

# Three Factor Authentication Systems For High Secured Network

Ms. P. Devi<sup>1</sup>, Ms. N.Umamaheswari<sup>2</sup>

<sup>1</sup>Assistant Professor, Dept of Electronics and Communication Engineering

<sup>2</sup>Dept of Communication Systems

<sup>1,2</sup> Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India.

**Abstract-** *The Three Factor Authentication System for High Secured Network is a security mechanism that uses three factors for authentication: admin approval, email OTP, and mobile OTP. The admin approval factor ensures that only authorized users can request access to the system. The second factor involves sending an OTP to the user's registered email account, and the third factor involves sending an OTP to the user's registered mobile device. This system provides a high level of security and is suitable for use in applications where data protection is of utmost importance.*

## I. INTRODUCTION

The Three Factor Authentication System for High Secured Network is a security mechanism designed to provide an additional layer of security to traditional username and password-based authentication systems. This system uses three factors for authentication; including admin approval, email OTP, and mobile OTP.

The first factor involves admin approval, where a designated administrator must approve the user's login request before proceeding to the second factor. The second factor involves sending an OTP to the user's registered email account, which the user must enter on the login page. The third factor involves sending an OTP to the user's registered mobile device, which the user must also enter on the login page.

This three-factor authentication system provides a high level of security by requiring multiple forms of authentication, making it difficult for unauthorized users to gain access to the system. The admin approval factor provides an additional layer of security by ensuring that only authorized users can request access to the system.

Overall, this Three Factor Authentication System for High Secured Network provides a secure and reliable method for authenticating users in high-security environments, making it suitable for use in applications where data protection is of utmost importance.

## II. EXISTING SYSTEM

In the existing system [1], the system is designed in such a way that it will provide security via multifactor. Multi-Factor Authentication requires additional time and effort from users to complete the authentication process, which may lead to user frustration and decreased productivity. Some Multi-Factor Authentication methods, such as those based on biometrics or token devices, may require additional hardware and infrastructure, which can be costly to implement and maintain. Some Multi-Factor Authentication methods may be confusing or difficult to use, leading to poor user experience and decreased adoption. Multi-Factor Authentication methods may produce false positives or false negatives, either denying access to legitimate users or allowing access to unauthorized users. While Multi-Factor Authentication can provide added security, it is not foolproof and may still be vulnerable to attacks such as phishing, social engineering, or physical theft of authentication tokens.

In the existing system [2], the system is designed in such a way that it will provide security via graphical passwords. Graphical password authentication schemes typically have a limited number of images or patterns to choose from, which can make it easier for attackers to guess the password or use brute force attacks. Graphical password authentication schemes may be less familiar to users than traditional text-based passwords, which can lead to poor user adoption and decreased security. Graphical password authentication schemes may not be accessible to users with visual impairments or other disabilities, which can lead to discrimination and exclusion. While preventing shoulder surfing attacks can enhance security, it may not provide complete protection against other forms of attacks, such as phishing or social engineering. Users may make mistakes when selecting or entering their graphical passwords, which can lead to authentication failures and decreased usability.

## III. PROPOSED SYSTEM

A Three-Factor Authentication System for High-Secured Networks is an advanced authentication mechanism

that requires the user to provide three types of authentication factors before they can gain access to the network. This system incorporates admin approval, email OTP, and mobile OTP as the three factors of authentication.

**Admin Approval:** The first factor is the approval of an authorized administrator who verifies and approves the user's request for access to the network. The administrator must validate the user's credentials and ensure that the user is authorized to access the network. This extra layer of approval adds an additional level of security to the authentication process.

**Email OTP:** The second factor is an email OTP, which is a one-time password sent to the user's registered email address. The user must enter the OTP to gain access to the network. The email OTP is highly secure, as it is valid only for a short period, reducing the risk of hacking attempts.

**Mobile OTP:** The third factor is a mobile OTP, which is a one-time password sent to the user's registered mobile number. The user must enter the OTP to gain access to the network. The mobile OTP is generated in real-time and is highly secure, reducing the risk of hacking attempts.

To access the network, the user must provide all three factors of authentication. The system will verify the user's identity by matching the information provided with the registered information in the database. If all the information matches, the user will be granted access to the network.

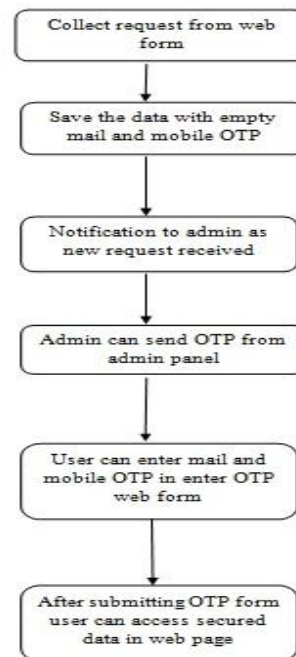
The Three-Factor Authentication System for High-Secured Networks offers several advantages over traditional authentication methods. This system provides enhanced security, improved user authentication, greater flexibility, real-time verification, admin approval, cost-effectiveness, user-friendliness, and scalability, making it an effective and efficient method for securing networks and data.

In summary, the Three-Factor Authentication System for High-Secured Networks is a highly secure and efficient authentication mechanism that requires the user to provide three different types of authentication factors, including admin approval, email OTP, and mobile OTP, to gain access to the network.

**Flow Chart**

The below shown diagram represents the overall data flow of our project “THREE FACTOR AUTHENTICATION SYSTEM FOR HIGH SECURED NETWORK”. The flow chart describes the process of collecting requests from a web

form, saving the data, and granting access to secured data using a Three-Factor Authentication System that includes admin approval, email OTP, and mobile OTP. The process starts when a user fills out a request form on a web page to access secured data. Once the user submits the request form, the data is saved in the system database along with an empty email OTP and mobile OTP. The system sends a notification to the admin that a new request has been received. The admin can log in to the system's admin panel and send email and mobile OTP to the user who submitted the request. The user receives the OTP via email and/or SMS and can enter the OTP in the designated web form. If the OTP entered by the user matches the OTP sent by the admin, the user is granted access to the secured data on the web page. The Three-Factor Authentication System offers enhanced security, improved user authentication, greater flexibility, real-time verification, admin approval, cost-effectiveness, and scalability. The system requires the user to provide three different types of authentication factors, including admin approval, email OTP, and mobile OTP, to gain access to the secured data. By incorporating admin approval and OTP-based authentication, the system ensures that only authorized users can access the secured data, providing a high level of security.



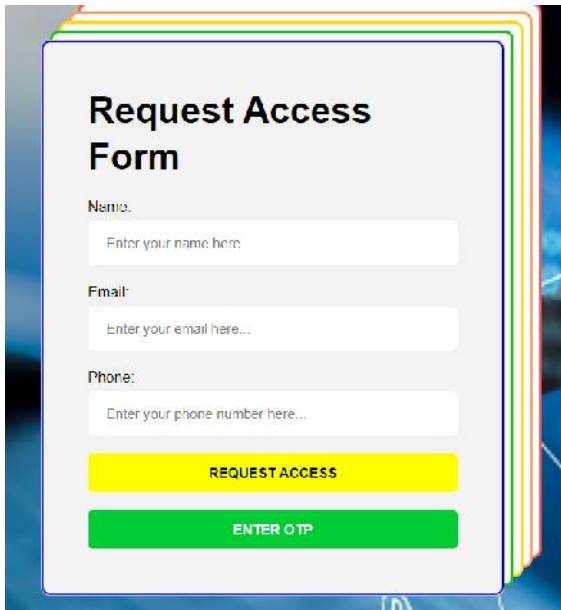
**Figure 1:**Dataflow Diagram

**IV. SOFTWARE IMPLEMENTATION RESULTS**

| ID | Name         | Type         | Collation          | Attributes | Null | Default | Comments | Charset        | Actions              |
|----|--------------|--------------|--------------------|------------|------|---------|----------|----------------|----------------------|
| 1  | id           | INT(1)       |                    |            | No   | None    |          | AUTO INCREMENT | Change @ Drop @ More |
| 2  | name         | varchar(100) | utf8mb4_general_ci |            | No   | None    |          |                | Change @ Drop @ More |
| 3  | email        | varchar(100) | utf8mb4_general_ci |            | No   | None    |          |                | Change @ Drop @ More |
| 4  | phone_number | varchar(100) | utf8mb4_general_ci |            | No   | None    |          |                | Change @ Drop @ More |
| 5  | mobile_otp   | varchar(200) | utf8mb4_general_ci |            | No   | None    |          |                | Change @ Drop @ More |
| 7  | mail_otp     | varchar(100) | utf8mb4_general_ci |            | No   | None    |          |                | Change @ Drop @ More |
| 7  | status       | INT(2)       |                    |            | No   | None    |          |                | Change @ Drop @ More |

**Figure 2:**Database table structure

The above figure represents the overall database table structure of our project



**Request Access Form**

Name:  
Enter your name here

Email:  
Enter your email here...

Phone:  
Enter your phone number here...

**REQUEST ACCESS**

**ENTER OTP**

**Figure 3:**Request access form

The above figure shows the frontend web form we are developed for getting the requests from users. We are saving this request in MySQL database.



**Access Requests**

| Name | Email           | Status                    |
|------|-----------------|---------------------------|
| Test | test@jstail.com | Send OTP / Delete Request |

**Figure 4:** Request access form

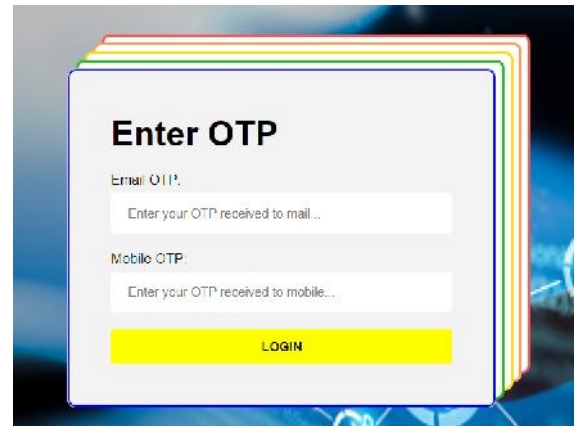
After getting the request from users from Figure 3, we are displaying requests in admin panel like in above figure. Admin can either send OTP or delete request after validating request entry.

ncreply@iot-project23.000webhostapp.com via us-imm-noc92a.000webhost.io to me

OTP request received from test  
Check admin panel for more detail.

**Figure 5** Email notifications to admin

After getting the request from users from Figure 3, we are sending email notification to admin for checking admin panel for new request entry.



**Enter OTP**

Email OTP:  
Enter your OTP received to mail...

Mobile OTP:  
Enter your OTP received to mobile...

**LOGIN**

**Figure 6:**Enter OTP Form

The above figure shows the form to enter both the email and mobile OTP's that the user receives. After clicking Login button user can see the secured data.

**Citizen aachar portal**

| Register       | Registration Agency               | State         | District  | Sub District | Pin Code | Gender | Age | Authentications | Operational Approval | Residence providing email | Residence providing mobile number |
|----------------|-----------------------------------|---------------|-----------|--------------|----------|--------|-----|-----------------|----------------------|---------------------------|-----------------------------------|
| Abhishek Singh | KCC/Ambedkar/18/20                | Uttar Pradesh | Alwarajai | Maje         | 202303   | F      | 7   | 1               | 2                    | 0                         | 1                                 |
| Abhishek Singh | Agri/Secular/Charit/Secular/0     | Uttar Pradesh | Saichhedi | Kanpur-Nagar | 201703   | M      | 8   | 1               | 2                    | 0                         | 0                                 |
| ABHISHEK SINGH | SCS/INDIA/PMU/200                 | Uttar Pradesh | Saichhedi | Saichhedi    | 201002   | F      | 12  | 1               | 2                    | 0                         | 1                                 |
| Abhishek Singh | Sec-Group/Secular/20K/20/20/1/200 | Uttar Pradesh | Shahd     | Shahd        | 201705   | M      | 8   | 1               | 2                    | 0                         | 1                                 |
| Abhishek Singh | Secular/Secular/000               | Uttar Pradesh | Lakhimpur | Vareanwa     | 201601   | M      | 8   | 1               | 2                    | 0                         | 1                                 |
| ABHISHEK SINGH | Secular/Secular/000               | Uttar Pradesh | Kaushambi | 11900        | 201711   | M      | 8   | 1               | 4                    | 0                         | 1                                 |
| Abhishek Singh | Secular/Secular/000               | Uttar Pradesh | Varanasi  | Varanasi     | 201001   | M      | 9   | 1               | 2                    | 0                         | 1                                 |
| Abhishek Singh | SECULAR/SECULAR/000               | Uttar Pradesh | Varanasi  | Varanasi     | 201603   | M      | 4   | 1               | 1                    | 0                         | 1                                 |
| ABHISHEK SINGH | Secular/Secular/000               | Uttar Pradesh | Kaushambi | 104000       | 201002   | M      | 10  | 1               | 1                    | 0                         | 1                                 |

**Figure 7:** Final secured data

The above figure shows the secured data. This is how we can see the secured data after three factor authentication.

You can't see this message. It's protected by JavaScript.

**Figure 8:** Final secured data

Without three factor authentication user will see above error message as in Figure 8.

**V. CONCLUSION**

In conclusion, the Three-Factor Authentication System for High Secured Network that includes admin approval, email OTP, and mobile OTP is a highly secure and effective method of granting access to secured data. By requiring the user to provide three different types of authentication factors, this system offers improved user authentication, greater flexibility, real-time verification, and admin approval, which significantly enhances the security of the system. Additionally, the use of email and mobile OTP-based authentication makes the system cost-effective and easily scalable, making it ideal for small and medium-sized businesses that require a highly secure authentication method

without incurring significant expenses. Overall, the Three-Factor Authentication System for High Secured Network offers enhanced security, improved user authentication, and cost-effectiveness, making it a highly effective method of securing valuable data in today's highly digital and interconnected world.

## REFERENCES

- [1] Bandar Omar ALSaleem; Abdullah I. Alshoshan, "Multi-Factor Authentication to Systems Login", in 2021 National Computing Colleges Conference (NCCC)
- [2] A. N. O. Hammed M, "preventing shoulder surfing attack in graphical password authentication scheme," *Ann. Comput. Sci. Ser. Tome 18, Fasc. 1, vol. XVIII*, 2020.
- [3] S. Yang and J. Meng, "Research on Multi-factor Bidirectional Dynamic Identification Based on SMS," *Proc. 2018 IE E E 3 rd Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2018, no. Iaeac*, pp. 1578-1582, 2018, doi: 10.1109/IAEAC.2018.8577505.
- [4] L. Dostalek, "Multi-Factor Authentication Modeling," *2019 9th Int. Conf. Adv. Comput. Inf. Technol. A C IT 2019 - Proc.*, pp. 443-446, 2019, doi: 10.1109/ACITT.2019.8780068.
- [5] V. Venukumar and V. Pathari, "Multi-factor authentication using threshold cryptography," *2 0 1 6 Int. Conf. Adv. Comput. Commun. Informatics, IC A C C I2016*, pp. 1694-1698, 2016, doi: 10.1109/ICACCI.2016.7732291.
- [6] E. E. E. Ugochukwu and Y. Y. Jusoh, "A review on the graphical user authentication algorithm: Recognition-based and recallbased," *Int. J. Inf. Process. Manag.*, vol. 4, no. 3, pp. 238-252, 2013, doi: 10.4156/ijipm.vol4.issue3.23.
- [7] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical User Authentication System Resistant to Shoulder Surfing Attack," *Adv. R es.*, vol. 19, no. 4, pp. 1-8, 2019, doi: 10.9734/air/2019/v 19i430126.
- [8] H. Umar Suru and P. Murano, "Security and User Interface Usability of Graphical Authentication Systems - A Review," *Int. J. Comput. Trends Technol.*, vol. 67, no. 2, pp. 17-36, 2019, doi: 10.14445/22312803/ijctt-v67i2p 104.
- [9] M. A. S. Gokhale and V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," *Procedia Comput. Sci.*, vol. 79, pp. 490-498, 2016, doi: 10.1016/j.procs.2016.03.063.
- [10] S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices," *Math. Comput. Model.*, vol. 58, no. 1-2, pp. 108-116, 2013, doi: 10.1016/j.mcm.2012.07.005.