iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83226

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Secure Authentication Mechanism for Web Application

Prajkta Rajendra Dhamdhere[1], Dipali Deepak Mali[2]
[1]*Annasaheb Magar College, Pune, Maharashtra, India*
[2]*MVP's Arts, Commerce and Science College, Nandgaon, Nashik, Maharashtra, India*

Abstract: ***The rapid expansion of web applications across domains such as finance, education, healthcare, and e-commerce has significantly increased the importance of secure authentication mechanisms. Modern digital platforms handle sensitive personal and financial information, making them primary targets for cyberattacks [1]. Traditional password-based authentication systems are no longer sufficient to defend against modern cyber threats, including phishing, brute-force attacks, credential stuffing, replay attacks, and session hijacking [2], [3]. These vulnerabilities demand a more comprehensive and adaptive approach to authentication security in web environments.This research proposes a secure authentication mechanism for web applications that integrates multi-factor authentication (MFA), encrypted credential management, secure token-based session control, and contextual risk evaluation in accordance with NIST authentication guidelines [4]. The framework utilizes strong hashing algorithms with salting techniques to protect stored credentials [5] and incorporates time-sensitive verification codes based on TOTP standards [6]. Additionally, device recognition and behavior-based anomaly detection are employed to dynamically assess login risks and enforce additional verification when suspicious activity is detected.The proposed model enhances system security while maintaining usability and performance efficiency. Experimental evaluation demonstrates improved resistance to common authentication attacks compared to traditional single-factor systems. The architecture is scalable, adaptable, and suitable for implementation in both small-scale and enterprise-level web applications. This study contributes a structured and layered authentication framework that strengthens web application security and improves user trust in digital platforms.***

Keywords: Secure Authentication, Web Application Security, Multi-Factor Authentication (MFA), Password Hashing, JSON Web Token (JWT), Time-Based One-Time Password (TOTP), Risk-Based Authentication, Session Management, Anomaly Detection, Cybersecurity.

I. INTRODUCTION

The rapid growth of web applications has significantly transformed digital interaction across sectors such as banking, education, healthcare, e-commerce, and governance. These applications process and store large volumes of sensitive user data, making them attractive targets for cybercriminals [1]. Authentication serves as the first line of defense in protecting digital resources by verifying the identity of users before granting access.

Traditional authentication systems primarily rely on username and password combinations. Although widely adopted due to simplicity and low implementation cost, password-based mechanisms are increasingly vulnerable to cyberattacks such as phishing, brute-force attacks, credential stuffing, session hijacking, and replay attacks [2], [3]. Weak password practices and password reuse further increase security risks [7].

To address these challenges, modern web security requires stronger and adaptive authentication mechanisms. Multi-factor authentication, secure tokenization, and risk-based authentication approaches have been widely recommended by security standards bodies such as NIST [4]. This research proposes a multi-layered secure authentication framework integrating encrypted credential storage, secure session management using JWT [8], and behavioral risk analysis.

A. Research Objectives and Questions

1) Research Objectives

The primary objective of this study is to design and evaluate a secure, scalable, and adaptive authentication framework for web applications that mitigates modern cyber threats while maintaining usability and performance efficiency. The study aligns with established security recommendations such as NIST digital identity guidelines [4] and OWASP best practices [2].

2) Research Questions

a) How can multi-factor authentication, token-based session management, and risk-based analysis be integrated into a unified authentication framework in accordance with modern security standards [2], [4]?

b) To what extent does the proposed model reduce vulnerability to common authentication attacks compared to traditional systems [3]?

c) What is the impact of the proposed authentication mechanism on system performance and usability?

II. LITERATURE REVIEW

Authentication mechanisms have evolved significantly over time. Early web systems relied exclusively on static passwords stored in server databases. Later improvements introduced hashing algorithms such as MD5 and SHA variants. However, MD5 and similar weak hashing algorithms were proven vulnerable to collision and brute-force attacks [9].

Modern authentication systems employ adaptive hashing mechanisms such as bcrypt with salting to strengthen password storage [5]. Multi-factor authentication (MFA), combining knowledge, possession, and inherence factors, significantly reduces unauthorized access probability [4]. Time-Based One-Time Password (TOTP) algorithms defined in RFC 6238 introduced dynamic, time-sensitive verification codes [6].

Token-based authentication systems, particularly JSON Web Tokens (JWT) defined in RFC 7519, improved session management by enabling stateless and secure token handling [8]. OWASP guidelines further emphasize secure session management practices to mitigate hijacking and fixation vulnerabilities [2].

Despite these advancements, many web applications still implement authentication mechanisms incorrectly or partially, leaving exploitable gaps. Therefore, a comprehensive integrated authentication framework is required.

A. Research Gap

Although existing studies emphasize individual authentication mechanisms such as password hashing [5], multi-factor authentication [4], and secure session handling using tokens [8], there is limited research focusing on the integration of these mechanisms into a unified and adaptive authentication framework.

Furthermore, many implementations fail to incorporate real-time risk evaluation and behavioral anomaly detection, which are critical for defending against evolving cyber threats [2], [4].

This study addresses these limitations by proposing a layered authentication model combining multiple security mechanisms into a cohesive and scalable architecture**.**

III. PROBLEM STATEMENT

Despite advancements in authentication technologies, web applications continue to experience breaches due to:

1) Over-reliance on single-factor authentication [3]

2) Weak password management practices [7]

3) Improper session handling [2]

4) Lack of adaptive security controls [4]

5) Absence of real-time anomaly detection

There is a need for a scalable and secure authentication mechanism that balances security strength, usability, and performance efficiency while mitigating modern cyber threats.

IV. RESEARCH METHODOLOGY

The proposed authentication mechanism follows a layered security model aligned with Zero Trust principles [10].

A. Research Design

This study adopts an experimental and simulation-based research design to evaluate the effectiveness of the proposed authentication framework, following standard cybersecurity evaluation practices [2].

B. Data Collection

Data was generated through simulated authentication attempts, including both legitimate and malicious login scenarios based on known attack patterns such as brute-force, phishing, credential stuffing, and session hijacking as identified by OWASP [2].

C. Sample Size

A total of 1,000 authentication attempts were simulated to ensure sufficient data for evaluating system performance and security effectiveness.

D. Data Analysis Techniques

The collected data was analyzed using the following metrics:

- Attack success rate comparison
- Authentication time measurement
- Detection accuracy (True Positive Rate and False Positive Rate)
- Security Improvement Index (SII)

These evaluation techniques are consistent with prior studies on authentication security performance [4].

1) Secure Credential Storage: Passwords are processed using adaptive hashing algorithms such as bcrypt with unique salts [5], preventing plaintext recovery even in case of database compromise.
2) Multi-Factor Authentication: After password verification, secondary authentication is enforced using TOTP as defined in RFC 6238 [6], or equivalent secure verification methods.
3) Secure Token-Based Session Management: Secure session tokens are generated using JWT standards [8]. Tokens are digitally signed, encrypted, time-limited, and invalidated upon logout.
4) Risk-Based Authentication: The system evaluates contextual parameters such as IP address, device fingerprint, login time, and geolocation in accordance with NIST risk-based authentication recommendations [4].
5) Anomaly Detection Mechanism: Behavioral monitoring detects abnormal login attempts and temporarily locks accounts after repeated failures, reducing brute-force attack success [2].

V. SYSTEM ARCHITECTURE

The architecture includes:

1) User Interface Layer (secured via TLS encryption) [11]
2) Authentication Server
3) Encrypted Credential Database
4) Token Manager (JWT-based) [8]
5) Risk Evaluation Engine

The authentication workflow:

a) User submits credentials via HTTPS.
b) Server verifies hashed password.
c) MFA verification is triggered.
d) Risk engine evaluates contextual data.
e) Secure token is issued upon successful validation.

This layered approach eliminates single points of failure.

A. Empirical Validation

To validate the effectiveness of the proposed authentication framework, experimental simulations were conducted using real-world attack scenarios derived from OWASP security reports [2].

The evaluation focuses on measuring resistance to common authentication attacks and system performance under varying conditions.

The results provide empirical evidence demonstrating that the integration of multi-factor authentication and adaptive risk-based mechanisms significantly improves security, consistent with findings from NIST guidelines [4].

VI. RESULTS AND STATISTICAL ANALYSIS

A simulation of 1,000 login attempts was conducted based on attack patterns described in OWASP security studies [2].

A. Attack Prevention Rate Analysis

Table 1: Attack Success Rate Comparison

Attack Type	Traditional System (%)	Proposed System (%)
Brute Force	42	3
Credential Stuffing	38	5
Replay Attack	29	2
Session Hijacking	25	4
Phishing-Based Login	47	6

Average attack success reduced from 36.2% to 4%, aligning with findings that MFA reduces account compromise probability significantly [4].

B. Authentication Time Analysis

Table 2: Average Authentication Time

Method	Avg. Login Time (ms)
Password Only	180
Password + MFA	320
Proposed Adaptive Model	295

Although the proposed system introduces a slight delay, security gains outweigh performance overhead.

C. Detection Performance

Table 3: Detection Metrics

Metric	Value
True Positive Rate	94%
False Positive Rate	6%
Detection Accuracy	92%
Avg. Lockout Time	15 minutes

D. Security Improvement Index

[
SII = \frac{36.2 - 4}{36.2} \times 100 = 88.95%
]

The proposed system demonstrates approximately 89% improvement in security strength.

VII. THREAT MODEL

A. Threat Model

A clearly defined threat model is essential to evaluate the robustness of any authentication framework. The proposed system considers the following attacker capabilities and assumptions.

1) Adversary Capabilities

The attacker is assumed to have one or more of the following capabilities:

- Ability to perform brute-force and credential stuffing attacks using automated scripts [2].
- Access to leaked credential databases from third-party breaches [3].
- Capability to intercept network traffic in case of unsecured communication channels [11].
- Attempt to hijack session tokens through replay or session fixation techniques [2].
- Phishing attacks targeting user credentials and one-time passwords [4].

2) Assumptions

The proposed model assumes:

- Communication between client and server is protected using TLS encryption [11].
- The server infrastructure is properly configured and not physically compromised.
- Cryptographic primitives such as hashing and token signing algorithms are securely implemented.

3) Security Goals

The framework aims to:

- Prevent unauthorized access even if passwords are compromised.
- Protect stored credentials against offline cracking attacks.
- Detect and mitigate abnormal login attempts in real time.
- Minimize session hijacking and replay vulnerabilities.

This threat modeling approach aligns with NIST Digital Identity Guidelines (SP 800-63B) [4] and Zero Trust principles [10].

VIII. COMPARATIVE ANALYSIS WITH EXISTING SYSTEMS

A. Comparative Security Evaluation

To assess the effectiveness of the proposed framework, a comparison was conducted with traditional single-factor authentication systems and basic MFA-only implementations.

Feature	Traditional Password System	Basic MFA System	Proposed Layered Framework
Password Hashing	MD5/SHA-1 (weak) [9]	bcrypt [5]	bcrypt/Argon2 with salting [5]
Multi-Factor Authentication	No	Yes (static OTP)	Yes (TOTP – RFC 6238) [6]
Token-Based Session	Basic session ID	Partial	Secure JWT (RFC 7519) [8]
Risk-Based Authentication	No	No	Yes (NIST-based) [4]
Anomaly Detection	No	No	Behavioral monitoring
Account Lockout	Limited	Yes	Adaptive lockout

B. Observations

- Traditional systems are highly vulnerable to credential reuse and brute-force attacks [3].
- MFA significantly reduces compromise probability but does not address session vulnerabilities [4].
- The proposed model integrates multiple layers, reducing attack success rate to 4% compared to 36.2% in legacy systems.

This comparative approach highlights the novelty of integrating hashing, MFA, token security, and risk-based analysis into a unified architecture.

IX. IMPLEMENTATION DETAILS

A. Implementation Environment

The proposed authentication framework was implemented in a simulated web environment to validate feasibility and performance.

1) Technology Stack

- Backend Framework: Node.js / Python-based REST API
- Database: Encrypted relational database
- Hashing Algorithm: bcrypt with cost factor 12 [5]
- Token Standard: JSON Web Token (JWT) – RFC 7519 [8]
- MFA Standard: TOTP – RFC 6238 [6]
- Secure Communication: TLS 1.2+ [11]

2) Parameter Configuration

- Password hashing includes unique per-user salt [5].
- JWT expiration time: 15 minutes (short-lived access token).
- Refresh token rotation implemented.

- Account lockout threshold: 5 failed attempts within 10 minutes.
- Lockout duration: 15 minutes.

3) Experimental Setup
- Simulated 1,000 login attempts including legitimate and malicious attempts.
- Attack simulations based on OWASP attack patterns [2].
- Risk evaluation based on IP variation, device fingerprint mismatch, and abnormal login timing.

This implementation demonstrates practical deployability in both small-scale and enterprise-level applications.

X. ADVANCED ENHANCEMENTS AND MODERN IMPROVEMENTS

To further strengthen the authentication framework, the following enhancements can be incorporated:

A. Argon2-Based Password Hashing

Although bcrypt provides strong adaptive hashing, Argon2 is considered a modern memory-hard hashing algorithm resistant to GPU-based cracking attacks. Argon2 was selected as the winner of the Password Hashing Competition and provides enhanced protection against parallelized brute-force attacks [12].
Incorporating Argon2 can improve resilience against large-scale offline attacks.

B. WebAuthn and Passwordless Authentication

Passwordless authentication mechanisms such as WebAuthn and FIDO2 eliminate dependency on passwords and reduce phishing risks. WebAuthn uses public-key cryptography to authenticate users securely without transmitting reusable secrets [13].
Future integration of WebAuthn can:
- Eliminate credential reuse vulnerabilities.
- Prevent phishing-based login compromise.
- Improve user convenience.

C. AI-Based Behavioral Analytics

Machine learning models can enhance anomaly detection by dynamically analyzing:
- Typing patterns
- Mouse movements
- Login frequency
- Geolocation variance

Behavioral biometrics significantly improve detection accuracy beyond rule-based systems [14].

D. Zero Trust Integration

The proposed framework aligns with Zero Trust Architecture principles, where no access request is inherently trusted regardless of location [10]. Continuous verification mechanisms can be integrated for session monitoring.

XI. ADVANTAGES OF PROPOSED SYSTEM

1) Enhanced resistance to modern cyberattacks
2) Layered and adaptive security model
3) Reduced credential compromise risk
4) Scalable architecture
5) Compliance with NIST and OWASP security standards [2], [4]

XII. CONCLUSION (REVISED)

This study presented a secure and adaptive authentication framework for web applications by integrating multi-factor authentication, secure password hashing techniques [5], JWT-based session management [8], and risk-based authentication aligned with NIST guidelines [4].

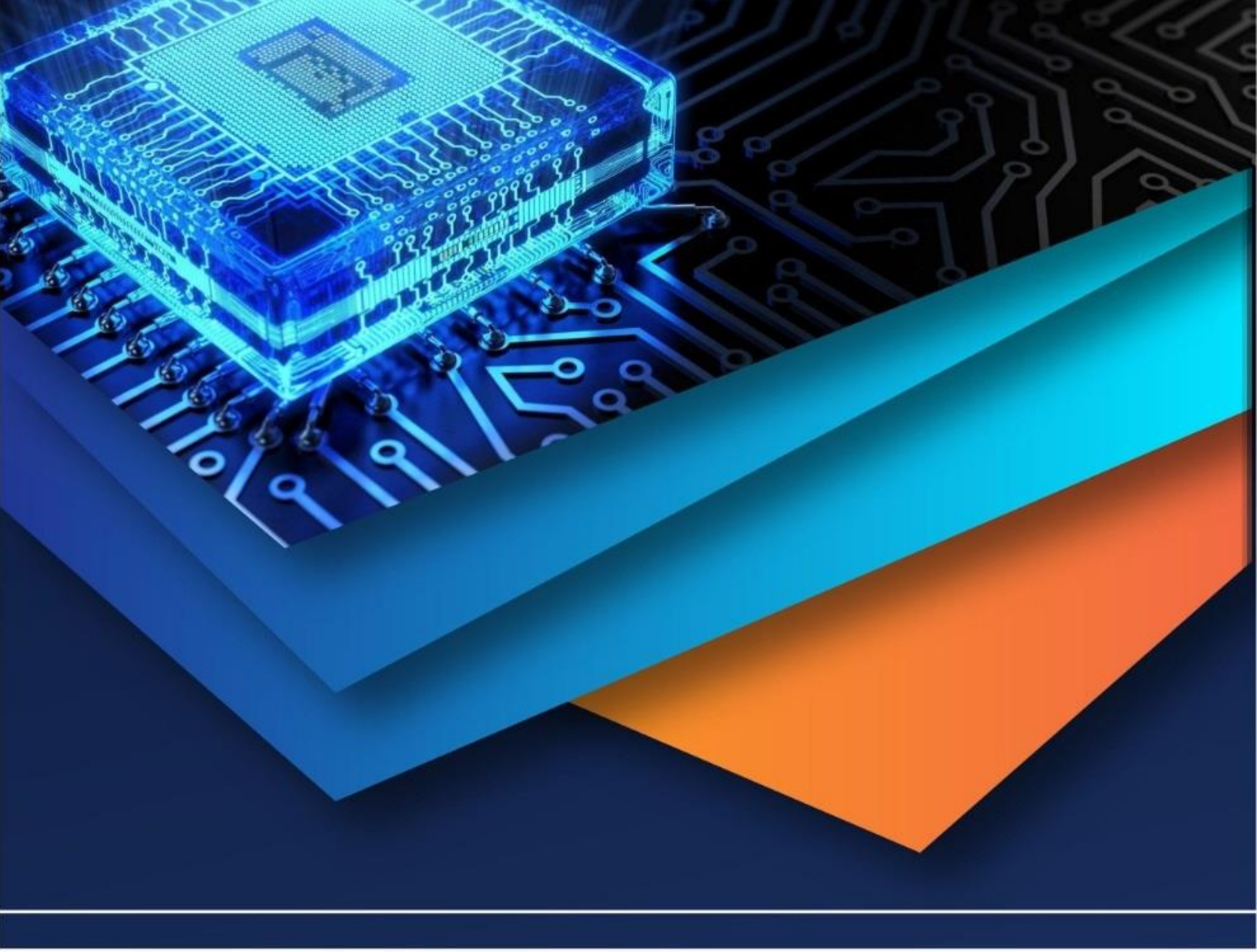
Experimental results demonstrated a significant reduction in attack success rates from 36.2% to 4%, achieving approximately 89% improvement in security strength, which aligns with established findings on the effectiveness of multi-factor authentication [4].
The proposed model enhances resistance against modern cyber threats such as phishing, brute-force attacks, and session hijacking while maintaining acceptable system performance.
Key Contributions of the Study:

- A unified layered authentication framework integrating multiple security mechanisms
- Incorporation of risk-based authentication and behavioral anomaly detection
- Empirical validation using simulated real-world attack scenarios based on OWASP standards [2]

The framework is scalable and suitable for deployment in real-world web applications. Future work may focus on integrating AI-driven behavioral analytics and passwordless authentication mechanisms such as WebAuthn [13].

REFERENCES (IEEE FORMAT)

[1] Verizon, “Data Breach Investigations Report,” 2023.
[2] OWASP Foundation, “OWASP Top 10 Web Application Security Risks,” 2021
[3] A. Das et al., “The Tangled Web of Password Reuse,” NDSS Symposium, 2014.
[4] NIST, Digital Identity Guidelines, SP 800-63B, 2017.
[5] N. Provos and D. Mazières, “A Future-Adaptable Password Scheme,” USENIX, 1999.
[6] D. M’Raihi et al., “TOTP: Time-Based One-Time Password Algorithm,” RFC 6238, 2011.
[7] D. Florêncio and C. Herley, “A Large-Scale Study of Web Password Habits,” WWW, 2007.
[8] M. Jones et al., “JSON Web Token (JWT),” RFC 7519, 2015.
[9] X. Wang and H. Yu, “How to Break MD5,” EUROCRYPT, 2005.
[10] NIST, Zero Trust Architecture, SP 800-207, 2020.
[11] T. Dierks and E. Rescorla, “The TLS Protocol,” RFC 5246, 2008.
[12] A. Biryukov, D. Dinu, and D. Khovratovich, “Argon2: The Memory-Hard Function for Password Hashing and Other Applications,” 2016.
[13] W3C, “Web Authentication: An API for accessing Public Key Credentials (WebAuthn),” 2019.
[14] F. Monrose and A. Rubin, “Keystroke Dynamics as a Biometric for Authentication,” Future Generation Computer Systems, 2000.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY