective is to provide information about confidentiality.
- Implemented novel method of multifactor authentication to provide security in terms of confidentiality for the users.

## IV. PROPOSED SYSTEM

The proposed application examines the confidentiality of the users by verifying his/her identity. The purpose of multifactor authentication is to avoid the falsification made by the users while logging in to any of the applications. In the proposed system, android application is used for user's side. To login to an application, user must register primarily by entering the required details and must choose the photo from his/her own phone gallery and then needs to select any random four points, which is called check-points. Once the user is registered, he/she needs to login by providing credentials which includes user name and password. This shows single factor authentication. After providing the credentials, user must choose the same photo which was chose in the time registration, then must select four check-points which is called coordinates. If the coordinates and check-points match, then user will be able to access an application. From this kind of method, the users are safe to access their applications by providing what they know and what they have. The resultant of this, the user can make a safest authentication using proposed novel multi-factor authentication. [10]

## V. METHODOLOGY

In this section, the android application is for the authentication purpose for the users to access any of the applications. The android studio is designed and developed using android studio. The only module used here is User. The user has the authority to register and login to an application. Here, to verify the recognition/oneness of the users, the visual picture login technique is used in terms of multi-factor authentication. Login: This module is for the user to login to the application using his/her username and password.

Account details: In this module, users can view the account details from the bank.

Here, entire application is developed using Java programming. The first-time user has to primarily register to an application by providing all the required information and must choose the photo and coordinates/click-points. Once the user has registered to an application, he/she must login to an application by giving credentials and then user must choose the same photo and exact coordinates. If the login coordinates match with registered coordinates, then user will be logged in as an authentic user to access further.

## VI. LITERATIRE SURVEY

[1] Author explains the multifactor authentication in the field of biometrics which are sensitive information. So, to address this privacy concern, this paper represents 'privacy-preserving MFA' system for computer user called PINTA. (Privacy-preserving multifactor authentication). He also explains, in PINTA, the second factor is hybrid behavior profile user, while first authentication factor is password. Author also used 'fuzzy hashing' and 'fully homomorphic encryption (FHE)' to protect users sensitive profiles. At last in conclusion, he briefly explains the proposed system called PINTA. [2] Author explains why authentication is necessity in information system, as they are vulnerable to many kinds of cyber-attacks, one in which is unauthorized access. He also explains the flow of authentication. i.e., Firstly user sends out the request, then authentication server response with the challenge, and then user provides his/her identity by calculating a response which is validated by the server. Author proposed a solution of provably secure robust authentication in fragile communication environment which authenticates the user by password, smart-card and bio-metrics. He also states that his proposed new protocol provides a promising authentication solution in slow connection situation. This paper also contributed a stand-alone authentication, with which users can be authenticated correctly even the connection to the remote authentication server is down. [3] This paper proposes the novel multi-touch gesture-based authentication technique. Author proposed using set of 5-finger touch gestures, based on classification movement characteristics of the palm and fingertips. This paper uses pattern recognition techniques. Author built a classifier to recognize unique biometric gestures characteristics of an individual. [4] The author explains about the graphical password, in which an image will be password image which contains the enough click spots to the users. Click points will be touchable areas in which a user can recognize those areas by looking at the clickable points in key image. Author have achieved an intermediate difficulty in most of the attacks like brute force and shoulder surfing.

## VII. SYSTEM IMPLEMENTATION

Multifactor authentication is an approach implementing by using at least two or three authentication methods. This leads to decrease in credential falsification. In other word, authentication falsification. The proposed authentication system for user works with two phases, namely registering and login. The registration phase includes registering to the system. For registration, users have to click on the new registration button, it will display the registration form. For registration users, the users have to fill all the relevant data including username and password that is given in the registration form.

The username and password must be eccentric to the system. And also, while registering the user must choose the photo from his/her own gallery and must select 4 points in order to make a secure login. The details of the users obtained by the registration form is stored in the database. Next, while logging in the user has to fill the credentials initially. This shows single-factor authentication, and then must make the same image selection and choose those registered four points (Click-points) on the image for login. This shows multi-factor authentication.

The proposed application consists of android implementation for user module. User module is developed in android using XML as frontend for Designing using Android Studio IDE and MySQL as Backend. For Server-Side Development, Apache Tomcat is chosen as web server. Android studio is used for developing a user side application. MySQL database will be used in the backend to store data. Android is a buzzword that changes the Smartphone view from the past few years. It holds the largest part of the Smartphone world and is growing larger and larger every day. The interface of Android is foreseen on direct manipulation, using touch inputs that loosely corresponded to real-world actions, like swiping, tapping, pinching to control on-screen objects. Android software development is the process in which new applications are created for the Android OS. Application is developed in the Java programming language using the Android Studio. The Android Software Development Kit (Android SDK) provides all the necessary tools to develop Android applications. This includes a compiler, debugger, tool emulator, and has its own virtual machine to run Android programs. The Android SDK includes a mobile emulator, it is a virtual mobile device that runs on your computer. The emulator lets the user develop and test Android applications without using a physical device. The SDK also supports older versions of the Android platform just in case developers wish to target their applications at older devices. [12]

## A. WORKFLOW

This section defines the workflow of the users in terms of registration and login.

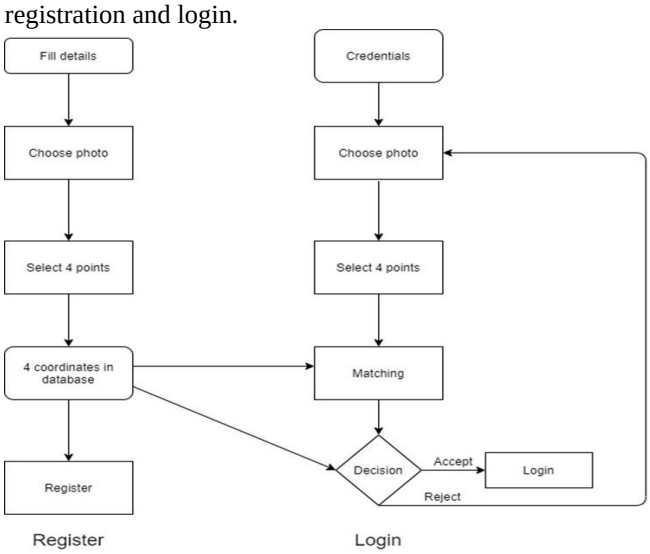


**Fig. 1. Workflow for the users**

In the above Fig. 1, the left side is the process of register and the right side is the process of login to the user for the application. Initially, the user needs to register for the application. While registering the user must give all the respective details and then upon clicking on the "choose" button in the android app, the user will navigate to his/her own gallery and must choose any one random photo and then need to click on any 4 points in the respective photo. These four points are known as click-points and are stored in the database. Upon choosing the photo and click-points, the user will be registered to an application. The right side in fig. 1 describes the login procedure for the users. After registering, in order to login to the android application, the user needs to fill the credentials, i.e., username and password. This shows single-factor authentication. Once the credentials are given, the user has to choose the same photo which is used in the time of registration. Then need to select the same 4 click-points which is also called co-ordinates. If those four co-ordinates match with the click-points, then the user will be considered as authentic user to log in to an application and navigates to the secondary activity.

## B. ALGORITHM

X11, Y11 is the coordinate registered by the user while registering.
X1, X11 is the coordinate registered while logging in.
±20 is given offset.

---

*Step 1:* ***Input****: list of points XY11=d1[0].split(),*

*XY22=d1[1].split(), XY33=d1[2].split(), XY44=d1[3].split()*

*Step 2:* ***Action****: Integer.ParseInt(XY11[0]);*

*Integer.ParseInt(XY22[1]);*

*……*

*……*

*Step 3:* ***Output****:*

*{*

*If ((X11 > X1 -20 && X11 < X1 +20) && (Y11 > Y1 -20 && Y11 < Y1 +20) && ……. (Y44 < Y4 + 20)*

*Step 4: res = "True",*

*else,*

*Step 5: res = "false"*

*}*

---

Algorithm 1

The above section shows the algorithm of multifactor authentication using picture / visual login. Here, the input (1st step) is from the user using android application, where when the user selects 4 coordinates it is assigned as XY11, XY22, XY33, XY44. The action (2nd step) is when the user selecting 4 coordinates using SetOnTouchListener method, initially the module takes it as a string. So, to convert string to integer values, we need to use ParseInt for those respective coordinates in. The output (3rd step) here is, X11 will be the coordinate registered by the user while registering. X1 is the coordinate registered by the user while logging in. The ±20 is given as offset because of user accessibility, where some of the user has big/small finger and also the mobile screen itself will differ.

If X11 coordinate value is 200, X1 is 210, then the result is 200 > 210 – 20 = 200 > 190. 200 is greater than 190, so true. Likewise, it will compare with Y11, Y22, Y33, Y44. If all the login coordinates are lesser than the registered coordinates, then the result is true. If not, user is again asked to select correct 4 points as it does not match registered coordinates.

## VIII. RESULT

This section shows the screenshots of the outcome. Here, first two figures describe the view for a user to register and to login to an application.

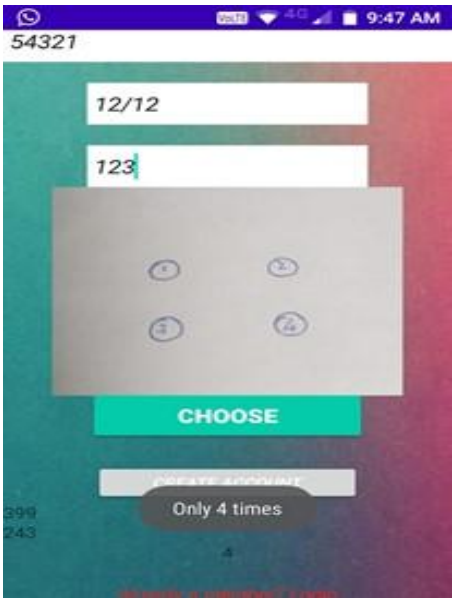


**Fig. 2. Registration process by choosing user's own choice of picture**

The Fig. 2, shows the android app for the users to register to a banking application. Here the user need to register with all the details required to a banking application and need to choose the photo of his/her own choice and must select 4 random points (coordinates) then need to click on create account.

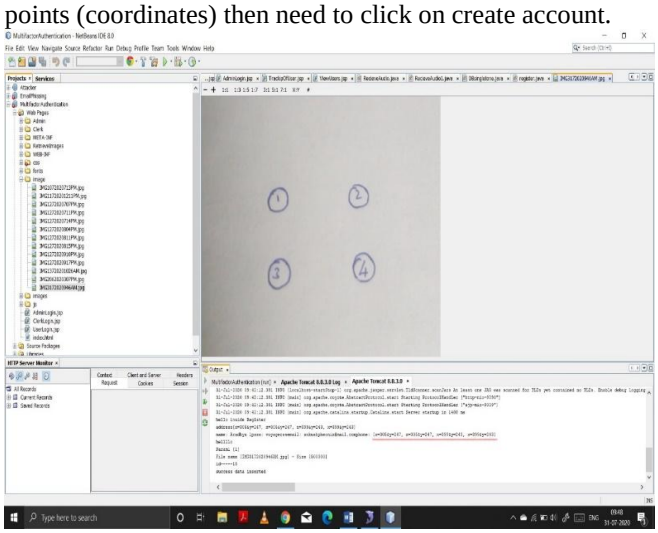

**Fig. 3. Photo chosen and coordinates are selected while registering**

The above Fig. 3, shows the coordinates selected by the user while registering. After user has given the required information, he/she must choose the photo and must selects four coordinates. The selected coordinates will be recorded as X and Y axis points. In the above fig 3, the red underlined values are the coordinates recorded by the user while registering.


**Fig. 4. Login process by choosing the same photo**

The above Fig. 4, shows login screen for the user. User must enter the credentials, i.e., username and password. This shows single factor authentication process. After providing credentials, user must choose the same photo which was selected in the time of registration and also need to choose the same coordinates to get into an application.

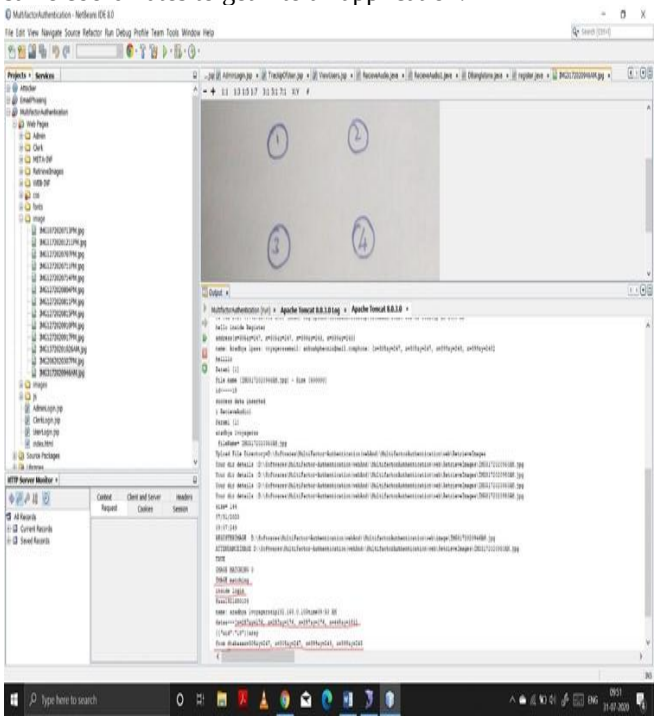

**Fig. 5. Photo chosen and coordinates are selected while logging in.**

In Fig. 5, the red underlined values are the login coordinates selected by the user while logging in. For example, if we consider X coordinate from the register, i.e., X11, we have the value 305, and the X coordinate from login, i.e., X1, we have the value 257, so according to the algorithm 1, if X11 > X1 -50 && X11 < X1 +50, then the result will be true. So, (305 > 257 – 50) && (305 < 257 + 50), that will resultant as (305 > 207) && (305 < 307), so in both the cases, the result is true and user will be allowed to login to the application based on single factor authentication as well as using these visual logins.

**Table 1 Experimental results**

| Registering coordinates (X11) | Logging in coordinates (X1) | Offset | Output (According to the algorithm) | Result |
|---|---|---|---|---|
| 200 | 210 | ±20 | (200>210-20) && (200<210+20) = **(200>190) && (200<230)** | True -Logged in |
| 305 | 257 | ±50 | (305>257-50) && (305<257+50) = **(305>207) && (305<307)** | True -Logged in |
| 150 | 350 | ±50 | (150>350-50) && (150<350+50) = **(150>300) && (150<400)** | False -Unable to login |

The above table 1 shows the best possible experimental result conducted during deployment. It is shown for only X coordinates. The same procedure is applicable for Y coordinates also.

## IX. CONCLUSION

In this paper, the novelty of authentication in terms of multi-factor authentication scheme supported visual-picture login has been developed using Java programming. Our approach is often beneficially and securely used for authentication mechanism for all types of un-trusted terminals. Experimental results are recorded in the tabular form which is most accurate with the coordinates. This new approach is exclusive in many ways:

1. This novel visual-picture login method will be helpful for several trusted and untrusted terminals.
2. The new approach resists shoulder surfing and brute force attacks.
3. This kind of authentication method is going to be more user-friendly and secured for untrusted/public terminals.
4. Can easily modified for user accessibility.

We can apply our new approach to the foremost trusted terminals like banking applications which includes online transactions, to take care of the confidentiality and integrity from the sensitive and personal data.

## REFERENCES

1. Abbas Acar, “A privacy-preserving MFA”, IEEE international journal, 2019.
2. Xinyi Huang, Yang Xiang, “Robust Multi-Factor Authentication for Fragile Communications”, IEEE international journal, 2014.
3. Napa Sae-Bae, “Biometric-rich gesture: based on multi-touch”, international journal, 2012.K. Elissa, “Title of paper if known,” unpublished.
4. Alireza Pirayesh, Angelos Stavrou, “Universal Multi-Factor Authentication Using Graphical Passwords”, IEEE international journal 2008.
5. Abbas Acar, Wenyi Liu, “A privacy-preserving multifactor authentication system”, Wiley journal, 2019M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.
6. B. Madhuravani, Dr. P. Bhaskara Reddy, “A Comprehensive Study on Different authentication factors”, IJERT 2013.
7. Alzahraa J. Mohammed and Ali A. Yassin, “Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator’s Fingerprint and Smart Mobile Device”, MDPI article, 2019.
8. Neenu Ann Shaji, Sumitha Soman, “Multi-Factor Authentication for Net Banking”, International Journal of system and software engineering, Vol 5, 2017.
9. Divya James, Mintu Philip, “A Novel Anti Phishing framework based on Visual Cryptography”, IEEE 2012
10. Sugata Sanyal, Ayu Tiwari, and Sudip Sanyal, “A Multifactor Secure Authentication System for Wireless Payment”, Springer-verlag, 2010
11. https://www.loginradius.com/blog/2019/06/what-is-multi-factor-authentication/
12. https://developer.android.com/docs

## AUTHORS PROFILE

**Ankush S** is pursuing his final year MTech in Networking and Internet Engineering from JSS Science and Technology University, Mysore. He has already one paper in his credit which was published in 2018 during his Bachelor of Engineering. His area of interest includes UI/UX, Networking and Security. Email Address: anku.aradhya@gmail.com

**Vinayprasad M S** obtained his MTech in Networking and Internet Engineering from SJCE, Mysore. He is currently pursuing his Ph.D. in JSS Science and Technology University. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering, JSS Science and Technology, Mysuru. His area of interests includes communication, Networking and IoT. Email Address: vpms1408@sjce.ac.in