



E-Authentication System With Multi-Factor Authentication (MFA)

^aS. Uma, ¹C.G.R Keerthee raj, ²K Kiirthick, ³M Logesh, ⁴B Lokesh

^aAssociate Professor Department of Information Technology, Panimalar Engineering College

^{1,2,3,4} Department of Information Technology, Panimalar Engineering College

^aumaokj@gmail.com, ¹Klk1919299100@gmail.com, ²k7kiirthick@gmail.com, ³ln887296@gmail.com

⁴Lokeshbalaji1180@gmail.com

ABSTRACT: As the web services are created and developed rapidly, more individuals utilize these services in day-to-day life. In this computerized world, hacking is any specialized exertion to control the ordinary conduct of system associations and associated frameworks. In current share market system, investors invest their funds through web services which is prone to hacking, for example, key loggers or brute force attack method to get user's password. Now proposing another method which is multifactor authentication consist of OTP with the combination of QR-code which is a variant of the 2D barcode, CAPTCHA and Face detection.

KEYWORDS : E-Authentication, OTP, QR code, CAPTCHA and Face detection, security.

1.INTRODUCTION

In this modern world Online trading has become the newest fad for people trying to invest their money. Anyone with access to the Internet can set up an investing account. This technology for personal investing has its advantages and disadvantages. It has made it easier for the people to make investment. It has also made it easier for people to become addicted to trading, which can become an expensive habit.

Online exchanges need to be secure to protect the funds of the people. Access is for the most part through a safe site utilizing a username and password, however security is a key thought in investing and numerous online exchanges additionally offer two factor confirmation using PIN and OTP.

The drawback in this method is that PIN and OTP can be hacked by keylogging method and by using bots.

Security of a client's investment data is significant, as without it exchanges couldn't work. Additionally, the reputational dangers to exchanges themselves are significant. In spite of the fact that single password authentication is still being used, it without anyone else isn't viewed as secure enough for in certain nations. OTP may seem secure enough but this method has several serious security drawbacks. Here is why one shouldn't be using OTP via SMS two-factor authentication. SIM information is often stored and transferred digitally. Hackers can transfer this information to their devices using trojans on the victim's phone or obtain information. With this information hackers can disconnect the victim's phone from the mobile network.

In this paper, propose verification framework for investing exchanges with Multi-Factor Authentication.

2.Literature survey

In this modern world, simple authentications are not enough, There are many approaches to authenticate the identify of the system like biometric or tokens but password is still the most used method due to the fact that password can be easily implemented without the need of any additional hardware and software.

However, there are some drawbacks of using passwords like memorization issues and complexity of managing many passwords which leads to the need of additional security services.

In 2019 AnoudBani-Hani, Munir Majdalawieh discussed the most common online security attacks motivates most organisations to look for and use stronger authentication methods instead of using a normal username and password authentication.[3]

In 2020 Masoud Alajmi, Ibrahim Elashry, Hala El-sayed and Osama S. Faragallah proposed a A Password-based Authentication System based on The CAPTCHA Problem the security of the proposed system is against two possible attacks the brute force attack and the replay attack and the results prove that the proposed system is immune to these attacks.[2]

In 2022YazanAlshboul, WaelOdat discussed the study adopts a text mining approach to uncover the design principles of PMSs extracted from online users' reviews and feedbacks to improve the adoption of PMSs.[8]

All these methods were Two-Factor Authentication (2FA) ,Now proposing a most secure Multi-Factor Authentication(MFA) consist of OTP, QR code , CAPTCHA and face recognition.

3.DESIGN

This project consist of OTP, QR code, CAPTCHA and Face detection. The organisation provides OTP, QR code and the client has to enter CAPTCHA which prevents the software from bot attack . Face detection scans the face of the client and verifies it.

OTP (One-Time Password)

An OTP is a one time password which just substantial once. It is a produces numeric characters that validates the client login session.

In OTP-based validation strategies. The one-time passwords is received in client's device in which the client has to enter the number and the server verifies it . The OTP evaluates moment or second timestamps for more prominent security. The advantage of one-time passwords is that they become invalid in minutes, which keeps attackers from getting the secret codes and reusing them.



Figure 1:OTP

QR Code

The QR is stands for “**quick response**” – code is basically a barcode on steroids. While the barcode holds information horizontally, the QR code does so both horizontally and vertically. QR code is invented in 1994 by the Japanese automotive company Denso Wave. A barcode is a machine-readable label that contains data to which it is attached. QR code is scanner to obtain data by catching a photograph of the code by a camera.

A QR code is a graphical image that stores information horizontally as one-dimensional barcodes do, as well as vertically. So the storage capacity for 2D barcodes is higher than 1D codes.

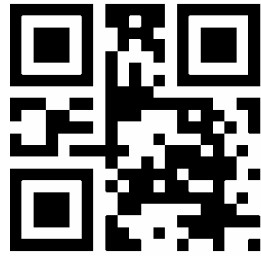


Figure 2:QR Code

CAPTCHA

CAPTCHA is a security measure known as challenge-response authentication. CAPTCHA helps the software by preventing it from bot attacks by asking you to complete a test that proves you are human and not a bot trying to break into a password protected account.

A CAPTCHA test consist of two parts a randomly generated letters and numbers or appear a distorted image, and a text box. Passing the test proves that your human.

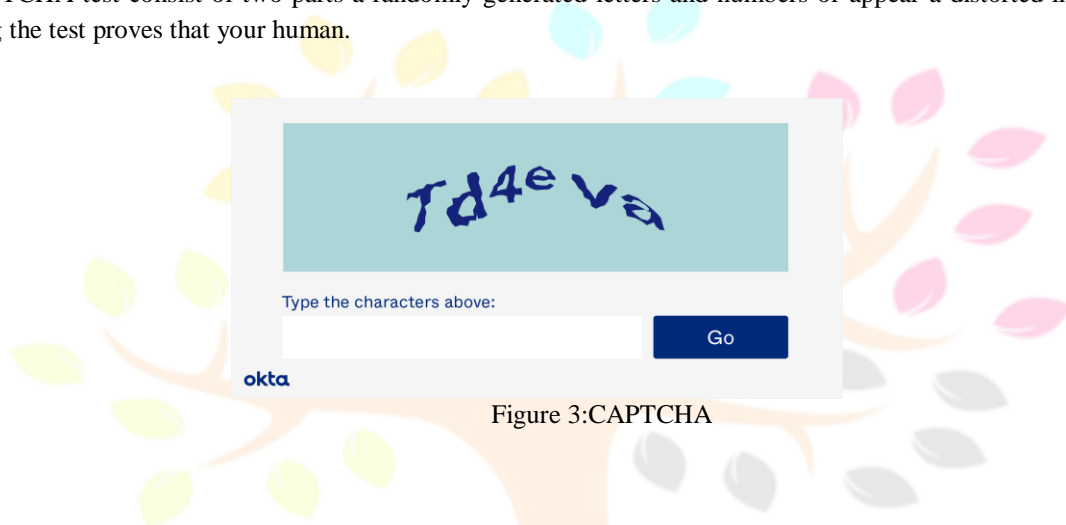


Figure 3:CAPTCHA

Face Detection

Face detection and direction are important in face recognition. In personal identification with cameras, as an example, it's is necessary to detect the face whose size, position, and pose are unknown. After the face detection, the face direction estimation is beneficial for the proper face recognition because we can select the face image of the most desirable direction from the face images taken by the multiple cameras.





Figure 4:Face detection

Software Requirements:

- Windows Xp, Windows 7
- Java.

Hardware Components:

- Processor – i3
- Hard Disk – 5 GB
- Memory – 1GB RAM

4.IMPLEMENTATION

In this paper, propose verification framework for exchanges which can give more prominent security and accommodation by mobile OTP with the QR-code, The 2D scanner tag received by current worldwide and national principles. The organization produces the QR-code utilizing the client's enter transfer information , the client uses a phone to peruse the code. At that time client enters the created OTP code and finish the verification procedure with CAPTCHA and face recognition.

5.RESULT

As many online trading Exchanges uses only two factor authentication which can be time efficient, but to make it more secure it is necessary to use multi-factor authentication, security is vital to safeguard client's data. So we propose the utilization of OTP,QR code, CAPTCH and face recognition.

6.CONCLUSION

The usage of investing in online services is expanded step by step in everyday life and existing exchanges required the use of additional security, since we don't have the foggiest idea when and where attacks like Pharming and phishing occurs it is necessary to add extra authentication to achieve higher level of security.

In electronic monetary administrations, the significance of resembles two side of a coin. It can't be given thinking about that appear on single side. Subsequently, we ought to be looked for gadgets to meet all simplicity and security of electronic money related administrations.

REFERENCES

- [1] Haria, Aashni, et al. "Hand gesture recognition for human computer interaction." *Procedia computer science* 115 (2017): 367-374.
- [2] M. Sumithra and Dr. S. Malathi, "A Brief Survey on Multi Modalities Fusion", *Lecture Notes on Data Engineering and Communications Technologies*, Springer, 35, pp. 1031-1041, 2020.
- [3] Sharanyaa, S., and Madhumitha RP. "Eyeball Cursor Movement Detection Using Deep Learning." *RP, Madhumitha and Rani. B, Yamuna, Eyeball Cursor Movement Detection Using Deep Learning (July 12, 2021)* (2021).
- [4] M. Sumithra and S. Malathi, "A survey on Medical Image Segmentation Methods with Different Modalities", *International Journal of Engineering Research and Technology (IJERT) – Vol. 6 Issue 2, Mar 2018*.
- [5] B. Buvaneswari and Dr. T. Kalpalatha Reddy, "ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial", *International Journal of Advanced Trends in Computer Science and Engineering*, ISSN 2278-3091, Vol. 8, No. 1, Pp. 12-17, 2019
- [6] K. Sridharan, and Dr. M. Chitra, "Proficient Information Retrieval Using Trust Based Search On Expert And Knowledge Users Query Formulation System", *Australian Journal of Basic and Applied Sciences*, 9(23) July 2015, Pages: 755-765.
- [7] Sharanyaa, S., and K. Sangeetha. "Blocking adult account in osn's using iterative social based classifier algorithm." *International Journal of Scientific Engineering and Science* 2, no. 1 (2018): 33-36.

