IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADAPTIVE MULTI-FACTOR AUTHENTICATION SYSTEM FOR SECURE CLOUD APPLICATIONS BASED ON USER RISK LEVEL

[1]Dr. R. Devi, [2]Abul Fazal, [3]Subramanian Prajanya, [4]Mohamed Suhail, [5]Annalakshmi S

[1]Professor and Head, [2345]UG Student

[12345]DEPARTMENT OF APPLIED COMPUTING AND EMERGING TECHNOLOGIES,

[12345]Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India

Abstract: Nowadays, most of our daily activities like banking, shopping, and communication happen online. Because of this, protecting user accounts has become very important. Many systems still depend only on passwords or fixed multi-factor authentication, which are not always secure and sometimes make the login process difficult for users. So, the attackers can easily access it without the user knowledge. In this project, we propose an Adaptive Multi-Factor Authentication system that works based on the risk level of each login attempt. Instead of asking the same verification every time, the system checks details like user location, device, and IP address and the behaviour of the user. Based on this, it decides whether to allow access directly or ask for extra verification such as OTP, email verification. We have created a web application by testing the real time actions. From the results, it is clear that this approach improves both security and user experience in a better way and different from compared to traditional methods.

Keywords - Adaptive authentication, Multi-Factor Authentication (MFA), Cloud Security, Risk-Based Authentication, Secure Cloud Authentication, User Risk Assessment, OTP (One-Time Password)

I. INTRODUCTION

Today we almost use every service that requires users to log in, whether it is social media, banking, or educational platforms. Most of these systems still use passwords as the main method of authentication (traditional method). But passwords can be easily guessed, stolen, or leaked it make the attackers easy path way to access the credentials

To improve security, many systems use multi-factor authentication (MFA). Even though MFA is more secure, it applies the same verification process for every login, which can sometimes be annoying and not relevant for the user to use it

So, instead of using the same method every time, this project focuses on Adaptive MFA. The idea is simple. if the login looks normal, the system allows quick access. But if something looks unusual like new device different location and many attempt etc., then extra security steps are added.

This makes the system both secure and user-friendly at the same time. The project is also implemented as a working web application to show how it works in real life.

II. RELATED WORK

Traditional authentication is fully depended in password basis or basic authentication methods. These are easy to use but not very secure and this is one of the old methods of authentication
Some common issues are:

- Passwords can be guessed or stolen
- Same process for all users
- No ability to detect suspicious activity

Recent days the systems try to improve security by using user activity or behaviour and login patterns. from These the systems can identify unusual activities and increase security when needed. However, many of these solutions are complex and require more resources, which makes them difficult to use in simple applications.

III. SYSTEM MODEL AND ARCHITECTURE

The system is designed with the following parts:

- User interface where users enter login details
- Authentication server that processes the request
- Risk analysis module that checks the login conditions
- Verification module for OTP or email confirmation
- Notification module which alerts the user if anything goes wrong
- Decision engine which calculates the risk score and decide what type of authentication is required

IV. METHODOLOGY

Analyze each login attempt and apply the required level of security based on the risk involved.

A. Data Collection

When a user tries to log in, the system collects important details such as:

- User location (IP address)
- Device information
- Login time
- Number of failed attempts
- User behavior patterns

These details are used to understand whether the login attempt is normal or suspicious.

B. Risk Evaluation

After collecting the data, the system evaluates the risk level of the login attempt. Each factor contributes to the overall risk score.
The risk score helps in deciding the next step in authentication.

C. Decision Making

The Adaptive Decision Engine uses the calculated risk score to decide the level of authentication required. This ensures that security is applied only when necessary.

D. Authentication Process

Based on the decision, the system performs one or more authentication methods:

- Password verification

- OTP sent to mobile/email
- Email confirmation
- Device recognition

This step ensures that only authorized users can access the system.

E. System Implementation

The proposed system is implemented as a web application. The login module, risk analysis engine, and verification modules are integrated to work together in real time.

The system is tested using different login scenarios to verify its performance and accuracy.

F. Result Analysis

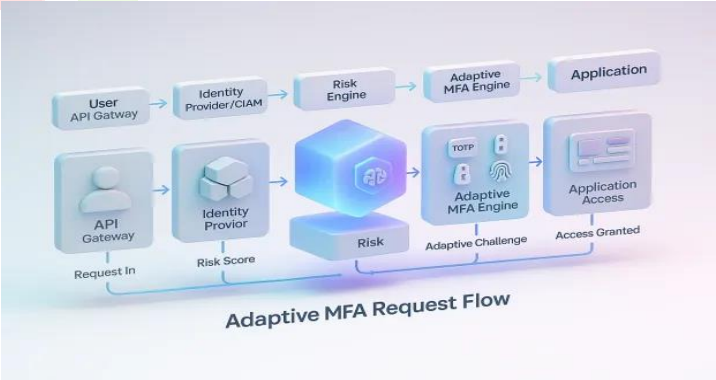
After implementation, the system is evaluated based on:

- Security improvement
- Reduction in unauthorized access
- User convenience

4.1 ADAPTIVE MFA FLOWCHART

When a user tries to log in, the system collects information such as device and location. Then it calculates a risk level. If the risk is low, the user is allowed to log in directly. If the risk is higher, the system asks for additional verification like OTP

4.2 SYSTEM ARCHITECTURE DIAGRAM



The diagram shows how different parts of the system work together. The user sends login data, the server processes it, and the risk module decides the level of authentication required.

4.3 Risk Factors Considered

The system checks different factors such as:

- Location of login
- Device being used
- Time of login
- Number of failed attempts
- User behavior

V. PROBLEM STATEMENT

Traditional systems are not able to handle modern cyber threats effectively. They either provide low security or make the process too complicated for users so the users get mad at the MFA. So, the aim of this project is to build a system that can adjust security levels based on the situation while keeping it easy for users.

5.1 Proposed AMFA Framework

The system divides login attempts into three levels:

- Low risk: Only password is enough
- Medium risk: Password and OTP
- High risk: More verification steps

5.1.1 Adaptive Decision Engine

The Adaptive Decision Engine is one of the most important parts of the system. It is responsible for deciding what level of authentication is required for each login attempt. Instead of using the same method every time, it makes decisions based on the risk level calculated by the system and it also take the risk score for the user to view the activity.

Because of this, the system becomes both secure and user-friendly at the same time

5.1.2 Authentication techniques

The system uses different methods such as:

- Password login
- OTP verification
- Email confirmation
- Recognizing known devices

5.2 Implementation and results

The system is developed as a web application and deployed online for testing at www.macrosatic.com

Compared to normal systems, this approach provides better security, is more flexible and gives a smoother experience. From testing, it was observed that the system can reduce unauthorized access effectively. At the same time, it avoids unnecessary steps for trusted users. So, it maintains a good balance between security and usability.

VI. CONCLUSION AND FUTURE WORK

This project shows that authentication systems can be improved by making them adaptive. Instead of using the same method like traditional authentication every time, adjusting security based on risk gives better results. The system is both secure and easy to use, which makes it suitable for modern applications and very user friendly for the user to access and use it.

6.1 Future work

- Use AI for better risk detection
- Add biometric authentication
- Improve continuous monitoring

REFERENCES

1. A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang,
"The Tangled Web of Password Reuse,"
in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, 2014, pp. 1–15.
2. D. Florencio and C. Herley,
"A Large-Scale Study of Web Password Habits,"
in *Proceedings of the 16th International World Wide Web Conference (WWW)*, Banff, Canada, 2007, pp. 657–666.
3. S. M. Bellovin and M. Merritt,
"Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks,"
in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1992, pp. 72–84.
4. H. Aloul, S. Zahidi, and W. El-Hajj,
"Two Factor Authentication Using Mobile Phones,"
in *IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, Rabat, Morocco, 2009, pp. 641–644.
5. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano,
"The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,"
in *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2012, pp. 553–567.
6. N. Clarke and S. Furnell,
"Advanced User Authentication for Mobile Devices,"
Computers & Security, vol. 26, no. 2, pp. 109–119, 2007.
7. M. Jakobsson, E. Shi, P. Golle, and R. Chow,
"Implicit Authentication for Mobile Devices,"
in *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec)*, Montreal, Canada, 2009, pp. 1–6.
8. National Institute of Standards and Technology (NIST),
"Digital Identity Guidelines,"
NIST Special Publication 800-63B, Gaithersburg, MD, USA, 2017.
9. OWASP Foundation,
"Authentication Cheat Sheet,"
[Online]. Available: https://owasp.org
[Accessed: Apr. 2, 2026].
10. Microsoft Corporation,
"What is Multi-Factor Authentication (MFA)?,"
[Online]. Available: https://learn.microsoft.com
[Accessed: Apr. 2, 2026].
11. IBM Corporation,
"What is Adaptive Authentication?,"
[Online]. Available: https://www.ibm.com/security
[Accessed: Apr. 2, 2026].
12. Google LLC,
"2-Step Verification,"
[Online]. Available: https://support.google.com
[Accessed: Apr. 2, 2026].