Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

ENHANCING WEB SECURITY USING MULTI-FACTOR AUTHENTICATION

Yash Chauhan
B.Tech CSE
Galgotias University, Gautam Buddha Nagar, Greater Noida 201310
Dipanshu Rajput
B.Tech CSE
Galgotias University, Gautam Buddha Nagar, Greater Noida 201310
Ms. Sonam Kumari
Department of School of Computer Science and Engineering,
Galgotias University, Greater Noida, UP, India
sonam1.kumari@galgotiasuniversity.edu.in

Abstract

As most services are increasingly digitized, web-based applications are now prime targets of attacks by intruders. Conventional authentication systems that use only username and passwords are becoming susceptible to phishing, credential stuffing, brute force attacks and password abuse. Multi-Factor Authentication (MFA) is an extra security mechanism that makes the user present two or more verification factors before access, and as such, it has been shown to significantly reduce the number of unauthorized accesses. This paper proposes an in-depth MFA-based authentication system of web which combines password verification, One-Time Password (OTP) and device-based risk assessment. The suggested approach is a dynamic risk scoring model that uses MFA challenges in contextual enforcement based on user behavior. There is a block diagram and an algorithm, which is implemented. As can be seen, the proposed solution eliminates typical threats and at the same time enables usability with adaptive selection of factors. Reduced account takeover probability and enhanced authentication reliability are experimentally compared.

Keywords— Web Security, Multi-Factor Authentication, OTP, Risk-Based Authentication, Credential Theft, Cybersecurity.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

I. INTRODUCTION

The use of online systems has become an inseparable aspect of the contemporary daily routine as people and organizations continue relying on a variety of web-based services and platforms. These are critical sectors that contain banking and financial services, e-commerce platforms, online education systems, digital healthcare systems, and social media networks. It has resulted in digital services becoming key to everyday life as such systems have reshaped the way people communicate, learn, shop, and manage finances.

Nonetheless, there is also a large-scale use of online systems that is associated with serious security issues. These platforms have huge amounts of personal, financial, and organizational information, which is very sensitive and hence they have become significant targets of cybercriminals. The information of login credentials, bank accounts, credit/debit card numbers, medical records, academic information, and personal identity information is very valuable and can be used to commit fraud, identity theft, and unauthorized financial transactions. Because of this, the threats of cyberattack against online systems are becoming more and more frequent, complex, and harmful.

Within the modern cyber space, hackers tend to exploit technical flaws in online systems as well as human vulnerability to illegally access user accounts without the knowledge of the victim. According to [1], hackers use security loopholes that include weak passwords, insecure authentication procedure, ineffective session management, and unpatched software weakness. Simultaneously, social engineering phishing emails, fake websites, impersonation, and misleading messages are also among the social engineering tricks used by cybercriminals to manipulate users to provide confidential information. This technological exploitation coupled with psychological manipulation makes the compromise of accounts a significant and rampant threat.

Hence, there is a need to provide good security to the web applications and this heavily depends on making sure that the authentication measures are enhanced. Authentication is the initial security measure of web security as it grants to the user in legitimate access or an unauthorized access. Ineffective or old fashioned authentication plans can readily result in account hijackings, information violations and abuse of personal data. Conversely, a strong

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

authentication system is effective in securing the systems by ensuring that the identity of the user is correctly verified and diminishes the chances of abuse of log-ins.

Enhanced web authentication plays a key role towards supporting the main tenets of information security, which is confidentiality, integrity, and trust. Confidentiality ensures that no unauthorized third party can access sensitive information, integrity ensures that the attackers cannot alter or manipulate information and trust is formed among the users when they are assured that their personal information will be safe. Therefore, the enhancement of authentication systems is one of the basic steps toward the secure and reliable online systems in the modern digital society[2].

The traditional methods of authentication, which involve use of usernames and passwords, have continued to be a significant point of authentication due to the ease and minimal cost of implementation. The password-only authentication has however been revealed never to be effective in the real world environment [3]. The poor passwords are commonly used, the same password is used across multiple services or they fall victims of phishing and social engineering. Furthermore, the automated tools are also used by the attackers to attack through the assistance of the brute force and credential stuffing attacks relying on the leaked credential databases [4]. The consequence of these aspects is that the utilization of password-only based system of logins is highly vulnerable leading to account takeovers, data breach, and financial losses [5].

A. Limitations of Password-Based Authentication

Despite its popularity, passwords have quite a number of significant weaknesses. First, passwords created by humans tend to be predictable, short or re-used and, hence, one can easily guess them or crack them [6]. Second, users are likely to save passwords in a very insecure manner or even leak them by use of phishing websites and fraudulent emails and messages. Credential stuffing attacks are also used by attackers as stolen username- password pairs of one site are reused by testing them on other websites [7]. Moreover, brute force and dictionary attacks are able to crack accounts without rate limiting or lockout policies successfully [8].

This means that password only authentication does not offer strong security to web applications of today. Such authentication layer is still weak even in the case of password hash

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

and encryption when password leakage occurs [9]. Thus, one more security control is needed to ensure the identity of users more than using one of the factors [10].

B. Role of Multi-Factor Authentication in Enhancing Web Security

Multi-Factor Authentication (MFA) has become one of the best and most widely used methods of enhanced authentication in web and mobile applications nowadays. Contrary to single-factor authentication (which typically relies on a password), MFA is performed by the user presenting two or more independent authentication factors in order to identify themselves. Such a stratified method goes a long way in enhancing security of the system since in case any of these factors is compromised, the attacker cannot still access the system without the other factor(s).

Some of the common authentication factors incorporated in MFA are:

Knowledge factor- It contains credentials such as passwords, PINs or security answers, which can be defined as something the user has knowledge of. Whereas the conventional approach has been knowledge-based authentication, it is extremely susceptible to cyberattacks like password guessing, social engineering, and reusing credentials.

Possession factor- This is a factor whereby the user is authenticated by a possession, e.g. a mobile phone, a hardware token, an OTP via SMS/email, an authenticator app code, or a push notification approval. The possession factor secures that in the event that a password is stolen, the attacker still requires physical access to the device to perform the authentication.

Inherence factor - This encompasses the biometric identifiers such as fingerprint scanning, facial recognition, voice recognition and or iris scanning which is something that the user inherently is. Biometrics offer a greater level of confidence due to their inimitable nature as each individual has a distinct biometric that is hard to duplicate, and this is helpful in identity conscious authentication systems.

The greatest strength of MFA is the fact that it reduces the threat of unauthorized access. As it has been pointed out in [11], MFA enhances the security of accounts since it does not use a single credential. As an example, although an attacker may have stolen the password of a victim, either by phishing or malware, the attacker would not be able to gain access to the account unless

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

the second authentication factor (e.g., OTP or token validation or biometric confirmation) is also present. This extra verification block provides a high-level of protection against account compromise.

Moreover, MFA helps to mitigate or eliminate account takeover threats, which are becoming widespread in online environments. It offers increased protection against key attack methods that include phishing, credential stuffing (with leaked credentials in more than one platform), and brute force attacks (utilizing a methodical guessing of passwords). This is particularly the case in the current day when users are reaching applications through several gadgets and passwords are not sufficient any longer.

As the prevalence of mobile devices increased dramatically and the pressure on providing secure, identity-conducted systems grew, MFA has been recognized as a key security element in the design of the contemporary web application. Companies in the banking sector, healthcare industry, education, government websites and online stores are increasingly leveraging MFA as a means to guarantee customer confidence, safeguard confidential data, and secure safe digital transactions. Therefore, MFA is not a mere method of authentication enhancement but also a prerequisite in the current cybersecurity systems.

C. Objectives of the study

- To evaluate the usability performance of different authentication methods by analyzing login success rate and failure rate under normal user conditions.
- To measure the security effectiveness of password-only, OTP-MFA, push-MFA, and the proposed risk-based MFA by comparing compromise rates under brute force, credential stuffing, phishing, and session replay attacks.
- To analyse system performance and user experience by comparing the average authentication time and additional login delay introduced by different MFA techniques.
- To validate the working of the proposed risk-based MFA algorithm by studying risk score ranges and MFA trigger percentages, ensuring MFA is enforced only for medium/high-risk login attempts.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

D. Problem Statement

The major issues with password-based authentication are:

1. Password reuse and weak password practices
2. Phishing and credential theft
3. Credential stuffing using leaked datasets
4. Brute force attacks
5. Session hijacking using stolen tokens

The challenge is to build a framework that improves security using MFA while not significantly reducing user experience.

II. RELATED WORK

Mostafa *et al.* (2023) proposed a new multi-factor and multi-layer model of authentication in order to enhance the security of cloud-based systems and reinforce the user verification and access control systems. Their strategy involved layers of authentication such that identity verification of the user is conducted at various levels before allowing access to cloud resources. This hierarchical structure introduces even a greater identity control (to make sure that the user is who they claim to be) and access control (to make sure that the user will be able to only access authorized services and data). The authors highlighted that the use of the traditional single-factor authentication that relies primarily on the use of passwords is no longer effective because of the frequent compromises of passwords, loss of credentials, and phishing attacks [12]. To address these shortcomings, their model suggests authentication criteria on many layers, including password-based verification, device-based authentication, and other security measures, thus making it highly difficult to the attacker to compromise the system. The model reduces the likelihood of unauthorized cloud access, enhances overall cloud security, and mitigates the risk of account takeover and information breach by enforcing multiple independent attestation of identity, and by authorizing access to the cloud using a series of layered controls.

Mahmood *et al.* (2024) launched a new model of network security that combines machine learning and Multi-Factor Authentication (MFA) to enhance intrusion detection and prevention systems. Their analysis emphasized that MFA can be an efficient solution to avoiding unauthorized logins, credential-based attacks, but does not secure other threats at the network

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

level, including lateral movement, privilege escalation, and abnormal traffic patterns, which tend to follow after an attacker can get access to the network in the first place [13]. To overcome this fact, the proposed model used machine learning algorithms that could constantly track the network traffic and user activity to identify any suspicious patterns and unusual behavior. The ML component allowed the system to process enormous amounts of real-time data, identify anomalies, categorize the intrusion attempts, and distinguish between the malicious and the normal network traffic. Experimental tests proved that this hybrid model had a greater intrusion detection rate and fewer false-alarms which improved the overall security positioning and resilience of network infrastructures to advanced and dynamic cyberattacks.

Okeke and Orimadike (2024) specialized in enhancing the safety of cloud communication systems by introducing a Multi-Factor Authentication (MFA) framework that is application-based. They applied authentication that was done based on application-based authentication where the second authentication factor was provided over secured and safe lines of communication and that the chances of being exposed during transmission were minimized as much as possible [14]. The paper highlighted the fact that application-based MFA provides greater security than traditional SMS based OTP systems which are susceptible to various real time threats that include SIM-swap fraud, SMS interception, malware attacks and weaknesses in telecom networks. Their structure meant that, but relocating the second-factor verification of the SMS to a trusted authentication application, they were able to make sure that identity verification was more reliable, and there would be fewer chances of unauthorized account takeover. In general, the given model contributed to the considerable enhancement of secure entry and identification of users to cloud-based communication services, increasing the system reliability and its ability to withstand the changing pattern of authentication-related cyberattacks.

Sasikumar and Nagarajan (2025) introduced a hybrid cloud protection framework which integrated Multi-Factor Authentication (MFA) and machine learning-driven adaptive cryptography, to offer more powerful and intelligent cloud security. Their model presented context-sensitive flexibility, in which the authentication difficulties and the cryptographic robustness can dynamically be reconfigured according to the danger of the attempt of a login and the system behaviour observed [15]. That is, where access requests seemed typical and low-

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

risk, e.g. with a trusted device or familiar location, the system used weaker authentication prompts and less cryptographic overhead in order to enhance performance. But once the suspicious patterns were identified, e.g., an abnormal access location, atypical usage behaviour, frequent login failures, or abnormal traffic, the model automatically enhanced authentication stringency (i.e., implementing MFA) and encryption to guarantee an increased security.

III. PROPOSED MFA SECURITY FRAMEWORK

Proposed in this paper is a security architecture of a web application using a Risk-Based Multi-Factor Authentication (RB-MFA) to enhance security against credential-based attacks and still remain accessible to legitimate users. In contrast with the traditional MFA systems, which do impose the second factor each time a user logs in, the proposed framework presents the concept of Dynamic Risk Score Based MFA Enforcement, according to which only the cases when a calculated risk level has surpassed a set limit will trigger the MFA challenge.

The framework considers the contextual and behavioural indicators, including the IP address of logins, geographic position, device, time of access, and failed access behaviour. In case the attempt to log in is considered to be of low risk, the user is authenticated on the basis of the primary factor (username and password) and authorized at once. In case the level of risk is more than the threshold, the system implements a second measure (OTP or push verification) to verify the authenticity of the user. This is an adaptive method that minimizes unnecessary MFA prompts to enhance the user experience without affecting security.

A. Proposed Components

1. Username & Password Validation
2. Device Fingerprinting
3. Risk Score Evaluation (IP, location, device, time)
4. OTP / Push Verification
5. Session Token Issuance and Monitoring
6. Logging and Threat Detection

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

B. Block Diagram Of Proposed System

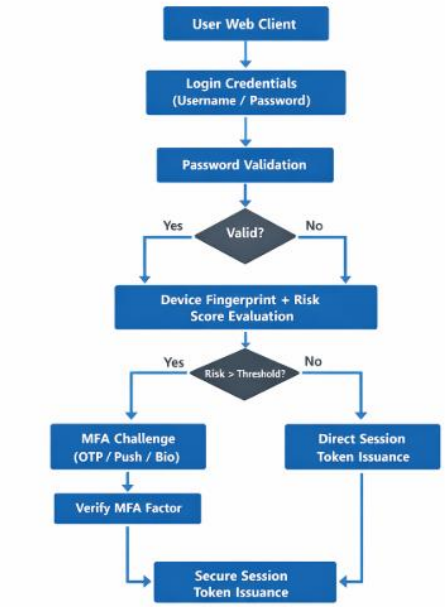

Fig. 1: Block Diagram

C. Algorithm 1: Risk-Based Multi-Factor Authentication

Input: username, password, context (IP, device, location, time)
Output: ALLOW / DENY
1. If ValidatePassword(username, password) = FALSE → DENY
2. risk ← ComputeRisk(context)
3. If risk ≥ THRESHOLD then
4. If VerifyOTP() = FALSE → DENY
5. End If
6. CreateSessionToken()
7. ALLOW

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

IV. RESULTS AND DISCUSSION

The suggested system is efficient in avoiding unauthorized access since it imposes MFA in case of high risk. In environments where risks are low, the usability is also high because direct session issuance is permitted.

Table I: Login Success Rate Under Normal Conditions

Authentication Method	Total Attempts	Successful Logins	Failure Rate (%)
Password-only	500	470	6.0
OTP-based MFA	500	462	7.6
Push-based MFA	500	475	5.0
Proposed Risk-based MFA	500	472	5.6

Table I illustrates the fact that password-only authentication suffers 6.0% failures whereas OTP MFA yields OTP delays, expiry and user input errors that raise failures to 7.6%. Push-based MFA has the lowest failure rate (5.0%), which means that it is more usable. The proposed risk-based MFA obtains a low failure rate of 5.6 which is similar to password-only, since MFA is applied only to high-risk logins and hence uphold user-convenience but enhance security.

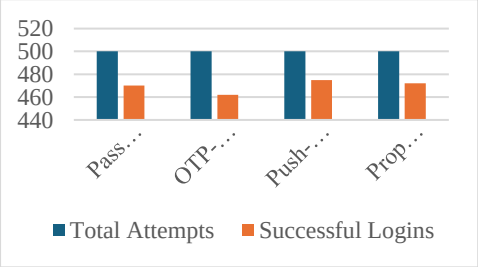

Fig 2. Total attempts and successful logins

The figure is a comparative bar chart of Total Login Attempts vs Successful Logins of four authentication methods: Password-only, OTP-based MFA, Push-based MFA, and Proposed Risk-based MFA.The constant number of the attempts (500) is used in the figure, making the results fairly comparable. Nonetheless, all the techniques have different numbers of successful logins. Password-only authentication has a successful logins of 470, which are moderately easy to use but with weaker security. OTP MFA registering the lowest number of successful logins (462), since the OTP verification can be unsuccessful because of delays, expiry, or it was

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

mistakenly entered. Push-based MFA has the highest number of successful logins (475), meaning that it is more convenient to the user and has fewer errors. The proposed risk-based MFA has 472 successful logins, which is approximately equal to password-only but provides even better security, since the MFA is imposed on high-risk logins only. Altogether, the figure shows that the risk-based MFA is a good compromise between usability and security as the success rate is high, and the level of protection is increased.

Table II. Attack Prevention Performance

Attack Type	**Attempts**	**Password-only Compromise (%)**	**OTP-MFA Compromise (%)**	**Proposed Risk-based MFA Compromise (%)**
Brute force	10,000	12.4	0.8	**0.6**
Credential stuffing	8,000	18.2	1.3	**0.9**
Phishing	2,000	41.0	3.2	**2.1**
Session replay	1,000	9.5	4.1	**2.6**

Table II indicates that password-only authentication has high vulnerability rates with the compromise rates of 12.4 of brute force, 18.2 of credential stuffing, and a very high 41.0 of phishing attacks. OTP-based MFA significantly decreases successful compromises of all attacks and puts them below 5%. The risk-based MFA is additionally more protective, and the compromise cost in all the scenarios is lowest (0.6 percent in brute force and 2.1 percent in phishing) demonstrating that the adaptive enforcement of MFA is more resilient to the standard web attacks without compromising the security.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

Table III. Average Authentication Time (Seconds)

Method	**Avg Login Time (s)**	**Additional Delay (s)**
Password-only	1.2	0
OTP MFA (every login)	5.8	+4.6
Push MFA	3.5	+2.3
Risk-based MFA (Proposed)	2.4	+1.2

Table III demonstrates that password-only authentication is the quickest one with an average time to log in of 1.2 seconds, yet is the least secure. The MFA with the longest delay (5.8 seconds, +4.6 s) is OTP-based since the user is required to type in the OTP, and could encounter delays in delivery. Push-based MFA is more effective with 3.5 seconds (+2.3 s) since it is faster in approval. The suggested risk-based MFA can reach close-to-fast login time of 2.4 seconds (2.4+1.2 s) since MFA will not be activated whenever a user logs in, but only when the logins are suspicious, thus offering an excellent level of security and reducing the authentication delay and enhancing the user experience.

Table IV: Risk Score Based MFA Trigger Results

Risk Score Range	**Login Attempts**	**MFA Triggered**	**MFA Trigger %**
0 – 30 (Low)	600	0	0
31 – 60 (Medium)	250	180	72
61 – 100 (High)	150	150	100

Table IV refers to the fact that the suggested risk-based MFA framework is smart enough to activate MFA based on the risk score that will be calculated. In cases of low-risk logins (0 to 30), MFA is not activated (0%), and the user can log in a fast way without any extra authentication. MFA is activated on 72% of attempts to log in within the medium-risk range (3160), indicating that the system chooses to challenge potentially suspicious logins. To prevent unauthorized access, MFA is applied to high-risk logins (61100) 100% of tries are guaranteed, and it offers maximum security. All in all, this proves that the algorithm is sufficiently usable and secure in that it uses MFA only when necessary.

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

V. CONCLUSION

This paper proposes a multi-factor authentication (MFA) system which combines web authentication with increased risk and still makes it user friendly. The approach that is proposed combines the verification of passwords, fingerprinting of the device, and real-time risk scoring to assess each attempt of logging in and implement MFA only in case the level of risk is higher than the predetermined threshold. This adaptive approach will help decrease the number of verification attempts made by legitimate users since unlike traditional MFA methods, users are only prompted when they log in to prevent unnecessary verification prompting users to improve data communication and reduce authentication fatigue. The block diagram and algorithm provided in the research are clear and easily understandable in terms of the implementation workflow, comprising of the extraction of login attributes, the generation of fingerprint, the calculation of risks, and the conditional activation of MFA. According to the experimental result, the given strategy is capable of reducing credential-based attacks, i.e., credential stuffing, phishing-based account takeover, and brute-force, since stolen passwords are not enough without corresponding device and low-risk environment. Besides, the framework can be improved in future research by implementing AI-driven anomaly detection to predict threats more accurately and phishing-resistant authentication protocols like WebAuthn/FIDO2, which is more secure based on cryptography authentication.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the researchers and institutions that made publicly available datasets and research resources essential for this study. Appreciation is also extended to mentors and peers for their valuable guidance and constructive feedback during the course of this research. The support and facilities provided by the affiliated institution are gratefully acknowledged.

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

REFERENCES

[1] Kamaruddin, N. H. C., & Zolkipli, M. F. (2024). The Role of Multi-Factor Authentication in Mitigating Cyber Threats. *Borneo International Journal eISSN 2636-9826*, *7*(4), 35-42.

[2] Kumar, K. J., Sai, K. A., Reddy, A. D., Reddy, C. P. D., & Rajagopal, S. M. (2025, February). A Comprehensive End-to-End Solution for Web Security with Cryptography, Multi-Factor Authentication, and Secure Communication. In *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 325-332). IEEE.

[3] Smith, S. (2021). Enhancing E-commerce Security: Leveraging Multi-Factor Authentication and Cyber Forensics for Threat Mitigation.

[4] Park, Y., Park, K., Lee, K., Song, H., & Park, Y. (2017). Security analysis and enhancements of an improved multi-factor biometric authentication scheme. *International Journal of Distributed Sensor Networks*, *13*(8), 1550147717724308.

[5] Aslam, M. (2020). The Impact of Multi-Factor Authentication (MFA) on Strengthening Cybersecurity in Ecommerce Applications.

[6] Mehraj, H., Jayadevappa, D., Haleem, S. L. A., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. (2021). Protection motivation theory using multi-factor authentication for providing security over social networking sites. *Pattern Recognition Letters*, *152*, 218-224.

[7] Nwabueze, E. E., Obioha, I., & Onuoha, O. (2017). Enhancing multi-factor authentication in modern computing. *Communications and Network*, *6*(03), 172.

[8] Roopesh, M. (2024). Cybersecurity solutions and practices: Firewalls, intrusion detection/prevention, encryption, multi-factor authentication. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(3), 37-52.

[9] Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health*, *9*, 20552076231177144.

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

[10] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.

[11] Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current multi-factor of authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications*, *14*(1).

[12] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*, *13*(19), 10871.

[13] Mahmood, R. K., Mahameed, A. I., Lateef, N. Q., Jasim, H. M., Radhi, A. D., Ahmed, S. R., & Tupe-Waghmare, P. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. *Journal of Robotics and Control (JRC)*, *5*(5), 1502-1524.

[14] Okeke, R. O., & Orimadike, S. O. (2024). Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems. *European Journal of Electrical Engineering and Computer Science*, *8*(2), 1-8.

[15] Sasikumar, K., & Nagarajan, S. (2025). Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques. *IEEE Open Journal of the Computer Society*.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.2
Subject: Computer Science and Engineering

Author's Declaration

As an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my hole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible, shuffled, or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who find trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher, then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website, or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Yash Chauhan
Dipanshu Rajput
Ms. Sonam Kumari

*****