Passwordless Authentication for Modern Digital Systems

Preethi Patel H G

Department of Computer Science, Sahyadri Science College, Shivamogga, Karnataka, India
preethipatelhg1996@gmail.com

Abstract

Password-based authentication has been the primary method for securing digital systems. However, it is more vulnerable to phishing, credential theft, password reuse, and usability issues. Recently, research has moved toward password less authentication, which replaces memorized secrets with stronger identity methods like public-key cryptography, biometrics, hardware tokens, and passkeys. This change aims to improve both security and user experience. Existing reviews show that password less authentication is gaining traction across various fields, including cloud computing, Internet of Things (IoT) environments, end-to-end encrypted (E2EE) services, and enterprise systems, where strong identity verification is crucial. In cloud and IoT ecosystems, password less methods boost authentication strength while lowering administrative complexity and improving scalability. For E2EE applications, they enable secure authentication and account recovery through recovery codes, social verification, and passkeys, all while protecting user privacy. Additionally, surveys show that combining password less authentication with multi-factor authentication (MFA), particularly through FIDO2 and biometric verification enhances protection against modern cyber attacks. Accessibility has also become an important factor. Studies show that blind and visually impaired users who rely on screen readers face significant usability and security challenges during authentication. This highlights the need for inclusive and secure login methods. Despite these advancements, widespread use of password less authentication still faces hurdles related to privacy, interoperability, standardization, regulatory compliance, and large-scale implementation. Overall, the literature indicates that password less authentication offers a promising path for future identity management by balancing security, usability, accessibility, privacy, and scalability in today's digital environments.

Keywords: Passwordless Authentication, Multi-Factor Authentication (MFA), FIDO2, WebAuthn, Passkeys, Biometrics, Public-Key Cryptography, Digital Identity, Identity Management, Cloud Security, Internet of Things (IoT), Privacy.

1. Introduction

The rapid growth of digital technologies, cloud computing, Internet of Things (IoT) devices, online services, and end-to-end encrypted (E2EE) applications has significantly increased the demand for secure and reliable user authentication. Authentication serves as the first line of defense against unauthorized access to sensitive information, digital assets, and network resources. For decades, password-based authentication has been the most widely adopted method because of its simplicity and ease of implementation. However, the increasing sophistication of cyber attacks has exposed several limitations of password-only systems. Users frequently create weak passwords, reuse the same credentials across multiple platforms, or become victims of phishing, credential stuffing, brute-force attacks, and password theft. These vulnerabilities not only compromise individual accounts but also threaten organizational security, making traditional password-based authentication increasingly inadequate for modern digital environments.

To fix these issues, experts are moving toward password less authentication. This means you don’t have to remember passwords anymore—your identity can be confirmed with things like fingerprints, face

scans, special security keys, or trusted devices you already own. These methods are much harder for hackers to break. Standards like FIDO2 and WebAuthn are helping by making sure these new ways of logging in work smoothly across different apps and devices, and are safe from phishing. Because of these benefits, password less authentication is becoming more popular as a safer and more practical option for the future.

The importance of password less authentication extends beyond improving security, as it also enhances usability and accessibility. Traditional authentication mechanisms are often designed assuming that users interact through visual interfaces, creating challenges for individuals with disabilities. Studies have shown that blind and visually impaired users who rely on screen readers frequently encounter difficulties during authentication because login instructions, state changes, and multi-device interactions are not adequately communicated by assistive technologies. These accessibility barriers may lead to authentication failures, user frustration, repeated login attempts, or even increased exposure to phishing and shoulder-surfing attacks. Consequently, authentication should not only provide strong security but also support inclusive and accessible user experiences that accommodate diverse user populations.

The need for stronger authentication is particularly evident in Internet of Things (IoT) environments, where billions of interconnected sensors, smart appliances, industrial devices, and enterprise systems continuously exchange sensitive information. Managing passwords across such large-scale and heterogeneous networks is complex, inefficient, and highly vulnerable to credential leakage and unauthorized access. Furthermore, many IoT devices have limited computational resources, making conventional authentication mechanisms difficult to implement effectively. Password less authentication offers a promising alternative by leveraging cryptographic identity verification, biometrics, and lightweight authentication protocols that provide stronger security while minimizing administrative overhead. These approaches improve scalability and support efficient identity management across diverse IoT ecosystems without compromising usability.

Similarly, the widespread adoption of end-to-end encrypted (E2EE) communication platforms and cloud-based services has introduced new authentication challenges. Unlike traditional web services, E2EE systems cannot recover encrypted user data after password or device loss because service providers do not possess decryption keys. As a result, authentication and account recovery have become closely interconnected. Modern password less solutions address these challenges by integrating passkeys, synchronized credentials, encrypted backups, recovery codes, and trusted social recovery mechanisms that allow users to regain account access while preserving privacy and maintaining strong cryptographic protection. These developments highlight the importance of designing authentication systems that balance security, usability, privacy, and recoverability.

Cloud computing environments further emphasize the need for advanced authentication mechanisms because users, applications, and services operate within distributed infrastructures that are continuously exposed to evolving cyber threats. Unauthorized access to cloud resources can result in data breaches, financial losses, and disruption of critical services. Multi-factor authentication (MFA) has significantly strengthened cloud security by combining multiple identity verification factors, thereby reducing the effectiveness of phishing, password theft, and credential reuse attacks. More recently, password less authentication has emerged as the next stage in this evolution by integrating FIDO2 standards, biometric verification, and device-based authentication to provide stronger protection while reducing user friction. This transition enables organizations to improve authentication security without sacrificing convenience or operational efficiency.

Although password less authentication offers numerous advantages, its widespread adoption continues to face several technical and organizational challenges. Issues related to interoperability across different platforms, privacy protection, regulatory compliance, deployment complexity, accessibility, device

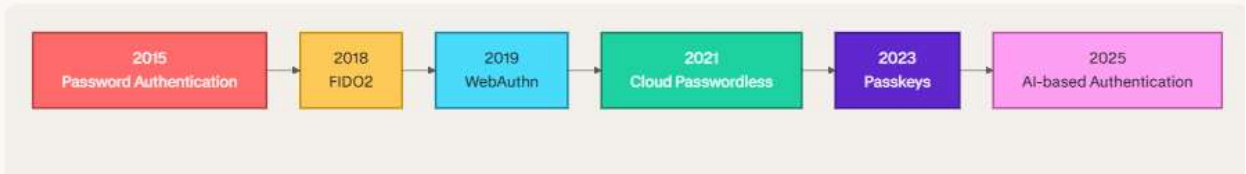
compatibility, and large-scale implementation remain active areas of research. Furthermore, no single password less technology is suitable for every application, requiring organizations to carefully evaluate security requirements, user needs, infrastructure constraints, and recovery mechanisms before deployment.

Overall, the existing literature demonstrates that password less authentication represents a significant advancement in modern identity management by addressing the limitations of traditional password-based systems while improving security, usability, accessibility, privacy, and scalability. As digital ecosystems continue to expand across cloud computing, IoT, enterprise applications, and E2EE services, password less authentication is expected to play a central role in the future of secure digital identity. This review therefore examines recent developments, technologies, applications, benefits, and challenges associated with password less authentication, providing a comprehensive understanding of its potential to transform authentication systems in modern computing environments.

1.1 Contributions of This Survey

- Presents a comprehensive review of recent advancements in passwordless authentication technologies reported between 2019 and 2025.
- Provides a comparative analysis of widely adopted authentication approaches, including biometric authentication, FIDO2, WebAuthn, passkeys, hardware security keys, and behavioral authentication.
- Explores the implementation and significance of passwordless authentication across cloud computing, Internet of Things (IoT), enterprise environments, and end-to-end encrypted (E2EE) applications.
- Highlights existing research challenges and open issues related to interoperability, user accessibility, privacy protection, and secure account recovery.
- Outlines promising research directions aimed at developing more secure, scalable, interoperable, and user-centric passwordless authentication frameworks.

1.2 Evolution of Passwordless Authentication (Timeline) (Diagram: 1)



2. Passwordless Authentication Technologies

Passwordless authentication has gained attention as a more secure and convenient alternative to traditional password-based login systems. Instead of depending on memorized secrets, it verifies users through trusted devices, biometric traits, cryptographic keys, or contextual signals. By removing passwords from the process, these methods help reduce problems such as weak passwords, credential reuse, phishing, and password theft, while also improving the user experience. Passwordless authentication is not a single technique. Rather, it refers to a group of related technologies that serve different security needs and deployment environments. The following subsections describe the main passwordless authentication technologies, their operating principles, strengths, limitations, and typical use cases.

2.1 Biometric Authentication

Biometric authentication is one of the most common passwordless approaches because it identifies users through unique physical or behavioral traits. Examples include fingerprint scanning, face recognition, iris recognition, and voice recognition. Since users authenticate with characteristics that are part of themselves, the login process is usually fast, simple, and convenient.

However, biometrics also have important drawbacks. Unlike passwords, biometric traits cannot be changed if they are exposed or misused. There are also ongoing concerns about spoofing, privacy protection, secure storage of biometric templates, and compliance with data protection regulations. For this reason, biometric methods are often paired with cryptographic techniques to improve overall security.

2.2 Public-Key Cryptography

Public-key cryptography is the basis of most modern passwordless authentication systems. Unlike password systems that rely on shared secrets, this approach uses a key pair: a private key and a public key. The private key stays securely on the user's device, while the public key is registered with the service provider. When a user logs in, they prove possession of the private key without sending sensitive credentials across the network. This greatly lowers the risk of credential interception, replay attacks, phishing, and database breaches. Because of these advantages, public-key cryptography is now a central component of passwordless authentication.

2.3 FIDO2 and WebAuthn

FIDO2 and WebAuthn are widely recognized standards for secure, phishing-resistant passwordless authentication. Based on public-key cryptography, they allow users to authenticate using platform authenticators such as smartphones and laptops, or roaming authenticators such as hardware security keys. During authentication, the private key remains on the trusted device and is never exposed to the network. This makes theft of credentials much more difficult than in traditional password-based systems. Even so, successful deployment depends on browser support, operating system compatibility, user migration planning, and organizational readiness.

2.4 Passkeys

Passkeys are a newer development in passwordless authentication that allow users to sign in with synchronized cryptographic credentials across multiple trusted devices. Unlike passwords, they provide a smoother and more secure login experience while offering strong protection against phishing and credential theft. Modern passkey systems support encrypted synchronization, secure recovery options, device migration, backup mechanisms, and social recovery features. These capabilities improve usability, but they also create challenges related to cloud dependency, device replacement, backup management, and trust relationships among users, cloud services, and providers.

2.5 Hardware-Backed Authenticators

Hardware-backed authenticators add another layer of protection by storing cryptographic keys in tamper-resistant hardware such as hardware security keys, Trusted Platform Modules (TPMs),

Secure Enclaves, and Hardware Security Modules (HSMs). Because the private key remains inside the secure hardware, these solutions provide strong resistance to malware, theft, and unauthorized access. These authenticators are especially useful in enterprise, financial, and government environments where stronger identity assurance is required. At the same time, organizations must consider issues such as deployment cost, hardware management, token replacement, and user education.

2.6 Behavioral and Continuous Authentication

Behavioral authentication is an emerging passwordless method that verifies identity by observing how a user behaves rather than relying only on login credentials. Indicators may include typing patterns, mouse movement, touchscreen gestures, walking style, and device usage habits. By checking behavior throughout a session, this approach can help detect suspicious activity and reduce the chance of account compromise. However, it also raises concerns about privacy, behavioral inconsistency, false acceptance, false rejection, and system accuracy, which still limit widespread adoption.

2.7 Adaptive and Context-Aware Authentication

Adaptive authentication improves passwordless systems by changing authentication requirements based on context. It may consider factors such as location, trusted devices, network type, login history, behavioral patterns, and overall risk level. Instead of applying the same process to every login attempt, this approach evaluates the situation and asks for extra verification only when needed. This makes authentication more secure without creating unnecessary friction for legitimate users.

2.8 Additional Passwordless Mechanisms

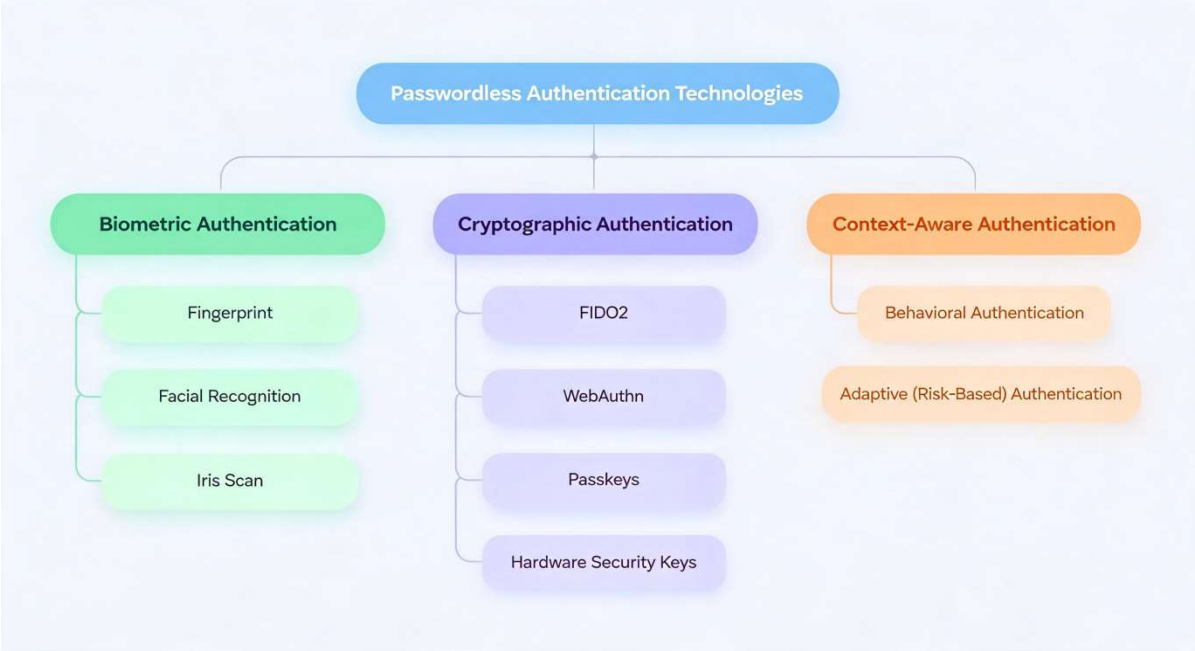
Several supporting techniques are also used in real-world passwordless deployments. These include push approval, one-time passwords (OTPs), phone-based verification, and FIDO-enabled multi-factor authentication. While these methods reduce dependence on passwords and can improve convenience, their security depends on proper implementation. Some may still be affected by phishing, SIM swapping, notification overload, or limited usability. As a result, they are often combined with stronger passwordless methods to achieve better protection.

Table-1. Here is the Comparison of passwordless Technologies

Technology	Authentication Method	Security Level	User Convenience	Advantages	Limitations	Typical Applications
Biometric Authentication	Fingerprint, Face Recognition, Iris Scan	High	High	Easy to use, eliminates passwords, quick authentication	Privacy concerns, spoofing attacks, biometric data cannot be changed if compromised	Smartphones, Banking, Enterprise Login

Technology	Authentication Method	Security Level	User Convenience	Advantages	Limitations	Typical Applications
FIDO2 / WebAuthn	Public-key cryptography with device-bound credentials	Very High	High	Phishing-resistant, no shared secrets, strong cryptographic protection	Device dependency, platform compatibility, recovery challenges	Enterprise systems, Cloud services, Web applications
Passkeys	Device-synchronized cryptographic credentials	Very High	Very High	Password-free login, seamless synchronization, improved usability	Device loss, credential synchronization and recovery issues	Consumer applications, Cloud platforms, Mobile devices
Hardware Security Keys	Physical security token (USB/NFC/Bluetooth)	Very High	Medium	Strong protection against phishing and credential theft	Additional hardware cost, loss or replacement of token	Government, Financial institutions, Enterprise security
Cryptographic Authentication	Public-private key pair	Very High	Medium	No password transmission, resistant to credential theft and replay attacks	Requires secure key management and infrastructure	Cloud computing, IoT, Secure communication
Behavioral Authentication	Typing pattern, Mouse movement, Gait, Device usage	Medium–High	High	Continuous identity verification without user intervention	Privacy concerns, accuracy and false positives	Banking, Continuous authentication, Fraud detection
Adaptive / Risk-Based Authentication	Context-aware verification using location, device, and behavior	High	High	Dynamic authentication based on risk level, improves usability	Complex implementation, depends on accurate risk assessment	Cloud services, Enterprise systems, Zero Trust Architecture
One-Time Password (OTP)	SMS, Email, Authenticator App	Medium	Medium	Simple implementation, widely supported	Vulnerable to SIM swap, phishing, delayed delivery	Banking, Two-Factor Authentication
Push Notification Authentication	Mobile device approval	High	High	Fast approval, better user experience than OTP	Requires trusted mobile device and internet connectivity	Enterprise MFA, Cloud authentication

The below Diagram help to easily understand the Flow Diagram of Passwordless Authentication Technologies (Diagram-2)



3. Literature Review

The literature on passwordless authentication demonstrates a consistent transition from traditional password-based security toward identity management systems based on stronger authentication factors such as biometrics, cryptographic credentials, hardware-backed devices, and adaptive verification mechanisms. Previous studies indicate that passwordless approaches can significantly improve resistance against common threats including phishing attacks, password reuse, credential theft, and database compromise. However, the reviewed literature also emphasizes that no single passwordless technology provides a universal solution, as each approach introduces specific security, usability, privacy, and deployment challenges.

Early research on authentication primarily focused on improving password security; however, increasing limitations associated with password-based systems encouraged the development of multi-factor and passwordless approaches. The literature shows that passwordless authentication should be considered as a broad family of technologies rather than a single replacement mechanism. Different application environments, including consumer services, enterprise systems, cloud infrastructure, and IoT networks, require different combinations of authentication factors, device trust mechanisms, and recovery strategies.

A major research direction identified in the literature is the integration of biometric authentication with cryptographic-based identity verification. Biometrics such as fingerprints, facial recognition, and other physiological characteristics improve user convenience by eliminating the need to remember passwords. However, researchers highlight concerns related to biometric privacy, template protection, spoofing attacks, and the difficulty of replacing compromised biometric information. To address these limitations,

many studies support hybrid authentication models that combine local biometric verification with cryptographic key-based remote authentication, providing both usability and stronger security assurance.

The development of FIDO2 and WebAuthn standards represents a significant advancement in passwordless authentication research. Studies highlight that FIDO-based systems improve protection against phishing by using public-key cryptography, where private keys remain securely stored on user devices and are never shared with service providers. These approaches reduce the risk of credential theft and provide stronger authentication assurance compared with traditional passwords. However, researchers also identify challenges related to ecosystem support, interoperability between platforms, user awareness, device migration, and recovery after device loss.

Accessibility has become an important consideration in recent authentication research. Earlier studies identified that user with disabilities, particularly visually impaired users, experience difficulties with authentication interfaces due to inaccessible layouts, unclear instructions, and poor compatibility with assistive technologies. Extending this area, recent research evaluates modern two-factor authentication and passwordless workflows through accessibility-focused frameworks such as AWARE. These studies reveal that even highly secure authentication mechanisms may create usability barriers when interactions depend on visual indicators, time-sensitive confirmation steps, or poorly supported screen reader functions. Therefore, authentication security improvements must be accompanied by inclusive design principles to ensure accessibility for diverse user groups.

In the context of Internet of Things (IoT) environments, the literature identifies passwordless authentication as an important solution for addressing identity management challenges. Traditional password mechanisms are often unsuitable for IoT devices due to limited computational resources, large-scale device deployment, and difficulties in password management. Survey studies propose biometrics, cryptographic authentication, hardware-backed identity, and trusted device mechanisms as effective approaches for improving IoT security. Research on smart-home and edge-IoT systems further demonstrates the practical implementation of passwordless methods by combining smartphone-based identification, biometric verification, and device authentication. These studies indicate that passwordless solutions can provide both improved security and enhanced user convenience in real-world IoT applications.

Beyond IoT environments, passwordless authentication has also gained significant attention in cloud computing and enterprise security. Literature surveys on cloud infrastructure security show a clear evolution from password-based authentication toward layered identity protection using multi-factor authentication (MFA), FIDO2, biometrics, and adaptive risk-based authentication. These studies highlight that passwordless mechanisms can strengthen cloud security by reducing dependence on reusable credentials while maintaining efficient user access. However, successful implementation requires careful consideration of device lifecycle management, authentication recovery processes, regulatory requirements, and organizational readiness.

Recent research also examines passwordless authentication within end-to-end encrypted (E2EE) services and modern web platforms. These studies extend the focus beyond authentication alone and analyze the complete identity lifecycle, including registration, login, recovery, Reauthentication, and cross-device continuity. The literature indicates that passwordless adoption depends not only on authentication strength but also on how securely users can recover accounts, migrate credentials, and maintain trust across multiple devices. This highlights the importance of designing authentication systems that balance security, usability, and long-term identity management.

Another important theme identified in the literature is the role of hardware-backed authentication mechanisms, including security keys ,secure elements, trusted execution environments, and smart cards. These technologies provide strong protection by storing authentication credentials within secure hardware components, reducing exposure to malware and credential theft. Nevertheless, researchers acknowledge practical challenges such as hardware cost, deployment complexity, replacement procedures, and user acceptance.

The literature also discusses emerging approaches such as behavioral and continuous authentication, which evaluate user identity based on behavioral patterns, device usage, and contextual information. These approaches aim to provide continuous trust verification rather than relying only on a single login event. Although promising, researchers identify challenges related to accuracy, privacy, fairness, and false acceptance or rejection rates. Adaptive authentication frameworks address some of these limitations by combining multiple signals, including device state, user behavior, location, and risk assessment, to dynamically determine authentication requirements.

Overall, the reviewed literature demonstrates that authentication research has progressed from improving password strength toward developing comprehensive identity management architectures. Passwordless authentication, supported by biometrics, cryptographic authentication, FIDO2/WebAuthn, hardware-backed credentials, and adaptive security models, provides significant advantages in reducing phishing risks, improving usability, and strengthening digital identity protection. However, successful adoption depends on addressing challenges related to privacy, accessibility, interoperability, recovery mechanisms, device dependency, and organizational implementation. Therefore, current research trends suggest that the future of authentication will rely on flexible, multi-layered, and context-aware passwordless systems rather than a single replacement technology.

4. Research Gaps

Although passwordless authentication technologies have advanced significantly and provide improved protection against phishing, credential theft, and password-related attacks, the reviewed literature reveals several unresolved challenges that limit their widespread adoption. Existing research demonstrates that passwordless authentication is not only a technical security problem but also a broader system design challenge involving interoperability, privacy, usability, recovery, accessibility, and operational deployment.

One of the major research gaps identified across the literature is the lack of interoperability among different passwordless authentication ecosystems. Modern authentication solutions involve multiple platforms, including operating systems, browsers, mobile devices, hardware authenticators, and identity providers. However, differences in implementation standards, credential storage mechanisms, synchronization methods, and recovery processes create inconsistent user experiences and limit seamless adoption. Future research needs to focus on standardized frameworks that enable secure and reliable authentication across heterogeneous platforms and service environments.

Another significant gap relates to privacy protection, particularly for biometric-based authentication systems. While biometrics improve convenience and reduce dependence on passwords, biometric characteristics such as fingerprints and facial features cannot be replaced once compromised. Existing studies highlight the need for stronger biometric template protection, privacy-preserving authentication methods, secure storage mechanisms, user consent management, and regulatory compliance frameworks to prevent misuse of sensitive identity information.

The literature also identifies challenges associated with large-scale deployment and migration from password-based systems to password less architectures. Many organizations continue to depend on passwords as fallback mechanisms due to concerns regarding implementation cost, user acceptance, legacy system compatibility, and operational complexity. Further research is required to develop practical migration strategies that allow organizations to transition gradually toward password less-first environments without disrupting existing services or reducing security.

User recovery and account restoration remain important unresolved issues in passwordless authentication. Unlike traditional passwords, where users can request a reset, passwordless systems depend heavily on devices, cryptographic keys, and trusted authenticators. Device loss, hardware failure, biometric recognition errors, or credential synchronization problems may prevent legitimate users from accessing their accounts. Current recovery approaches, including recovery codes, trusted contacts, and social recovery mechanisms, vary significantly across systems and require further investigation to achieve a balance between security, privacy, and usability.

Accessibility represents another critical research gap that has received limited attention in passwordless authentication studies. Although authentication methods may provide strong security guarantees, they may fail to support users with disabilities when workflows depend on visual notifications, time-sensitive interactions, or poorly designed assistive technology interfaces. Research involving screen reader users demonstrates that authentication challenges often arise from unclear audio instructions, inconsistent interface behavior, notification overload, and synchronization issues between multiple devices. A major limitation in current research is the lack of end-to-end accessibility evaluation of passwordless authentication workflows across realistic device combinations, including computers, smartphones, and hardware authenticators.

Furthermore, existing authentication research often evaluates security and accessibility separately rather than considering them together. A system may successfully prevent phishing or credential theft while still creating usability barriers that increase user errors or encourage insecure workarounds. Therefore, future studies should develop integrated evaluation frameworks that consider security assurance, accessibility, usability, and user behavior simultaneously.

In IoT environments, the literature identifies additional challenges due to the diversity and limitations of connected devices. IoT systems differ significantly in computational capability, communication protocols, storage capacity, and user interaction models, making it difficult to develop universal passwordless authentication solutions. Existing studies highlight the need for comprehensive evaluation frameworks that assess security performance, resource requirements, scalability, and usability under different IoT scenarios.

Interoperability and privacy preservation are particularly important gaps in IoT identity management. IoT ecosystems often involve devices from multiple manufacturers and operate across different networks and platforms. Current passwordless approaches are frequently designed for specific environments rather than heterogeneous IoT infrastructures. Future research should explore secure cross-platform identity management approaches that maintain privacy while reducing implementation complexity. Additionally, privacy-preserving mechanisms are required to protect biometric information, device identities, and authentication credentials from unauthorized access.

Research on end-to-end encrypted (E2EE) services highlights another important gap related to identity recovery and lifecycle management. Since service providers often cannot directly access user credentials

in E2EE systems, account recovery becomes a complex challenge. Existing approaches range from recovery codes to social or threshold-based recovery mechanisms, but there is still no widely accepted solution that provides strong security while maintaining usability. Future work should investigate reliable recovery architectures that support device replacement, multi-device access, and secure credential restoration.

Another limitation identified in the literature is the gap between academic research and real-world deployment. Many proposed passwordless authentication models demonstrate strong theoretical security properties but are not evaluated under practical conditions involving large-scale deployment, user behavior, organizational constraints, and commercial service requirements. Studies comparing academic proposals with real-world adoption indicate the need for more deployment-oriented research that considers operational challenges and user expectations.

Cloud authentication research similarly identifies gaps in evaluating passwordless and multi-factor authentication systems using comprehensive criteria. Existing studies often focus primarily on security effectiveness, while fewer consider usability, deployment cost, recovery processes, interoperability, and long-term operational management together. Future research should develop unified assessment frameworks that help organizations select appropriate authentication approaches based on their security requirements and practical constraints.

Overall, the literature indicates that passwordless authentication has progressed beyond simply replacing passwords and has become a broader identity management challenge. Future research should focus on developing secure, interoperable, privacy-preserving, accessible, and scalable authentication architectures. A successful passwordless ecosystem will require integration of cryptographic security, biometric protection, recovery mechanisms, accessibility standards, and real-world deployment considerations to achieve both strong security and practical usability.

5. Future Directions

The future of passwordless authentication will likely be more flexible, smarter, and better at protecting privacy. Instead of depending on just one solution, future systems will probably combine several methods such as biometrics, cryptographic keys, hardware security, and context-based checks. The main idea is to make login both secure and easy to use.

One major direction is combining biometrics with cryptographic authentication. Biometrics can make logging in faster and more convenient, while technologies like FIDO2 and WebAuthn can protect against phishing and stolen credentials. When these are used together with secure hardware and device verification, they can create a system that is both strong and user-friendly. Future research should also improve the privacy of biometric data so that it cannot be easily exposed or misused.

Another important area is adaptive and continuous authentication. Today, most systems check a user only when they log in, but future systems may keep checking trust during the session. They could look at things like behavior patterns, device details, location, and risk level. Artificial intelligence may help detect unusual activity and adjust the authentication process automatically. This would improve security without making life harder for normal users.

Accessibility is another key issue. Some authentication systems still create problems for people with disabilities, especially those who depend on screen readers or assistive tools. Future systems should be

designed with these users in mind. Better audio feedback, simpler steps, less time pressure, and improved support for assistive technology would make passwordless authentication more inclusive.

Researchers also need better ways to test both security and accessibility before these systems are widely used. This would help identify problems earlier and improve the final design. Accessibility should not be treated as an extra feature; it should be part of the core design.

In IoT environments, future passwordless authentication will need to work on devices with limited power, memory, and processing ability. These systems should be lightweight, efficient, and able to scale across many connected devices. Research should focus on secure device registration, efficient cryptography, and identity management methods that work well in large IoT networks.

IoT systems may also benefit from combining device identity, biometrics, and context-aware information. For example, a trusted device could be used along with biometric verification and environmental risk signals to improve security. Decentralized identity systems may also help with trust and compatibility across IoT networks, although more research is still needed.

Account recovery is another important area. Even though passwordless systems remove passwords, users can still lose devices or face biometric failures. Future recovery methods should be secure but also practical and privacy-friendly. Good options may include trusted recovery networks, threshold-based recovery, and user-controlled identity restoration.

Cross-device use will also matter more in the future because people now use several devices in daily life. Passwordless systems will need to let users move credentials between devices safely without creating new risks. That means secure synchronization and recovery methods are essential.

Cloud and enterprise environments will also need strong passwordless systems. These should be scalable, interoperable, and resistant to phishing. They will likely combine FIDO2/WebAuthn, hardware-backed credentials, device trust checks, and adaptive authentication. At the same time, organizations will need guidance on migration, training, policy updates, and integration with existing identity systems.

Finally, future research should focus more on real-world use. Many ideas work well in theory but have not been tested enough in actual organizations or everyday situations. More studies should look at deployment, user experience, and long-term performance.

Overall, the future of passwordless authentication will probably depend on combining security, privacy, usability, and accessibility. It will likely use a mix of cryptography, biometrics, smart risk analysis, decentralized identity, and reliable recovery methods. If these challenges are handled well, passwordless authentication can become a much safer and easier way to manage digital identity.

Table 2: Passwordless Futures: Combining Biometrics, Cryptography, and Context for Secure, Inclusive Authentication

Topic	Key points	Benefits	Research / Implementation needs	Risks / Challenges

Topic	Key points	Benefits	Research / Implementation needs	Risks / Challenges
Hybrid methods	Combine biometrics, cryptographic keys, hardware, context	Stronger security and usability	Standardized integrations, interoperability	Complexity of managing multiple methods
Biometrics + crypto	Biometrics for convenience; FIDO2/WebAuthn for phishing resistance	Fast, phishing-resistant logins	Privacy-preserving biometric storage, hardware support	Biometric data misuse, device loss
Adaptive & continuous auth	Ongoing risk checks using behavior, device, location, AI	Better detection with less user friction	Robust ML models, privacy-safe telemetry	False positives, privacy concerns
Accessibility	Design for screen readers and assistive tech	Inclusive access for users with disabilities	Accessibility-first design, testing with real users	Neglecting assistive workflows, time pressure
IoT constraints	Lightweight, efficient auth for low-power devices	Scalable, secure IoT networks	Efficient crypto, secure device registration	Resource limits, diverse device capabilities
IoT combined methods	Device identity + biometrics + context-aware signals	Stronger trust across devices	Decentralized identity, cross-device protocols	Interoperability, privacy in sensor data
Account recovery	Secure, practical recovery for lost devices/biometrics	Usable recovery without weakening security	Threshold recovery, trusted recovery networks	Social-engineering, recovery misuse
Cross-device use	Safe transfer and sync of credentials across devices	Seamless multi-device experience	Secure synchronization, migration tools	Sync vulnerabilities, unauthorized device pairing
Cloud & enterprise	Scalable FIDO2/WebAuthn + device trust + adaptive checks	Phishing resistance and policy control	Migration guidance, training, integration tools	Legacy system compatibility, rollout friction
Real-world research	Deployments and long-term user studies	Evidence-based improvements	Field trials, UX and security metrics	Limited deployment

Topic	Key points	Benefits	Research / Implementation needs	Risks / Challenges
		and adoption		studies, unknown long-term issues

6. Conclusion

Passwordless authentication is emerging as a more secure and user-friendly alternative to traditional password-based systems. By relying on methods such as biometrics, cryptographic credentials, hardware security keys, and adaptive authentication, it helps reduce common risks like phishing, password reuse, and credential theft. At the same time, the reviewed literature shows that passwordless authentication is not a complete replacement on its own. Its effectiveness depends on how well it supports accessibility, privacy, interoperability, recovery, and practical deployment across different environments.

The future of authentication is likely to be built on a combination of complementary technologies rather than a single approach. For passwordless systems to succeed in the real world, they must balance strong security with ease of use and ensure that all users can access them safely, including people who rely on assistive technologies. Continued research and careful implementation will be essential for creating passwordless authentication systems that are secure, inclusive, and sustainable.

References

[1] M. I. Md Yusop, *et al*., "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, 2025.

[2] L. Tran, *et al*., "The Passwordless Authentication with Passkey Technology from an Implementation Perspective," *arXiv preprint*, 2025.

[3] Akanda, *et al*., "Broken Access: On the Challenges of Screen Reader Assisted Two-Factor and Passwordless Authentication," *Proceedings of the ACM Web Conference*, 2025.

[4] V. A. Kommuri and K. B. Shaik, "Innovative Passwordless Authentication Approaches in IoT Identity Management," *Review Journal*, 2025.

[5] Blessing, *et al*., "SoK: Web Authentication in the Age of End-to-End Encryption," *arXiv preprint*, 2024.

[6] Otta, *et al*., "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure," *Future Internet*, vol. 15, no. xx, MDPI, 2023.

[7] "Passwordless Authentication: Challenges, Current Technologies and Future Directions," *IEEE/ACM*, 2022.

[8] FIDO Alliance Researchers, "FIDO2: Moving the World Beyond Passwords," FIDO Alliance White Paper, 2021.

[9] W3C, "Web Authentication: An API for Accessing Public Key Credentials Level 1 (WebAuthn)," W3C Recommendation, Mar. 2019.

[10] D. Balfanz, "FIDO2: Passwordless Authentication with WebAuthn," Google Security Blog, 2019.

[11] A. Czeskis, *et al*., "The Security of Modern Password Expiration: An Algorithmic Framework," *IEEE Security & Privacy*.

[12] Microsoft Security Team, "Passwordless Authentication in Microsoft Azure Active Directory," Microsoft White Paper, 2021.

[13] Apple Inc., "Passkeys Overview," Apple Developer Documentation, 2023.

[14] Google, "Passkeys: Safer Sign-ins Across Devices," Google Developers Documentation, 2023.

[15] FIDO Alliance, "Passkeys: The Future of Passwordless Authentication," FIDO Alliance Technical Report, 2023.