Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

Triple OTP Authentication

Shahzaib Bijapure
PG Student: Department of Information Technology
K.J. Somaiya college of Engineering
Mumbai, India

Dr. Irfan Siddavatam
Professor: Department of Information Technology
K.J. Somaiya college of Engineering
Mumbai, India

***Abstract*—In this work we propose to design and implement a secure one-time password (OTP) system to provide a better method of enforcing a stricter set of policies, that bypass natural human habits of choosing passwords that do not abide by the policies of an organization, leaving systems vulnerable to security threats. Analysis of the OTP system is done to ensure it is not vulnerable to different kinds of security threats and other risks**

Keywords— One-Time Password (OTP); Temporary One-Time Password (TOTP); Security Policy; Authentication System

I. INTRODUCTION

To give security to the user, existing frameworks utilize different degree of safety systems.

Even though intense encryption guidelines are given against network attacks, it is inclined to be broken. Intruders are sufficiently keen to recover the passwords of the users through online exchange. [3] According to the world payments report, in current innovation individuals like to utilize cashless payments as opposed to the checks or money installments. As we all realize that these sorts of e-exchanges give immense number of advantages to the users for instance, by making the exchanges simpler, quicker and moment installments. By and large, according to the study an Indian uses UPI once in seven days for installment. This online exchange may be through credit/debit cards, e-wallets, UPI's, food cards, travel cards and some approved e-installment frameworks. Numerous security execution techniques like equipment level security, antivirus, hostile to malware and antispyware programs, strong passwords, single time bound OTP framework, virtual private networks, secure site utilizes SSL certificate are utilized in practice. In any case, disregarding this load of safety components intruders go for brute force endeavors to decode the PIN numbers and passwords and so forth In this way, single level encryption standard isn't adequate to give undeniable level security to online exchange framework.[4] At present we need to have a staggered authentication mechanism wherein regardless of whether anybody encryption standard is broken, the online exchange mentioned by the user will be finished with the other person who has the rights to the OTP[6]. The proposed system believes in decentralizing the authentication by sending OTP not only to the user but also to the nominee mentioned by the user and the users Aadhar card linked email ID. verification of all the 3 will lead to activation of the service required by the user[10]

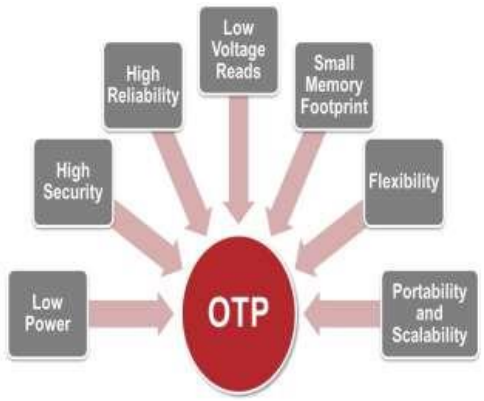

Figure 1 Advantages of OTP

H. Gupta, S. Mondal, B. Giri, R. Majumdar, N. S. Ghosh and V. P. Mishra, "An Authentication Model for Secure Electronic Transaction," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp.283-286, doi: 10.1109/ICCIKE47802.2019.9004334.[11]

II. RROMBLEM STATEMENT

Current password polices today recommend requirements in order to create a supposedly secure password.

- Length
- Case Sensitivity
- Inclusion of numerical characters
- Inclusion of special characters
- No words of significance

– Cannot be found in a dictionary
– Do no relate to habits of the individual
– Meaningful combinations (license plate, telephone numbers, etc.).
– Abbreviations

- Duration (e.g. 60-90-180 days before expiration).

Some of these standards are enforced through the training of *good password habits* A few include:

- No account sharing (Computer Crimes Act).
- Do not use the same password for multiple accounts.
- Do not write down a password.

Regardless of the above-mentioned points, individuals making passwords will in general utilize genuine words in language, as well as words that mean something to them. Despite the fact that these norms are set up, a little cryptanalysis based on the propensities for the individual has demonstrated to be powerful. [5][9] Further, no secret key is protected from a brute power attack. This is reliant upon the resources available for computing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

III. PROSPOSED SOLUTION

The present user authentication is entirely based on the credential of the specific user. In order to make sure the identity of the user accessing highly critical services is authorized the system proposed not only takes the OTP from 3 different sources. The proposed system takes the OTP from the email Id which is presently being used i.e., the email Id registered with the organization, OTP is received when the nominee details of the account are entered correctly .Email ID and the OTP which is sent to the registered email ID on the Aadhar card/PAN card. Also, as an added security measure after every mail Id entered a secret key is asked. If the above-mentioned email IDs don't match the details of the email which is now being used by the user can be sent to OSINT tools for further investigation and forwarded to the concerned authority. This idea is heavily inspired by multi-layer security and dual authentication system proposed in [1]. The proposed system is a solution the TOTP which is providing time constrains and also the issue of disclosed data leakage from QR codes is overcome. The proposed system also enforces the user to make sure his data is regularly updated with the Indian government providing centralization

A. Secret key generation: -

Following are the settings which have to be taken into consideration in order to receive the OTP mail

1. The user has to access his Google Account.
2. Select **Security**.
3. Under "Signing into Google," select **App Passwords**. You may need to sign in. If you don't have this option, it might be because:
    1. 2-Step Verification is not set up for your account.
    2. 2-Step Verification is only set up for security keys.
    3. Your account is through work, school, or other organization.
    4. You turned on Advanced Protection.
4. At the bottom, choose **Select app** and choose the app you using Select **device** and choose the device you're using Generate.
5. Follow the instructions to enter the App Password. The App Password is the 16-character code in the yellow bar on your device.
6. Tap Done.

Most of the time, user only have to enter an App Password once per app or device

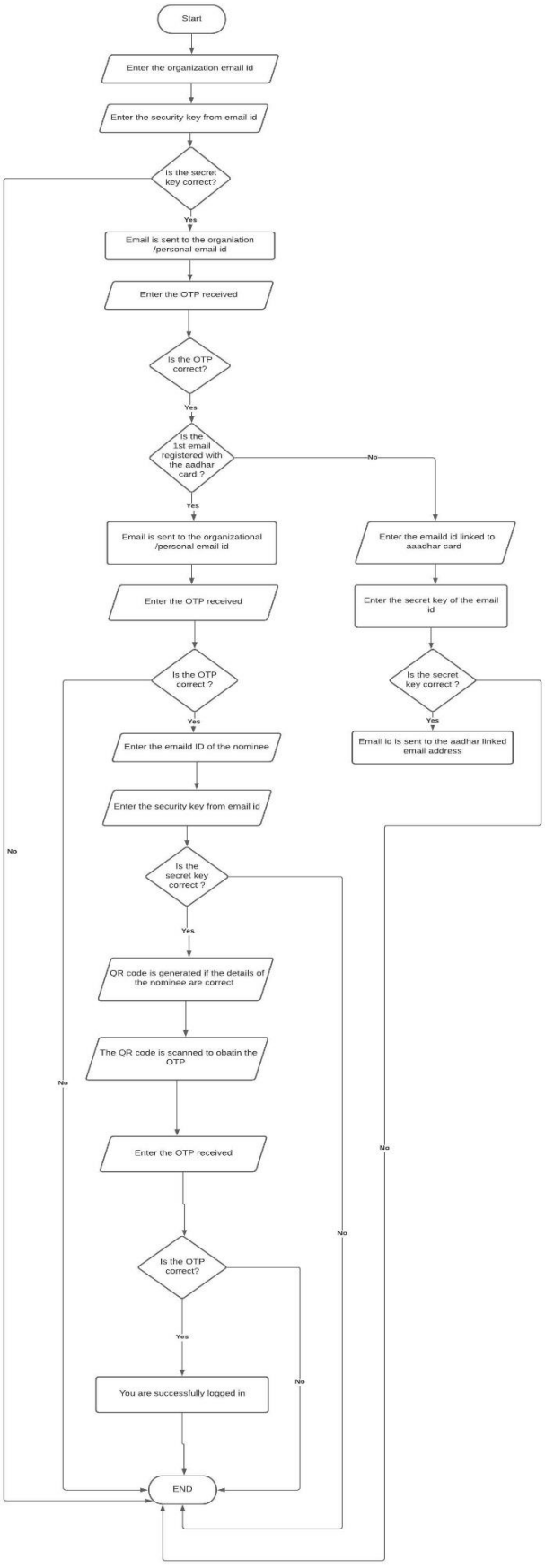

Figure 2:- Flowchart of the Proposed system

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

IV. EXPERIMENTAL RESULTS

The following experiment was conducted on a i7 7th generation machine with IDLE python 3.9 64-bit version installed. The hardware requirement does have any compulsion with respect to the processor or RAM of the system [2]

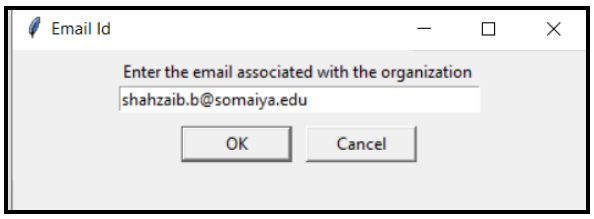

Fig.3 The authentication system asks for the login which is associated to the organisation

In Fig 3, the main purpose is to identify the association of the user with a certain organization / if not personal email can also be used

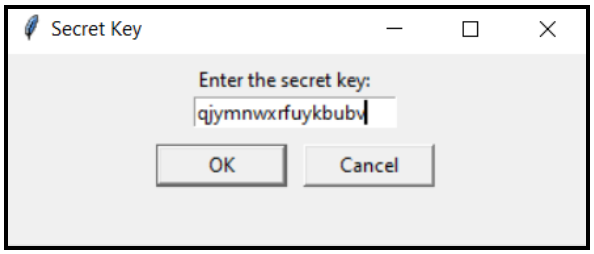

Fig 4:-The user has to enter the secret key as mentioned in section 3

The generation of the secret key (Fig 4.)is dependent on the domains to which the account is associated . In our case it is Gmail

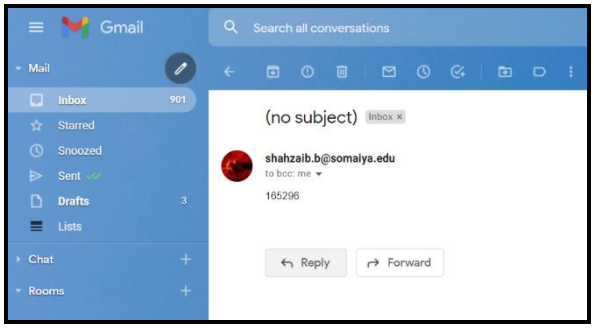

Fig 5 :- successful OTP is generated and received on the email id mentioned in Fig 1

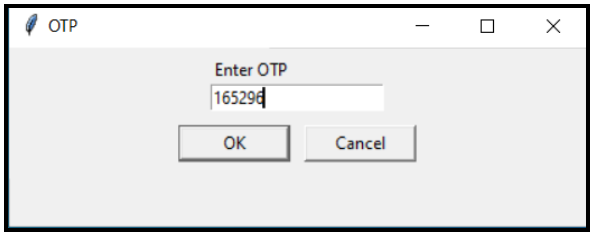

Fig 6: - Enter the OTP in the dialog box

Fig 7: -on successful verification the following dialog box is observed

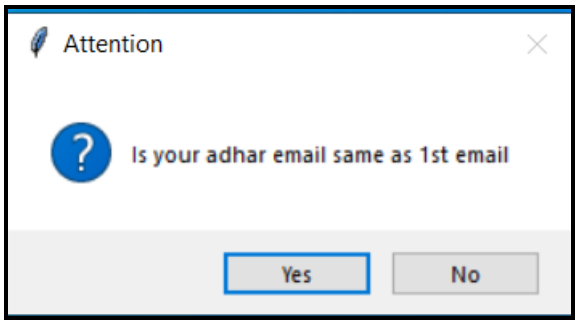

Fig 8:- Attention dialog box is displayed

The purpose of the dialog box(Fig 8.) is to ask the user whether the Aadhar email address is same as that of the email which is associated

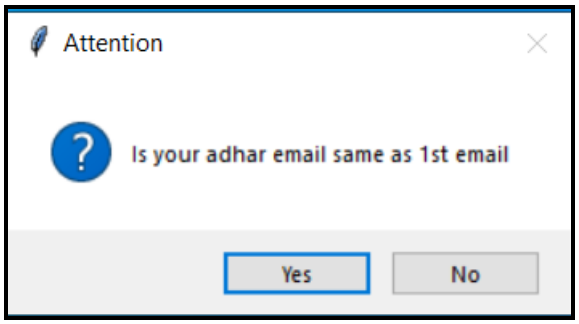

Fig 9: -The following dialog box id displayed

Fig 9 is signifying a situation where the email associated with the organization is same as that with the email associated with the Aadhar card

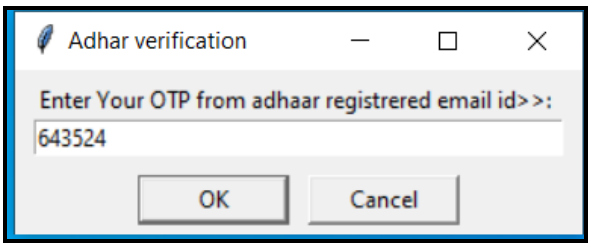

Fig 10:- If No then OTP is received on registered emaild

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

Fig 11: - Verification dialogue box

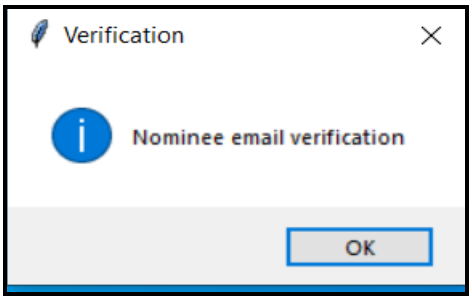

Fig 12: - Nominee Verification

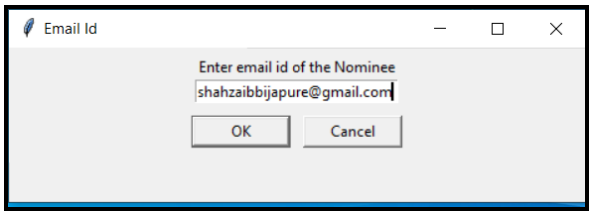

Fig 13: - Nominees email ID

Here (Fig 12) user enters the email id of the nominee. In order to receive the final OTP and complete the process

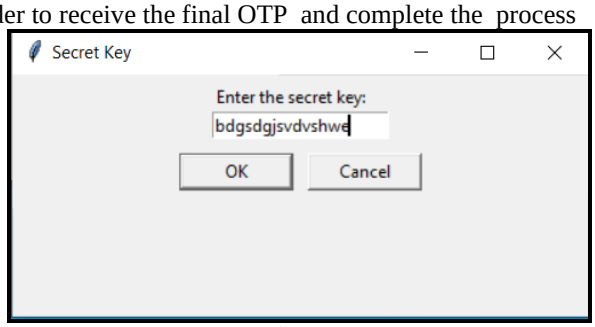

Fig 14:- Secret key for the nominees email id

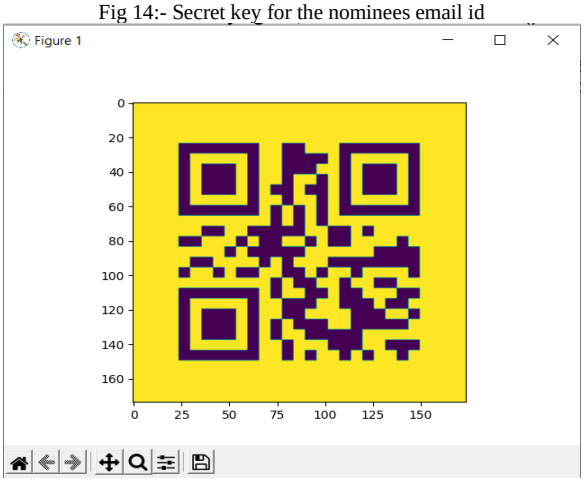

Fig 15:- QR code containing the final OTP

The following QR code is generated only when the email and the secret key of the nominee entered are correct

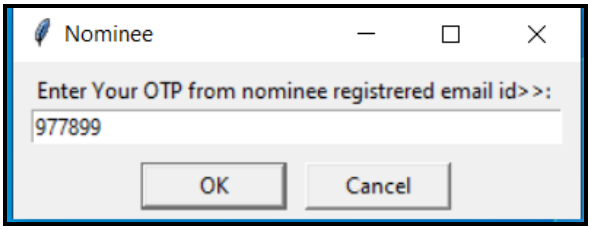

Fig 16:- OTP of nominee' email id

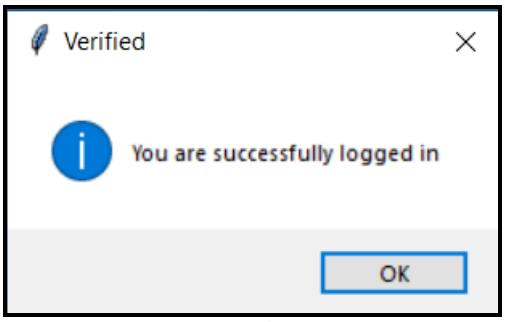

Fig 17: - Successfully logged in

The following dialogue box will appear when the third OTP is entered and verified.
From the following results the proposed system

- The current implementation clearly provides an alternative to multiple factor authentication
- The concept of "multi factor authentication" is replaced by "multi source authentication"
- The recognition to the nominee of the account is achieved
- The OTP algorithm predictability can't be possible since all the OTP are not present on the same page
- No issue of backups
- No QR codes required, encryption of scanned data is also overcome
- Even in cases where the system is corrupted (mobile/computers) login through other device and email is possible , the present authentication system doesn't restrict itself to one single system

CONCLUSION

As in the realm of digitization, a plethora attacks over e-exchanges has been a biggest danger for online business even banking security frameworks can be influenced through different noxious attacks by the intruders . Albeit tremendous security calculations through different measures and means has been consolidated yet more confirmed administrations required for exchanges on web. One such staggered security system has been forced on this paper and gives over 10% execution after some time and security contrasted with existing calculations. Triple OTP conspire is additionally one of the recognized high security throughout one-time OTP framework. In future more dependable visual cryptographic and tedious steganographic techniques can be utilized in e-exchanges

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

REFERENCES

[1] Swapnoneel Roy, Matt Rutherford, Charlene H. Crawshaw "Towards designing and implementing a secure one-time password (OTP) authentication system" 2016 IEEE 35th International Performance Computing and Communication Conference, DOI:10.1109/PCCC.2016.7820604

[2] Fuqiang Zhang, Lin Chen "OTP_SAM: DHCP security authentication model based on OTP" 2016 IEEE 20 the International Conference on computer Supported Cooperative Work in Design .

[3] Mettildha Mary, Priyadarshini, Dr. Karuppasamy, K., Marget Sharmila, "Online Fraud Detction System" 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) , Noida , India

[4] J. Thomas and R. H. Goudar, "Multilevel Authentication using QR code-based watermarking with mobile OTP and Hadamard transformation," *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 2421-2425, doi: 10.1109/ICACCI.2018.8554891.

[5] P. H. Kale and K. K. Jajulwar, "Design of Embedded Based Dual Identification ATM Card Security System," *2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19)*, 2019, pp. 1-5, doi: 10.1109/ICETET-SIP-1946815.2019.9092027.

[6] A. A. S. AlQahtani, H. Alamleh, J. Gourd and H. Mugasa, "0EI2FA: Zero Effort Indoor Two Factor Authentication," 2020 14th International Conference on Innovations in Information Technology (IIT), 2020, pp. 253-257, doi: 10.1109/IIT50501.2020.9299049.

[7] A. A. S. AlQahtani, H. Alamleh, J. Gourd and H. Alnuhait, "TS2FA: Trilateration System Two Factor Authentication," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 2020, pp. 1-4, doi: 10.1109/ICCAIS48893.2020.9096825.

[8] C. Chen, Y. Wang, H. Yu and X. Qiang, "The RFID mutual authentication scheme based on ECC and OTP authentication," 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), 2016, pp. 1-4, doi: 10.1109/ICUWB.2016.7790568

[9] G. Muneeswari and A. Puthussery, "Multilevel Security and Dual OTP System for Online Transaction Against Attacks," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 221-225, doi: 10.1109/I-SMAC47947.2019.9032466

[10] T. Kansuwan and T. Chomsiri, "Authentication Model using the Bundled CAPTCHA OTP Instead of Traditional Password," 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON), 2019, pp. 5-8, doi: 10.1109/ECTI-NCON.2019.8692255.

[11] H. Gupta, S. Mondal, B. Giri, R. Majumdar, N. S. Ghosh and V. P. Mishra, "An Authentication Model for Secure Electronic Transaction," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp. 283-286, doi: 10.1109/ICCIKE47802.2019.9004334