CHALLENGES OF PASSWORD-BASED AUTHENTICATION AND THE FUTURE OF PASSWORDLESS LOGIN

Author: Soliyev Ulanbek Student of Japan Digital University
Academic Supervisor: Lochinbek Boboev PhD, Head of IT department of Japan Digital University

Abstract

Passwords have served as the primary method of user authentication for decades, protecting access to digital systems, online services, and personal information. However, the rapid growth of cyber threats has exposed significant weaknesses in password-based authentication. Weak or reused passwords, phishing attacks, credential theft, and large-scale data breaches continue to compromise millions of user accounts each year, demonstrating that traditional password systems are increasingly difficult to secure.

To address these challenges, technology companies and standards organizations have introduced passwordless authentication methods based on cryptographic credentials, biometrics, security keys, and multi-device authentication. Solutions such as passkeys, developed under the FIDO2 and WebAuthn standards, eliminate the need for traditional passwords while improving both security and user convenience. These technologies reduce the risk of phishing attacks and credential reuse by replacing shared secrets with public-key cryptography.

This study examines the limitations of password-based authentication and reviews the emerging adoption of passwordless login technologies. It analyzes current authentication methods, compares their security characteristics, and discusses future directions for improving digital identity protection. The findings suggest that passwordless authentication provides a more secure and user-friendly alternative that is likely to become the dominant authentication model in future digital systems.

Keywords: Password Authentication, Passwordless Authentication, Passkeys, FIDO2, WebAuthn, Cybersecurity, Digital Identity, Authentication Security.

Introduction

Authentication is a fundamental component of modern information security, ensuring that only authorized users can access digital systems and online services. For decades, password-based authentication has been the dominant method for protecting user accounts across websites, mobile applications, banking systems, and enterprise networks. Despite its widespread adoption, traditional password authentication has become increasingly vulnerable to modern cyber threats, raising concerns about both security and usability. **[1][2]**

One of the greatest weaknesses of password-based systems is their dependence on human behavior. Many users create weak passwords, reuse the same credentials across multiple services, or fail to update compromised passwords regularly. These practices significantly increase the risk of phishing attacks, credential stuffing, brute-force attacks, and unauthorized account access. As cybercriminals continue to exploit these vulnerabilities, password-related incidents remain among the most common causes of data breaches worldwide. **[1][5]**

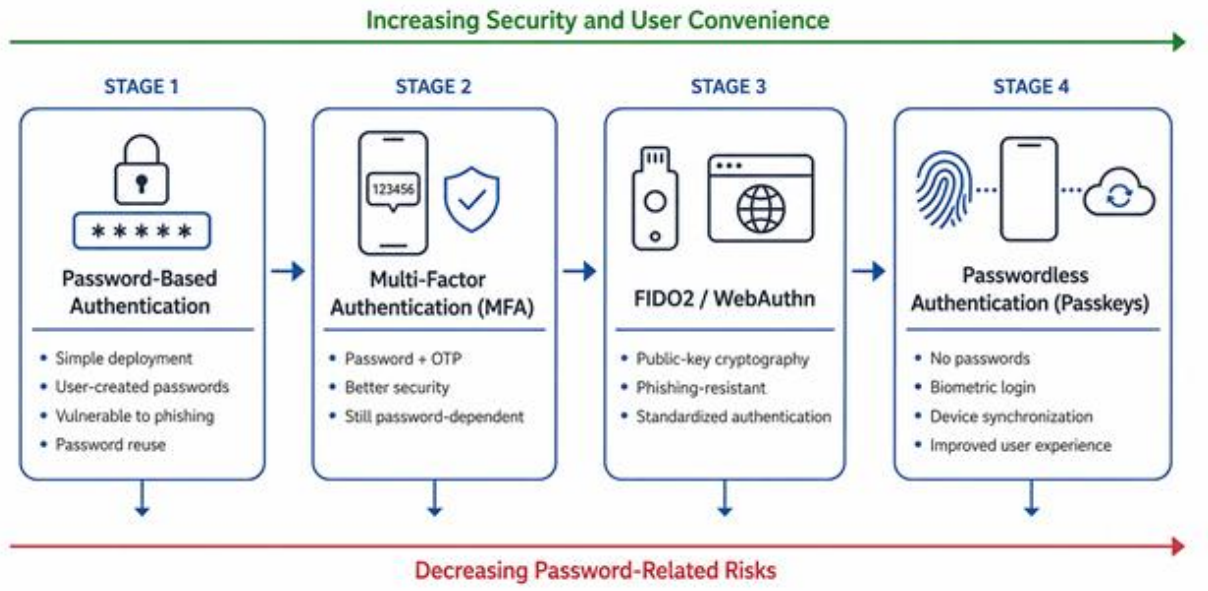
To address these limitations, technology companies and international standards organizations have developed passwordless authentication methods based on public-key cryptography. Technologies such as **FIDO2**, **WebAuthn**, and **passkeys** replace traditional passwords with cryptographic credentials stored securely on trusted user devices. These solutions improve both security and user experience by eliminating the need to remember complex passwords while providing strong protection against phishing and credential theft. **[3][4]**

Major technology providers, including Google, Microsoft, and Apple, have already integrated passwordless authentication into their products and services, signaling a significant shift in the future of digital identity management. As adoption continues to

grow, passwordless login is increasingly regarded as a practical alternative capable of reducing authentication-related cyber risks while simplifying access to online services. **[5][6]**

This study examines the challenges associated with password-based authentication and reviews the emerging role of passwordless technologies. It analyzes the security limitations of traditional passwords, compares modern authentication approaches, and discusses future directions for building more secure and user-friendly authentication systems.

Evolution of User Authentication Methods



Challenges of Password-Based Authentication

Despite being the most widely used authentication method, password-based systems have become increasingly vulnerable to modern cybersecurity threats. The security of a password depends largely on user behavior, yet many individuals continue to choose weak passwords, reuse the same credentials across multiple accounts, or fail to update compromised passwords. These practices significantly increase the likelihood of unauthorized access and account compromise. **[1][2]**

One of the most common threats is **phishing**, in which attackers deceive users into

revealing their login credentials through fraudulent emails, websites, or messages. Even strong passwords cannot protect users if they are voluntarily disclosed to malicious actors. In addition, credential stuffing attacks exploit previously leaked usernames and passwords, allowing attackers to gain access to multiple online services when users reuse the same credentials. **[1][5]**

Password management also creates usability challenges. As individuals maintain dozens of online accounts, remembering unique and complex passwords for every service becomes increasingly difficult. Many users therefore rely on simple passwords or store them in insecure ways, reducing the effectiveness of password-based security. Although password managers provide a practical solution, their adoption remains limited among the general public. **[2][6]**

Organizations also face significant costs associated with password management. Password reset requests, account recovery procedures, and help desk support consume considerable technical and financial resources. Furthermore, data breaches involving stolen credentials may result in financial losses, legal consequences, and reputational damage for both organizations and users. **[1][3]**

These limitations demonstrate that traditional password authentication is no longer sufficient to address current cybersecurity challenges. As cyber threats continue to evolve, stronger authentication methods that reduce dependence on user-created passwords are becoming essential for improving both security and user experience. **[3][4]**

Passwordless Authentication Technologies

Passwordless authentication has emerged as a modern alternative to traditional password-based login by replacing shared secrets with cryptographic credentials. Instead of requiring users to remember passwords, these systems verify identity using biometrics, security keys, or trusted devices. This approach improves both security and usability while reducing the risks associated with stolen or reused passwords. **[3][4]**

One of the most significant developments in this area is the adoption of **FIDO2** and **WebAuthn** standards. These technologies use public-key cryptography to create a unique key pair for each online service. The private key remains securely stored on the user's device, while only the public key is shared with the service provider. Since no password is transmitted or stored on the server, attackers cannot steal reusable login credentials through phishing or database breaches. **[3][4]**

A widely adopted implementation of these standards is **passkeys**. Passkeys allow users to authenticate using fingerprint recognition, facial recognition, or device PINs without entering a password. They can also be synchronized securely across trusted devices, providing a convenient login experience while maintaining strong cryptographic protection. Major technology companies, including Google, Microsoft, and Apple, have integrated passkey support into their operating systems and online services. **[5][6]**

Despite these advantages, passwordless authentication still faces several challenges. Some legacy systems continue to depend on traditional passwords, and user adoption remains gradual due to limited awareness and compatibility concerns. Organizations must also invest in updated authentication infrastructure and educate users about the benefits of passwordless technologies. **[2][5]**

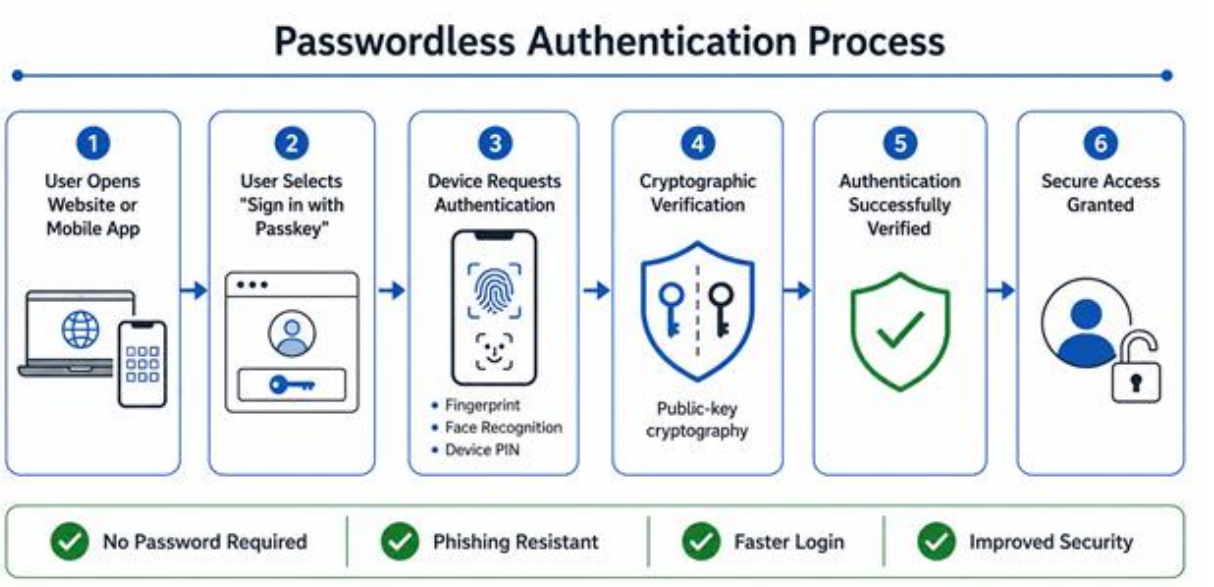
Overall, passwordless authentication represents a significant step toward improving digital identity protection. By combining strong cryptographic security with a simpler user experience, these technologies are expected to play an increasingly important role in the future of secure online authentication. **[3][6]**

Comparison Between Password-Based and Passwordless Authentication

Characteristic	**Password-Based Authentication**	**Passwordless Authentication**
Authentication Method	User-created password	**Cryptographic credentials (Passkeys/FIDO2)**
Phishing Resistance	Low	**High**

Credential Reuse Risk	High	**None**
User Convenience	Moderate	**High**
Password Management	Required	**Not Required**
Risk of Data Breaches	Higher	**Lower**
Biometric Support	Optional	**Native Support**
Overall Security	**Moderate**	**High**

Passwordless Authentication Workflow Using Passkeys



Future Challenges and Recommendations

The adoption of passwordless authentication is expected to continue growing as organizations seek stronger protection against evolving cyber threats. However, several challenges remain before passwordless login becomes the global standard. Many existing information systems still rely on legacy authentication mechanisms that

were designed around traditional passwords, making large-scale migration both technically complex and financially demanding. **[2][3]**

Another challenge is user awareness and acceptance. Although passwordless technologies simplify authentication, many users are unfamiliar with concepts such as passkeys, security keys, and public-key cryptography. Organizations should therefore provide clear guidance and educational resources to encourage adoption and reduce uncertainty during the transition from password-based systems. **[5][6]**

Interoperability is also essential for the future of passwordless authentication. Authentication methods should function consistently across different operating systems, web browsers, and mobile devices while maintaining high security standards. Continued collaboration among technology companies and standards organizations will play an important role in ensuring compatibility and improving the user experience. **[3][4]**

Future research should evaluate the long-term usability, accessibility, and security of passwordless authentication in different environments, including healthcare, education, banking, and government services. As authentication technologies continue to evolve, combining strong cryptographic protection with a simple and user-friendly experience will remain a key objective for secure digital identity management. **[1][6]**

Conclusion

Password-based authentication has protected digital systems for many years, but its effectiveness has gradually declined due to evolving cybersecurity threats and human-related vulnerabilities. Weak passwords, credential reuse, phishing attacks, and large-scale data breaches continue to expose individuals and organizations to significant security risks. These challenges demonstrate that traditional password authentication alone is no longer sufficient for modern digital environments. **[1][2]**

This study has shown that passwordless authentication technologies, including **FIDO2**, **WebAuthn**, and **passkeys**, provide a more secure and user-friendly alternative by

replacing passwords with cryptographic credentials. These technologies improve protection against phishing, simplify the authentication process, and reduce the risks associated with stolen or reused credentials. As a result, they are becoming an important component of modern digital identity management. **[3][4]**

Future progress will depend on wider adoption of passwordless technologies, improved interoperability across digital platforms, and greater user awareness of secure authentication practices. Continued collaboration among technology companies, standards organizations, and researchers will support the development of authentication systems that provide stronger security while maintaining a simple and convenient user experience. **[5][6]**

References

[1] Verizon. *2025 Data Breach Investigations Report (DBIR).* Verizon Enterprise, 2025.

[2] National Institute of Standards and Technology (NIST). *Digital Identity Guidelines (SP 800-63B): Authentication and Lifecycle Management.* Gaithersburg, MD, USA, 2024.

[3] FIDO Alliance. *Passkeys: The Future of Passwordless Authentication.* FIDO Alliance, 2024.

[4] World Wide Web Consortium (W3C). *Web Authentication: An API for Accessing Public Key Credentials (WebAuthn) Level 3.* W3C Recommendation, 2025.

[5] Microsoft. *The Passwordless Future: Secure Authentication with Passkeys.* Microsoft Security Blog, 2024.

[6] Google. *Introducing Passkeys: A Simpler and More Secure Sign-In Experience.* Google Security Blog, 2024.