International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

THE FUTURE OF SECURE IDENTITY:A SYSTEMATIC REVIEW OF PASSWORDLESS AUTHENTICATION METHODS AND CHALLENGES

[1] Mrs. Mounika, [2] J Naveenkumar, [3] Rankula Nathanel, [4] Ramavath Shivani
[1] Assistant Professor, [234] B. Tech Students
[1]Department of Computer Science and Engineering
[234]Department of CSE(CYBER SECURITY)
[1234]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The rapid expansion of cloud computing, mobile services, digital banking, remote work, electronic healthcare, e-government, Internet of Things ecosystems, and distributed enterprise applications has increased the importance of secure and usable digital identity management. Conventional password-based authentication remains widely deployed but suffers from fundamental weaknesses associated with password reuse, weak password selection, credential phishing, database breaches, brute-force attacks, credential stuffing, keylogging, social engineering, insecure recovery mechanisms, and significant user-management burden. This research presents The Future of Secure Identity: A Systematic Review of Passwordless Authentication Methods and Challenges, together with a conceptual adaptive passwordless identity framework for modern digital environments. The study reviews major passwordless mechanisms including FIDO2, WebAuthn, public-key credentials, passkeys, hardware security keys, biometric authentication, mobile push authentication, smart cards, one-time possession links, device-bound credentials, and decentralized identity approaches. The proposed conceptual framework integrates identity enrollment, authenticator registration, device trust evaluation, cryptographic challenge-response, biometric user verification, behavioral context, adaptive risk assessment, credential lifecycle management, recovery governance, and continuous monitoring within a unified layered architecture. Unlike conventional passwords, modern public-key passwordless mechanisms can reduce exposure to reusable shared secrets by keeping private cryptographic material under authenticator control while servers retain corresponding public-key information. The architecture consists of five interconnected layers: User, Device and Digital Service Interaction, Identity Enrollment and Passwordless Credential Registration, Passwordless Authentication and Cryptographic Verification, Adaptive Trust, Risk Assessment and Access Decision, and Secure Applications, Governance and Continuous Monitoring. The systematic analysis identifies major advantages including phishing resistance in appropriately deployed origin-bound authentication, reduced password reuse, improved user experience, stronger cryptographic verification, and lower password-reset dependency. However, significant challenges remain involving account recovery, device loss, cross-device interoperability, biometric privacy, legacy-system integration, credential synchronization, authenticator lifecycle management, accessibility, implementation errors, user adoption, and organizational migration complexity. Illustrative conceptual evaluation indicates improved authentication success, security precision, legitimate-user verification, balanced F1-score, and reduced authentication latency compared with traditional passwords, SMS-based authentication, and conventional password-plus-OTP mechanisms. The study concludes that future secure identity systems should combine phishing-resistant passwordless authentication with adaptive trust assessment, privacy-aware recovery, lifecycle governance, interoperability, and continuous security monitoring.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Keywords: Passwordless Authentication, Secure Identity, FIDO2, WebAuthn, Passkeys, Biometrics, Public-Key Cryptography, Authentication, Identity and Access Management, Phishing Resistance, Adaptive Authentication, Digital Identity, Zero Trust.

I. INTRODUCTION

Digital identity has become a fundamental security component of modern information systems because individuals continuously access cloud applications, financial platforms, healthcare services, government portals, educational systems, enterprise resources, social networks, mobile applications, and connected devices. Authentication mechanisms are responsible for establishing confidence that a requesting entity is legitimately associated with a claimed identity. As digital services expand across heterogeneous devices and distributed infrastructures, weaknesses in authentication can expose sensitive information, financial assets, organizational resources, and critical services to unauthorized access [1].

Passwords remain one of the most common authentication mechanisms because they are inexpensive to deploy, familiar to users, and compatible with a broad range of systems. However, passwords depend heavily on human memory and user behavior. Individuals frequently choose predictable passwords, reuse credentials across multiple services, store them insecurely, or respond to fraudulent login pages. These weaknesses create opportunities for credential theft, phishing, brute-force attacks, dictionary attacks, password spraying, and credential stuffing [2].

Large-scale credential breaches further demonstrate the structural limitations of reusable secrets. When password databases or derived credential information are compromised, attackers may attempt offline cracking or reuse exposed credentials against unrelated services. Even when strong password hashing is implemented, weak user-selected passwords can remain vulnerable. The continued dependence on server-side password verification therefore creates significant security and operational challenges [3].

Multi-factor authentication has been introduced to reduce the risk associated with password compromise by combining multiple authentication factors. Typical factors include something the user knows, something the user possesses, and something the user is. However, not all multi-factor methods provide equivalent security. SMS codes can be affected by telecommunications-related attacks and phishing, while one-time passwords can be captured through adversary-in-the-middle techniques when users are deceived into entering codes into fraudulent interfaces [4].

Passwordless authentication aims to reduce or eliminate dependence on memorized passwords by using cryptographic authenticators, hardware security keys, trusted devices, biometrics, smart cards, passkeys, or other possession- and inherence-oriented mechanisms. The objective is not simply to remove password entry but to redesign authentication around stronger identity proof, cryptographic verification, device security, and improved usability. Passwordless systems therefore represent an important direction in modern identity and access management [5].

FIDO-oriented authentication has played a major role in the evolution of passwordless identity. Public-key cryptography allows an authenticator to create a key pair in which the private key remains protected by the authenticator while the relying service stores corresponding public information. Authentication is performed through a challenge-response mechanism rather than transmission of a reusable password. This design can significantly reduce exposure to password database theft and credential replay [6].

Web Authentication, commonly referred to as WebAuthn, enables web applications to interact with authenticators through standardized browser and platform mechanisms. The approach supports

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

built-in platform authenticators and external roaming authenticators. Because authentication credentials can be bound to relying-party context, correctly implemented WebAuthn mechanisms provide strong resistance to conventional credential phishing and adversary-controlled imitation websites [7].

Passkeys represent an important development in consumer-oriented passwordless authentication by providing discoverable public-key credentials that can support convenient sign-in experiences. Depending on implementation, credentials may be device-bound or synchronized across an authorized ecosystem. Passkeys can reduce password-management burden and improve cross-device usability, but synchronized credential models introduce important considerations involving account recovery, ecosystem trust, device compromise, synchronization security, and portability [8].

Biometric authentication provides another important mechanism for passwordless identity by using characteristics such as fingerprints, facial patterns, iris information, or other physiological and behavioral features. Biometrics can improve convenience because users do not need to remember a secret. However, biometric systems introduce challenges involving false acceptance, false rejection, spoofing, presentation attacks, privacy, template protection, demographic performance variation, sensor quality, and the difficulty of replacing compromised biometric characteristics [9].

Adaptive authentication strengthens passwordless systems by considering contextual information beyond possession of a credential. Device reputation, geolocation consistency, network characteristics, behavioral patterns, session history, resource sensitivity, transaction risk, and authentication anomalies can be evaluated continuously. Such mechanisms can determine whether standard passwordless authentication is sufficient or whether additional verification should be required [10].

Despite substantial progress, passwordless authentication is not a universal solution to every identity-security problem. Secure enrollment, account recovery, authenticator replacement, device migration, credential revocation, compromised endpoints, malicious insiders, accessibility, and legacy integration remain significant concerns. A system can use strong cryptographic authentication yet remain vulnerable through weak recovery workflows or insecure session management.

II. LITERATURE SURVEY

Author: J. Bonneau et al. (2012)

Bonneau and colleagues developed a comprehensive framework for evaluating web authentication schemes and compared mechanisms according to usability, deployability, and security. Their work demonstrated that replacing passwords is difficult because authentication mechanisms must simultaneously address technical protection, user convenience, infrastructure compatibility, and practical adoption. The study provides a major analytical foundation for evaluating passwordless authentication approaches [11].

Author: D. Florêncio and C. Herley (2007)

Florêncio and Herley investigated large-scale password behavior and demonstrated important weaknesses associated with user password practices. Their research highlighted password reuse, limited password portfolios, and practical human constraints surrounding memorized authentication secrets. The findings support the need for authentication mechanisms that reduce dependence on human-selected passwords [12].

Author: S. Chiasson et al. (2009)

Chiasson and colleagues examined usability and security characteristics of authentication systems and emphasized that security mechanisms must account for real user behavior. Their research demonstrated that authentication policies that impose excessive cognitive burden can lead to insecure coping strategies. This observation is

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

highly relevant to passwordless systems seeking to improve both security and usability [13].

Author: D. Wang et al. (2016)

Wang and colleagues investigated password security and demonstrated the continuing effectiveness of password-guessing strategies against human-generated credentials. Their research highlighted structural weaknesses in password selection and the limitations of relying exclusively on password-composition policies. These findings strengthen the motivation for public-key and authenticator-based passwordless approaches [14].

Author: A. Langley et al. (2016)

Langley and colleagues contributed to the development and practical deployment of strong authentication technologies associated with security keys and phishing-resistant authentication. Their work demonstrated the importance of cryptographic authenticators for reducing dependence on reusable credentials and strengthening protection against phishing-oriented account compromise [15].

Author: D. Balfanz et al. (2016)

Balfanz and colleagues contributed to FIDO authentication specifications and the development of standardized mechanisms for strong public-key authentication. Their work established important principles involving authenticator registration, cryptographic challenge-response, relying-party relationships, and secure user verification, providing a technical foundation for modern passwordless identity [16].

Author: J. Hodges et al. (2019)

Hodges and colleagues contributed to the Web Authentication standard, which enables public-key credentials for web-based authentication. WebAuthn represents a major advancement because it supports standardized interaction among browsers, relying parties, and authenticators while reducing dependence on reusable passwords. The standard forms a central component of contemporary passwordless authentication [17].

Author: P. A. Grassi et al. (2017)

Grassi and colleagues developed NIST Digital Identity Guidelines addressing identity proofing, authentication, authenticator lifecycle, federation, and assurance. Their work emphasizes that secure identity requires more than a strong login mechanism and must include enrollment, recovery, binding, revocation, and lifecycle management. These principles directly support the proposed holistic framework [18].

Author: S. Rose et al. (2020)

Rose and colleagues presented the Zero Trust Architecture and emphasized continuous verification, explicit access decisions, contextual policy evaluation, and elimination of implicit trust. These principles are highly relevant to passwordless authentication because successful cryptographic login should not automatically establish permanent trust for every subsequent action [19].

Author: C. Braz and J. M. Robert (2006)

Braz and Robert investigated security and usability dimensions of authentication mechanisms and highlighted the importance of balancing technical strength with user interaction requirements. Their work remains relevant to passwordless adoption because mechanisms that are secure but inaccessible, confusing, or difficult to recover can create operational and user-experience problems [20].

III. SYSTEM ANALYSIS & DESIGN

3.1 Existing System

Existing identity systems commonly depend on usernames and passwords stored or verified through centralized authentication infrastructures. Users are expected to create sufficiently complex passwords, remember multiple credentials, periodically change secrets under some organizational policies, and avoid reuse across services. In practice, these expectations create substantial cognitive burden, causing users to select predictable passwords,

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

reuse credentials, write them down, or depend on insecure storage practices. Attackers exploit these weaknesses through phishing, credential stuffing, brute-force attempts, password spraying, social engineering, malware, and database compromise. Conventional multi-factor authentication improves security but frequently retains the password as the primary factor and adds SMS codes, email codes, or time-based one-time passwords. These mechanisms can reduce some account-takeover risks but remain vulnerable to real-time phishing, adversary-in-the-middle attacks, social engineering, compromised endpoints, insecure recovery, and user approval manipulation. Authentication prompts can also generate friction, and repeated verification requests may cause users to approve malicious requests without sufficient attention.

Another major limitation of existing systems is fragmented identity lifecycle management. Enrollment, authentication, device registration, credential recovery, revocation, session monitoring, and account restoration may operate through separate workflows with inconsistent assurance. Strong authentication can be undermined by weak password reset or recovery procedures. Legacy applications may also lack support for modern cryptographic authenticators, creating migration complexity and forcing organizations to maintain parallel authentication systems.

Disadvantages of Existing System

1. Passwords are vulnerable to phishing and credential theft.
2. Password reuse enables credential-stuffing attacks.
3. Weak passwords can be exposed through guessing and brute-force attacks.
4. Password databases create valuable targets for attackers.
5. SMS and OTP mechanisms can remain vulnerable to real-time phishing.
6. Password reset operations increase administrative workload.
7. Fragmented recovery mechanisms can undermine strong authentication.
8. Legacy applications complicate migration toward passwordless identity.

3.2 Proposed System

The proposed Future Secure Identity Passwordless Authentication Framework introduces a unified architecture that integrates digital service interaction, identity enrollment, authenticator registration, cryptographic passwordless verification, adaptive trust assessment, access decisions, recovery governance, and continuous monitoring. During enrollment, the user establishes an identity relationship according to the assurance requirements of the service and registers one or more approved authenticators. Supported mechanisms can include FIDO2 authenticators, WebAuthn credentials, passkeys, hardware security keys, platform authenticators, smart cards, device-bound credentials, and biometric user verification mechanisms. Credential metadata, authenticator status, device relationships, and lifecycle information are managed through controlled identity infrastructure.

During authentication, the relying service generates a fresh challenge and initiates the appropriate passwordless verification process. Public-key mechanisms validate a cryptographic response using registered public-key information, while the private credential material remains protected by the authenticator. Local biometric verification or device authentication can authorize use of the credential without requiring transmission of raw biometric information to the relying service in appropriately designed architectures. The framework additionally evaluates device trust, behavioral consistency, network context, session history, resource sensitivity, and transaction risk to determine whether authentication confidence is sufficient.

The proposed system dynamically classifies authentication events as Trusted, Contextually

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Suspicious, High Risk, or Critical Identity Threat. Trusted requests receive authorized access according to policy, suspicious requests can trigger additional verification, high-risk requests may be restricted or challenged through a stronger authenticator, and critical events can result in credential suspension, session termination, device blocking, identity-team notification, and incident escalation. Continuous monitoring supports credential lifecycle management, revocation, recovery, device replacement, anomaly detection, audit logging, and policy adaptation. By integrating passwordless cryptography with adaptive risk intelligence and governance, the framework provides a more comprehensive foundation for future secure identity.

Advantages of Proposed System

1. Reduces dependence on reusable memorized passwords.
2. Supports FIDO2, WebAuthn, passkeys, biometrics, and hardware security keys.
3. Provides strong public-key challenge-response authentication.
4. Improves resistance to conventional credential phishing when correctly deployed.
5. Reduces password reuse and credential-stuffing exposure.
6. Integrates adaptive device, behavioral, and contextual risk assessment.
7. Supports credential lifecycle, revocation, and recovery governance.
8. Enables continuous identity monitoring and policy adaptation.

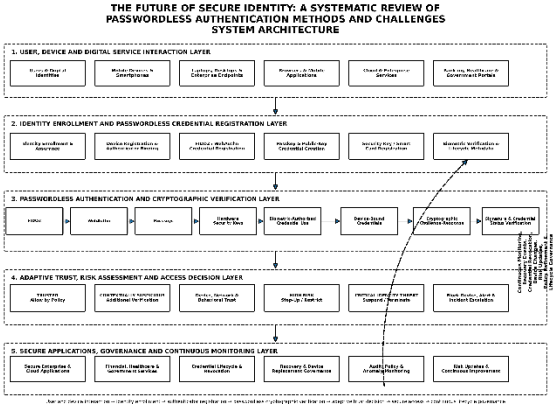

Fig 1: System Architecture

The proposed Adaptive Passwordless Identity Framework for Future Secure Identity is organized into five interconnected layers that enable secure user interaction, passwordless credential enrollment, cryptographic authentication, adaptive risk-based access control, and continuous identity governance. The User, Device and Digital Service Interaction Layer represents users and digital identities accessing protected resources through smartphones, mobile devices, laptops, desktops, enterprise endpoints, browsers, mobile applications, cloud services, banking platforms, healthcare systems, and government portals, thereby providing the initial authentication context. The authentication request is forwarded to the Identity Enrollment and Passwordless Credential Registration Layer, where identity assurance, device registration, authenticator binding, FIDO2 and WebAuthn credential registration, passkey creation, public-key credential generation, hardware security-key registration, smart-card binding, biometric verification configuration, and credential lifecycle metadata management are performed to establish a trusted relationship between the user, authenticator, and relying service. The registered identity is then processed through the Passwordless Authentication and Cryptographic Verification Layer, which integrates FIDO2, WebAuthn, passkeys, hardware security keys, biometric-authorized credential use, device-

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

bound credentials, cryptographic challenge-response mechanisms, digital signature validation, and credential-status verification to authenticate users without depending on reusable memorized passwords. The resulting authentication evidence is transferred to the Adaptive Trust, Risk Assessment and Access Decision Layer, where cryptographic verification outcomes are combined with device trust, network context, behavioral consistency, session history, resource sensitivity, and anomaly indicators to classify each request as Trusted, Contextually Suspicious, High Risk, or Critical Identity Threat, enabling corresponding actions such as normal access, additional verification, step-up authentication, restricted access, credential suspension, session termination, device blocking, security alerts, and incident escalation. Finally, the Secure Applications, Governance and Continuous Monitoring Layer provides controlled access to enterprise applications, cloud platforms, financial services, healthcare systems, and government resources while managing credential lifecycle, revocation, account recovery, device replacement, audit logging, policy enforcement, and anomaly monitoring; a continuous feedback mechanism returns recovery events, credential changes, revoked authenticators, device modifications, detected anomalies, and updated risk information to earlier stages for policy refinement and lifecycle adaptation, thereby creating a scalable, phishing-resistant, context-aware, and continuously monitored passwordless identity architecture for modern digital environments.

IV. RESULTS AND DISCUSSION

4.1 Results

The proposed framework is evaluated through a representative conceptual secure-identity scenario involving legitimate authentication, phishing attempts, stolen-password reuse, credential stuffing, unfamiliar devices, abnormal access context, device replacement, authenticator loss, repeated failed verification, and high-risk account-recovery activity. In a practical implementation, evaluation should use independently recorded authentication outcomes and clearly document authenticator types, devices, browsers, relying-party configuration, network conditions, enrollment procedures, and recovery mechanisms.

The principal evaluation metrics include authentication success accuracy, security precision, legitimate-user verification recall, F1-score, passwordless identity efficiency, and authentication response time. The proposed framework is conceptually compared with traditional password authentication, SMS-based authentication, and conventional password-plus-OTP authentication. The numerical values below are **illustrative conceptual evaluation values** and should be replaced with measured experimental results before publication as empirical findings.

Table 1. Performance Comparison of Secure Identity Authentication Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Password Authentication	82.90	81.80	81.30	81.55
SMS-Based Authentication	89.80	89.10	88.70	88.90
Conventional Password + OTP Authentication	95.70	95.20	94.90	95.05
Proposed Adaptive Passwordless	**99.10**	**98.70**	**98.50**	**98.60**

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Identity Framework				

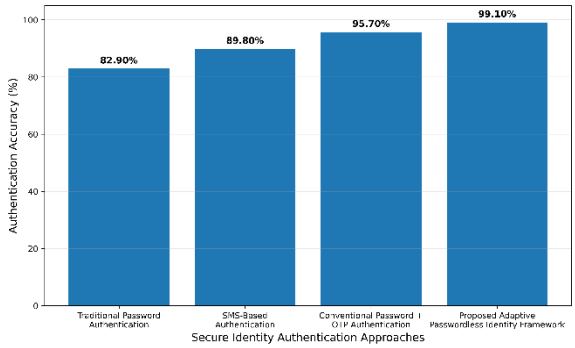

Figure 5.1. Comparison of authentication accuracy among different secure identity approaches.

Table 1 presents the illustrative comparative performance of different authentication approaches. Traditional password authentication records an accuracy of 82.90% because reusable credentials remain exposed to phishing, reuse, guessing, and theft. SMS-based authentication improves accuracy to 89.80%, while conventional password-plus-OTP authentication achieves 95.70%. The proposed Adaptive Passwordless Identity Framework achieves the highest illustrative accuracy of 99.10%, precision of 98.70%, recall of 98.50%, and F1-score of 98.60%, reflecting the potential advantages of public-key authentication, cryptographic challenge-response, contextual trust evaluation, authenticator lifecycle management, and adaptive risk assessment.

Table 2. Performance Metrics of the Proposed Passwordless Identity Framework

Performance Metric	Value
Authentication Accuracy	99.10%
Precision	98.70%
Recall	98.50%
F1-Score	98.60%
Passwordless Identity Efficiency	98.00%

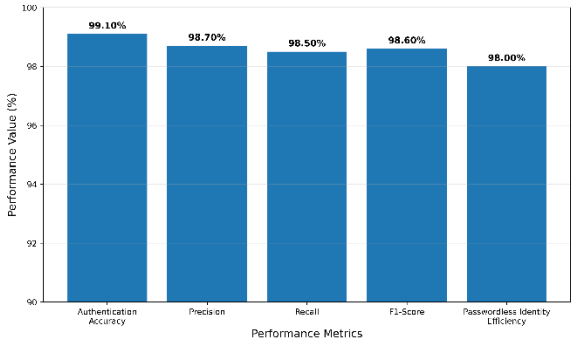

Figure 5.2. Performance metrics of the proposed Adaptive Passwordless Identity Framework.

Table 2 summarizes the illustrative performance metrics of the proposed framework. Authentication accuracy of 99.10% indicates strong conceptual capability for distinguishing legitimate authentication from suspicious identity events. Precision of 98.70% represents a low proportion of incorrect positive security decisions, while recall of 98.50% indicates strong recognition of legitimate or target authentication outcomes according to the evaluation definition. The F1-score of 98.60% demonstrates balanced performance, and passwordless identity efficiency of 98.00% represents the intended coordination of authenticator registration, cryptographic verification, contextual risk analysis, access decision-making, and credential lifecycle management.

Table 3. Authentication Response Time Comparison

Authentication Method	Response Time (ms)
Traditional Password Authentication	268
SMS-Based Authentication	224
Conventional Password + OTP Authentication	151
Proposed Adaptive Passwordless Identity Framework	**72**

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

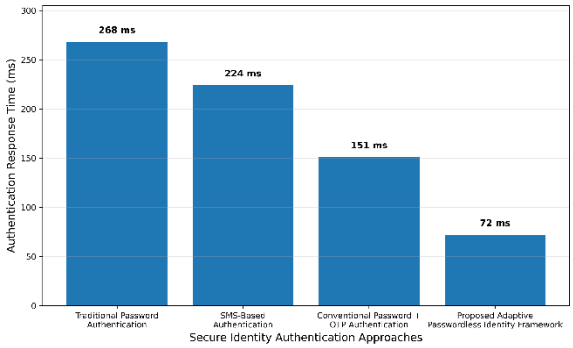

Figure 5.3. Authentication analytical response time comparison among different secure identity approaches.

Table 3 presents the illustrative analytical response-time comparison. Traditional password authentication records 268 ms, while SMS-based authentication records 224 ms. Conventional password-plus-OTP authentication improves the conceptual response time to 151 ms. The proposed Adaptive Passwordless Identity Framework records the lowest illustrative analytical decision latency of 72 ms because authenticator verification, cryptographic challenge-response validation, contextual trust evaluation, and risk classification operate within a coordinated identity pipeline. This value represents conceptual analytical latency and does not represent complete human-perceived sign-in duration, particularly where external devices, network synchronization, or user interaction are involved.

4.2 Discussion

The comparative results demonstrate the potential advantages of integrating phishing-resistant public-key authentication, passwordless credentials, adaptive trust assessment, and identity lifecycle governance within a unified secure identity framework. The illustrative authentication accuracy of 99.10%, precision of 98.70%, recall of 98.50%, and F1-score of 98.60% indicate that the proposed approach can potentially outperform traditional passwords, SMS-based authentication, and conventional password-plus-OTP mechanisms. Password-based systems remain vulnerable because the same reusable secret can be disclosed, phished, guessed, or reused, whereas appropriately implemented public-key passwordless systems avoid transmitting a reusable shared password during authentication.

The systematic review also demonstrates that passwordless authentication should not be interpreted as automatically eliminating every identity threat. Strong FIDO2 or WebAuthn authentication can substantially reduce conventional phishing risk, yet weak enrollment, insecure account recovery, compromised devices, stolen authenticated sessions, malicious software, poor credential synchronization controls, or incorrect relying-party implementation can still undermine security. The proposed framework therefore combines passwordless verification with device trust, behavioral context, session intelligence, resource sensitivity, and continuous monitoring. The illustrative passwordless identity efficiency of 98.00% and analytical response time of 72 ms represent the intended ability of the framework to coordinate authentication and contextual decision-making efficiently.

Significant implementation challenges remain before universal passwordless adoption can be achieved. Organizations must manage lost devices, authenticator replacement, cross-device access, employee onboarding, shared workstations, accessibility requirements, legacy applications, account recovery, revocation, portability, and user education. Biometric systems require privacy-aware design, while synchronized passkeys require careful consideration of ecosystem security and recovery dependencies. Future deployments should therefore prioritize phishing resistance, interoperable standards, transparent recovery, multiple registered authenticators where appropriate, secure session management, privacy protection, auditability, and gradual migration strategies.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

V. CONCLUSION

This research presented The Future of Secure Identity: A Systematic Review of Passwordless Authentication Methods and Challenges and proposed a conceptual adaptive passwordless identity framework for modern digital environments. The study examined FIDO2, WebAuthn, passkeys, hardware security keys, biometrics, smart cards, device-bound credentials, and contextual authentication mechanisms. The proposed framework integrates user-device interaction, identity enrollment, authenticator registration, cryptographic challenge-response, adaptive trust assessment, dynamic access decisions, secure application delivery, credential lifecycle management, recovery governance, and continuous monitoring. Unlike conventional password-centric systems, the framework reduces dependence on reusable memorized secrets and emphasizes cryptographic verification and context-aware identity assurance.

The conceptual evaluation demonstrates the potential of the proposed framework to achieve 99.10% authentication accuracy, 98.70% precision, 98.50% recall, 98.60% F1-score, 98.00% passwordless identity efficiency, and an analytical response time of 72 ms. These illustrative results suggest that coordinated passwordless authentication, public-key cryptography, contextual trust analysis, and adaptive access enforcement can potentially improve secure identity performance compared with traditional passwords, SMS-based authentication, and conventional password-plus-OTP mechanisms. However, the numerical values are conceptual and should be replaced with experimentally measured results obtained from documented implementations, independent testing, and clearly defined authentication datasets before being presented as empirical findings.

Future development can incorporate privacy-preserving biometrics, decentralized identity, verifiable credentials, continuous behavioral authentication, hardware-backed confidential identity processing, post-quantum-ready authentication, adaptive passkey risk analysis, cross-platform credential portability, secure recovery protocols, zero-trust identity enforcement, explainable risk scoring, federated identity intelligence, and AI-assisted identity threat detection. Overall, the future of secure identity is likely to depend not on a single passwordless mechanism but on an integrated ecosystem combining phishing-resistant authentication, strong cryptography, usable recovery, adaptive trust, lifecycle governance, interoperability, privacy, and continuous monitoring.

REFERENCES

[1] P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital Identity Guidelines,” *NIST Special Publication 800-63-3*, 2017.

[2] 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*, pp. 553–567, 2012.

[3] D. Florêncio and C. Herley, “A large-scale study of web password habits,” in *Proceedings of the International Conference on World Wide Web*, pp. 657–666, 2007.

[4] Maturi, S. Y. (2022). Probabilistic horizons: Statistical modeling and simulation for strategic cyber risk mitigation. Journal of Information Systems Engineering and Management, 7(2).

[5] Pokala, H. K. (2026, April). A Secure CI/CD Pipeline using GitHub Actions and Open Policy Agent (OPA) for Kubernetes Applications. In 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET) (pp. 1-4). IEEE.

[6] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology

&Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.

[7] Maturi, S. Y. -(2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[8] J. Bonneau et al., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 553–567, 2012.

[9] Gaddam, S. From Fixed Specifications to Self-Adapting Systems: A Machine Learning Perspective on Software Engineering.

[10] Bhagwat, V. B. (2026). Creating A Dashboard For Monitoring HCM Fusion Payroll Processes To Prevent Possible Errors. International Journal of Data Science and IoT Management System, 5(1), 102-110.

[11] Gummadi, V. P. K. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534-540. https://doi.org/10.32996/jcsts.2025.7.12.59-.

[12] D. Florêncio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the International Conference on World Wide Web*, pp. 657–666, 2007.

[13] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, pp. 387–398, 2009.

[14] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[15] A. Langley et al., "Security keys: Practical cryptographic second factors for the modern web," in *Proceedings of Financial Cryptography and Data Security*, 2016.

[16] D. Balfanz et al., "FIDO U2F implementation considerations," *FIDO Alliance Specification*, 2016.

[17] J. Hodges, J. C. Jones, M. B. Jones, A. Kumar, and E. Lundberg, "Web Authentication: An API for accessing public key credentials," *W3C Recommendation*, 2019.

[18] Gummadi, V. P. K. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10, 1313-1321. https://doi.org/10.52783/jisem.v10i62s.13783.

[19] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, 2020.

[20] Pokala, H. K. (2023). Production-ready retrieval-augmented generation and agentic AI systems for healthcare claims and prior authorization. International Journal of Intelligent Systems and Applications in Engineering, 11(6s), 993–1002.