International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Three Step Multifactor Authentication Systems for Modern Security

**Soumyashree RK, Goutham S**

Student, Department of Computer Science, Jain University, Bangalore, Bangalore, India

## ABSTRACT

Three-factor authentication includes all major features in password authentication such as one-factor authentication. Using passwords and two-factor authentication is not enough to provide the best protection in the digital age significantly. Advances in the field of information technology. Even when one or two feature authentication was used to protect the remote-control system, hacking tools, it was a simple computer program to collect private keys, and private generators made it difficult to provide protection. Security threats based on malware, such as key trackers installed, continue to be available to improve security risks. This requires the use of safe and easy-to-use materials. As a result, Three Level Security is an easy-to-use software.

***KEYWORDS:*** *Three-level authentication, network, security, remote access, two-factor authentication*

***How to cite this paper:*** Soumyashree RK | Goutham S "Three Step Multifactor Authentication Systems for Modern Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.1652-1657, URL: www.ijtsrd.com/papers/ijtsrd49785.pdf

IJTSRD49785



## INTRODUCTION

A project is a verification program that ensures users have access to the system only if they provide the correct password. The project includes three levels of user authentication. There are a variety of password programs available, many of which have failed due to a bot attack while a few have retained it but reached the limit. In short, almost every password available today can be broken. We have therefore decided to design a project aimed at achieving maximum security in user authentication. Contains three logins with three different types of password system. Password difficulty increases when each level user has to enter the correct password in order to login successfully. Users will be given the right to set passwords according to their preference. This project contains a text password i.e., password, colour-based password and one-time password (OTP) sent to their registered mail ID / mobile levels of three levels respectively thus there will be less chance of a bot or anyone cracking passwords even if they are cracked first or second level, it would not be possible to break the third. Many users find password systems based on very unfriendly text. So, in the case of a password in three levels we have tried to create a simple visual interface and give users the best comfier in resolving the password.

Security plays a major role in all the network systems we use in our daily lives. In this case, the Third Amendment also attempts to extend the protection by installing a 3rd level security feature. User authentication is a great building block for any secure computer system. Security concerns are increasing in all industrial areas such as banks, health facilities, factories, etc. Due to the proliferation of mobile devices and the high interaction between mobile systems and web services, user authentication is very common on mobile devices. There are desktop users. In most multi-factor authentication cases, both the mobile device and the desktop are required and compatible to ensure adequate authentication. One of the problems with authenticity is that most users' IDs and passwords are high, with many users claiming to have more user IDs and passwords than they can remember.

Three-factor authentication is widely used in businesses and government institutions that require high degree of security. The use of at least one

element in each category is required for the system to be considered as three-factor authentication selecting three-factor authentication in two categories is only valid as 2-factor authentication (2FA). An additional feature, location, is sometimes used for four-factor authentication (4FA).

It is important to note that authenticity is affected not only by the number of factors involved but also by the way in which they are used. In each stage, the choices made by the verification rules greatly affect the safety of each feature. Incorrect or missing passwords, for example, can lead to the creation of passwords such as "visitor," which completely defeat the value of using a password. Advanced processes include requiring strong passwords that are regularly updated. Face recognition systems can sometimes be overcome by raising an image. Most efficient systems may need a blink or blink to register. Loose rules and regulations result in weak security; alternatively, better rules can result in better security for each item and better overall security for multiple-factor authentication systems.

**A. Literature review:**

To higher apprehend the elements in play with authentication, it's miles first vital to apprehend what authentication is. [5] Authentication and the numerous measures of authentication are used to affirm that a particular consumer or manner is who they are saying they are. It is that simple. There are 4 well-known methods that customers are authenticated: 1) something you know: This is the maximum fundamental shape of authentication with which maximum customers are familiar. This well-known is generally offered as a username or password which is understood handiest to the consumer. 2) Something you have: This shape of authentication is represented with the aid of using the consumer having ownership of a bodily entity or tool. This may be represented as a bodily token which includes the consumer's cell phone or different media tool producing a brief and on occasion unmarried use authentication code [5]. 3) Something You Are: This shape of authentication is represented as a biometric signature which includes a fingerprint, retina scan, or facial recognition. This is normally visible as one of the most powerful types of authentications whilst carried out properly. 4) Someplace you are: This shape of authentication corresponds to wherein a consumer or manner is located, and in reaction offers or denies get entry to sources accordingly. This well-known may be carried out via using quite a number of IP addresses or geographic area points [5]

Progress in validation strategies ought to don't forget the authentication inevitability of tomorrow, now no longer today. When the lot is in order, its miles essential to spend extra in an effort to acquire a better degree of protection. With time, retaining an excessive degree of protection turns into extra hard and inconvenient. Some problems may be predicted and projected, along with advances in computer systems which can be making dictionary- attacking a password database less difficult and less difficult. Some issues are extra hard to predict, along with the invention of new "day-zero" vulnerabilities in software program [1, 7]. In this Three Level Security we have got tired to boom the protection through concerning a 3-level protection method, concerning text in maximum instances based absolutely at degree one, image based absolutely Authentication at Level two, and automatic generated one-time password (received through an automatic message to the user) at degree three. In 2d degree, the use of awesome photograph set with inside the IBA System Authentication plays a vital role in shielding reassess in competition to unauthorized and smuggled use [4, 6]. With the use of biometrics and other authentication methods in an efficient manner, the implementation of a future market standard of a three-factor authentication approach becomes all but assured. Efficiency breeds confidence, and confidence breeds' dependability. It's difficult to dismiss the increased reliability of a more secure platform with three-factor authentication. With more research, the software might be extended to allow users to create their own accounts, as well as to save credentials and biometric reference tags in each user's account [5].

Multifactor authentication (MFA) is a secure tool type in which multiple shape of authentication is carried out to affirm the legitimacy of a transaction. In contrast, unmarried component authentication (SFA) entails most effective a person ID and password. In two-component authentication, the person gives twin manner of identification, one in every of that's normally a bodily token, including a card, and the alternative of that's normally something memorized, including a safety code. Additional authentication strategies that may be used in MFA consist of verification including finger scanning, iris reputation, facial reputation and voice ID [2, 3, 9, and 11]. The proposed technique makes use of 3 elements to authenticate the consumer into the goal application/website.

The first component is a regular method, which isn't very tough to utilize, reasonably-priced and steady, that is the conventional mode of validation referred to as Alphanumeric Password. The 2d component is the method this is additionally clean to apply and steady

that is a Graphical Password which includes click on points, pass faces, and picture and image primarily based totally data. After the consumer presents his/her username to login into their account, first authentication takes a look at can be the Alphanumeric Password which is selected on the time of registration for that unique site/account [1]. Once it's get proven through the admin, the consumer has to offer the picture password to pass the second one safety take a look at, so one can be a picture, click on point / pass faces. If the verification failed at both gateway, alarm message can be sent to the consumer declaring fake authentication. If the verification succeeded, as a 3rd component, one of the safety questions saved on the time of registration will randomly displayed and the consumer has to offer the appropriate solution. If incorrect solution is given then authentication fails in any other case the consumer can be authenticated to go into the website/account.

Features of the proposed validation gadget are, it's far less complicated to apply, steady and reasonably-priced. Both the passwords and solutions are consumer selected now no longer given through different password control gadget. And the ones passwords and solutions maintained through Carrier Company of the website/consumer account and now no longer through password control gadget. This will increase the fulfilment of the proposed gadget to the most extent [1].

The proposed system is an MFA scheme that has the advantages of diverse authentication schemes. Users have the entire freedom to pick out whether or not the 3-D password may be entirely recall, biometrics, recognition, or token based, or a mixture of schemes or more. This sort of choice is crucial due to the fact users are one of a kind and that they have various requirements. Hence, to make sure excessive user acceptability, the user's freedom of choice is crucial. Proposed system is as follows: Two Way authentication system (3-D password). In this study there are 3 stages. In first phase of security user should provide (Text) username and password, if username and password given by the user is authenticated by admin side then user will get into the 3-D surroundings. 3-D surroundings are the second phase of security, on this user will move a few objects and those places of objects may be taken into consideration as password, if the 3-D graphical password is accurate then user gets one-time generated code on their mobile. This is very last 1/3 phase of security, then user want to go into that to the website interface and if entered code is accurate then user once more get hold of colour code on mobile. User will set up that colour code if it's far accurate, then the website's web page containing various action items will be displayed in order to perform various actions.[3]

### B. Proposed methodology:

The concept of 1FA, 2FA the world of cyber security has evolved bringing in 3FA boosted the ability of information security to a next level, as and when technology adapts to new world systems the security part has to get updated all over again this leads to new and advanced innovation in the field of math, information science and computer science, the implementation of 3factor authentication is a lot cheaper compared to other traditional cloud hosting services. Usability index within cyber security community and as we observed was very tedious. The authentication factor requires technology that has to have a bare minimum security of its own, saying so this project has an efficiency rate of more than 76% in handling extreme threats. It can hold out mediocre attackers and script kiddies. When it comes to user friendliness the 3FA fails to keep its charm, in today's world people value time and the longer the verification takes the more frustrates the user gets he would prefer other means of authentication due to 3FA'S tedious authentication system. According to global index an average human being has a tendency of waiting for 25 seconds before he chooses to move on to his other chores. 3FA and MFA to some extent fails in this sector. Future research enthusiast can work upon making the existing system more feasible yet with strong security attributes to keep both the client's time and data secure. There can be addition of various technologies put into this system, one can include facial recognition, biometric, retinal scanning etc… It can also be implemented on newer technologies like the Block chain and the most recent WEB-3 the new age internet.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus, it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

- **Homepage**

This is the first page of the project where the user can either login or signup using the available features. Signup: To sign-in/register of User

Login: To continue login


**Fig. 1 Homepage**

- **About**

In this section of the project we have added a brief introduction and a warm information of basics of security and the threats modern security face in a day to day situation.

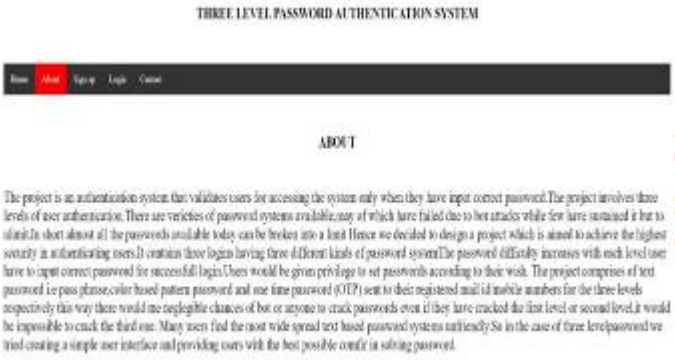


**Fig.2 about page**

- **Signup**

This step is where the user can interact with the module where he/she can input details required for initial registration they will have to enter their name, E-mail, password they want to choose, 32 confirm password and phone no, after entering all the above details they can simply click on the submit button where a message will pop saying registration successful.


**Fig. 3 Signup page**

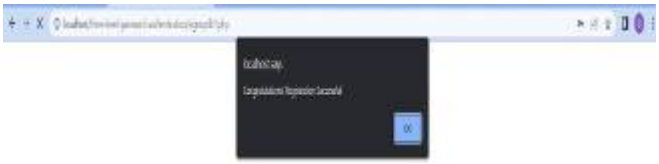

**Fig. 4 registration successful page**

- **Colour pattern**

This phase consists of a very fun interactive session where the user will be prompted the names of various colours, user can choose the colour of his/her choice and this choice of the user will be stored in a database.


**Fig. 5second-level authentication i.e. pattern**

- **OTP section**

Here the user has to enter his/her phone number where an OTP will be generated with the help of MF91 portal, along with DLT licensing, Sender ID, Auth Key generation.


**Fig.6 Third-level authentication i.e. OTP**

- **Login section**

Once the user has registered using the three-level authentication mentioned above he/she can successfully login by giving valid credentials in all three levels.


**Fig. 7 Login page**

- **Contacts page**

In this page we have mention our personal contact details with phone no and email address.


**Fig. 8 Contact page**

## ➢ Conclusion:

Authentication is critical for safeguarding resources against illegal access. There are a variety of authentication techniques available, ranging from simple secret-based authentication to overprice and computation-intensive identifying systems. However, the most widely used authentication method still relies on the use of text passwords. Text-based passwords don't appear to be safe enough for various applications that use access management technologies to enforce security. Text-based passwords with authentication functionality have significant limitations. We tend to face live in our anticipated system, offering security on three levels. The first level text password identification is followed by the second level text password identification.

Previously, much of the authentication was created based on traditional password i.e., using textual. With the advances in technology, a value can be added to the password authentication by using biometric data, which led to multifactor authentication and a more secure cloud environment. Thus, with the multilayer authentication, it is difficult for hackers to attack the system, especially related to the use of passwords. Further, more awareness on authentication is needed among Internet users to help create a secure online environment. In future, different biometric authentication methods can be combined for greater key encryption, which improves information security. Biometric authentication should also be used whenever there is in need for higher security. OTP can be used to increase surveillance and safety templates, as it changes on the device with each use.

## ➢ Future enhancement:

1. Reducing documents by introducing OCR The mobile application can be updated with OCR system. It can be trained to precisely understand a doctor's handwriting over time and after scanning any doctor's handwritten prescription or report, it will store the prescription or report in digital text format which will be much easier to understand by patients.
2. Cloud based multi-end application 39 the mobile application can be developed and made cloud based. Doctor's version of the application can be developed so that doctors can access their patient's data easily and follow up easily with their patients on a regular basis. Doctors will be able to update their status on their availability and patients will be able to use this information and set appointments with the doctor or their assistants.

Future research should combine authentication methods in large-scale studies and increase the sample size for better results. It is also recommended that future studies evolve in a multi-server environment. This systematic review also concluded that no study was done to examine the types of authentication methods being used in Malaysia among Internet users. Most of the studies were found to be in India, China, countries from Middle East, and Europe. Research about authentication method used in Malaysia is highly recommended. This is because Malaysia is one of the leading communication technology countries with almost 89% of its population which is equivalent to 25.4 million Internet users. Future research can propose a secure authentication scheme according to the suitability of subjects of study. We hope this study can provide cloud users with increased awareness of the types and importance of authentication.

**References:**

[1] C. LakshmiDevasena "Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number10 (2018) pp. 7576-7579

[2] N. Subashreddy, Ravi Mathey "Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication" International Journal of Scientific Engineering and Technology Research ISSN2319-8885 Vol. 03, Issue. 50 December-2014, Pages: 10187-10189

[3] Miss. Nilima D. Nikam, Mr. Amol P. Pande "Two Way Authentication System 3D Password-3 Levels of Security" International Journal of scientific research Volume: 3 | Issue: 1 | January 2014 • ISSN No 2277 –8179.

[4] M. Aparna, S. Gopalakrishnan, C. M. Anjusree "Three Level Security System using Image Based Authentication" International journal of advanced Research in Computer and

Communication Engineering Vol. 7, Issue 11, November 2018.

[5] William Kennedy, Aspen Olmsted "Three Factor Authentication" Research gate 325078650 |2017.

[6] IftakharHossain, SabrinaTasnim, ArifurRahaman "Vehicular Security System Using Three-way Authentication" International Journal of Scientific & Engineering Research Volume 10, Issue 5, May-2019 ISSN 2229-5518

[7] B. LAKSHMI PRAVEENA, M. ANITHA, J. SUPRIYA, T. LAKSHMI PRIYA "Student Portal with 3 Level Passwords Authentication System" IRE Journals|Volume 1 Issue 10 | ISSN: 2456-8880| Arp-2018

[8] AleksandrOmetov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, TommiMikkonen, YevgeniKoucheryavy "Multi-Factor Authentication: A Survey" MDPI Jan-2018.

[9] B. Madhuravani, Dr. P. Bhaskara Reddy "A Comprehensive Study on Different Authentication Factors" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 10, October - 2013

[10] FamutimiRantiola, EmuoyibofarheOzichi, AkinpuleAbiodun, GamboIshaya and OdeleyeDamilola "DEVELOPMENT OF A MULTIFACTOR AUTHENTICATION RESULT CHECKER SYSTEM THROUGH GSM" Computer Applications: An International Journal (CAIJ), Vol. 1, No. 2, November 2014

[11] Lazarus Kwao, RichardMillham, DavidOppong, WisdomXornamAtivi "Multi-Factor Biometrics for Enhanced User Authentication in an E-Health System" Texila International Journal of Management ISSN: 2520-310X DOI: 10. 21522/TIJMG. 2015. 06. 02. Art004