Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Passwordless Authentication: A Modern Approach to Secure Access

Venkata Krishna Ramesh Kumar Koppireddy

Metmox Inc. - UV Cyber (Ultraviolet), USA

ARTICLE INFO

ABSTRACT

The concept of passwordless authentication is a revolutionary breakthrough in the field of digital security that will resolve the fundamental weaknesses in the password-dependent structure of digital security, which have plagued organizations and individual users over the years. This technical paper discusses the principles, principles, and consequences of passwordless authentication systems, which do not require users to develop, store, and handle passwords because they use alternative authentication systems. The discussion covers several passwordless authentication mechanisms, such as biometric verification, one-time passcodes, magic links, hardware, and push notifications, and each of them presents unique security properties and implementation specifications. The benefits of security are significant, with passwordless systems helping to defeat the main types of attacks: phishing, credential stuffing, brute force attacks, and also distribute authentication factors across the devices, but not centralize them in the vulnerable databases. The benefits of user experience include less cognitive load, quicker authentication time, and greater accessibility, whilst organisations find a lower IT support cost and increased operational efficiency. Some of the challenges that arise during implementation include device dependency, complexity of account recovery, difficulties in integrating the legacy systems, biometric data privacy, and resistance to use by less technologically advanced groups. The introduction of passwordless authentication into the system has to be properly planned, implemented in stages, and managed as a whole change without sacrificing the security or usability concerns. With the maturity of authentication technologies and the widespread adoption of industry standards, such as FIDO2 and WebAuthn, passwordless authentication is set to become the new standard of access control that will irrevocably change the paradigm of verification of digital identities in both enterprise and consumer settings.

Keywords: Passwordless Authentication, Biometric Verification, Multi-Factor Authentication, Credential Security, Digital Identity Management

1. INTRODUCTION

Cyber threat development is getting faster than ever, and data breaches are becoming appallingly frequent in industries. Authentication systems that are based on passwords, which were thought to be sufficient protection, are currently a major weakness for organizations and individual users. The attackers are constantly improving their techniques and are attacking the systemic vulnerabilities of the infrastructure that relies on passwords. Verizon's extensive security incident research demonstrates that stolen or compromised credentials remain the leading cause of successful breaches, highlighting why organizations must urgently reconsider their authentication approaches and adopt more robust alternatives [1]. Passwordless authentication offers a revolutionary way forward, removing the vulnerabilities embedded in password systems while making access more convenient for legitimate users. Microsoft has successfully deployed passwordless authentication for millions of consumer accounts, proving this technology works at massive scale—their security teams report faster login times and significantly stronger defenses against phishing attacks [2]. Rather than relying on passwords, this approach uses biometrics, cryptographic tokens, and time-limited codes to confirm user identity. The transformation goes beyond simple upgrades; it fundamentally changes how digital identity verification functions, moving away from knowledge-based models

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(something users know) toward possession-based and inherence-based factors (something users have or are) that offer better security with less mental effort required from users.

2. UNDERSTANDING PASSWORDLESS AUTHENTICATION METHODS

Several different technologies comprise the passwordless authentication landscape, all aimed at replacing passwords with stronger alternatives that use various authentication factors and technical implementations. Biometric authentication relies on distinctive physical traits—fingerprints, facial structure, iris patterns, voice characteristics—to confirm identity with high accuracy, utilizing advanced pattern recognition algorithms and sensor technology that has improved dramatically over recent years. Fingerprint recognition has come a long way, with current systems using sophisticated image processing and machine learning to handle differences in how people place their fingers, variations in skin condition, and environmental challenges that once made authentication less reliable [3]. These systems detect particular ridge endings and bifurcations of fingerprint patterns in conjunction with liveness checking, which prevents fraudulent attempts with fake fingers or photos. Another commonly used passwordless approach is one-time passcodes, which form temporary codes delivered either by SMS, email, or authenticator apps and expire after a single use or after a time restriction elapses, generally using time-synchronized algorithms that coordinate between servers and client devices. Magic link authentication presents an especially convenient choice, sending unique authentication URLs straight to registered email addresses so users can authenticate with a single click, no credentials or password memory required [4]. This is done by generating cryptographically secure tokens, which are installed in the URLs, which are then verified when a user accesses it on the server, and a token that is normally set to expire shortly, say within a few minutes, to prevent a response to an unauthorized request by the user should the URL be intercepted. Physical systems, such as hardware tokens, such as USB security keys and smart cards, provide physical devices that are necessary to carry out authentication, based on public-key cryptography, which stores the keys locked within a secure hardware device, making them resistant to remote attacks and phishing. Push endears are authenticated to the established mobile devices via encrypted connections, requesting the user to authorize the login requests via trusted applications, which may contain additional context such as location, device attributes, and behavioral patterns, so as to identify suspicious authentication responses. Both approaches address particular security considerations and provide varying degrees of convenience and implementation complexity, providing organizations with choices that reflect their tolerance to risks, user base, and technical infrastructure.

Authentication Method	Technology Basis	Primary Advantage	Implementation Complexity
Biometric Authentication	Fingerprints, facial recognition, iris patterns, voice signatures	High accuracy using unique physical traits	Moderate to High - requires specialized hardware
One-Time Passcodes (OTP)	Time-based algorithms synchronized between servers and devices	Temporary codes expire after a single use	Low to Moderate - works with existing infrastructure
Magic Link Authentication	Cryptographically secure tokens embedded in URLs	Simple one-click authentication process	Low - requires only email infrastructure
Hardware Tokens	USB security keys, smart cards with public-key cryptography	Physical device required, resistant to phishing	Moderate - requires token distribution and enrollment
Push Notifications	Encrypted mobile channels with contextual validation	Real-time approval with behavioral analytics	Moderate - requires mobile app integration

Table 1: Comparison of Passwordless Authentication Technologies [3, 4]

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3 SECURITY BENEFITS AND IMPROVED SECURITY

The passwordless authentication conveys significant security benefits that solve the weaknesses of password-based systems' long-standing issues. Cessation of passwords completely takes away the primary entry point that criminals have been using over the decades. Widespread adoption of passwordless technology shows impressive security gains, with organizations reporting sharp drops in compromised accounts and successful phishing attacks [5]. Phishing schemes, which have become incredibly sophisticated using social engineering, fake websites, and credential theft, lose their effectiveness when there are no passwords to steal through deceptive emails or fraudulent login pages. Many passwordless approaches use asymmetric cryptography, and therefore, even when attackers observe such communication, they cannot reuse the captured authentication attempts or obtain authentication secrets out of what they see. Credential stuffing, whereby criminals attempt to gain access to multiple services using massive databases of previously compromised usernames and passwords, would be useless in passwordless setups since a static credential is not available to reuse. Password behavior studies have revealed that over the years of password security training and the adoption of more and more complex password rules, individuals continue to create predictable passwords and reuse them on numerous accounts, which creates chain-reaction security issues where a single account is compromised, revealing numerous services to attackers [6]. Brute force attacks that try countless password combinations cannot work when passwords do not exist, since the cryptographic puzzles in passwordless systems require computational power that would take impossibly long to crack without the correct private keys or biometric data. Removing password databases also means fewer concentrated collections of authentication secrets that attract attackers, changing the threat environment by spreading authentication factors across individual devices and hardware tokens instead of storing them centrally in backend systems. The cryptographic protocols in passwordless systems provide much stronger security than static passwords through mathematical principles that make unauthorized access essentially impossible even with massive computing power, while also enabling extra security features like attestation that confirms device authenticity and detects tampering.

Security Benefit	Attack Vector Addressed	Protection Mechanism	Impact on Threat Landscape
Phishing Resistance	Social engineering, fake login pages	No passwords to steal through deception	Renders credential harvesting ineffective
Credential Stuffing Prevention	Stolen username-password database exploitation	Eliminates static credential reuse	Makes previous breach data worthless
Brute Force Immunity	Automated password-guessing attacks	Cryptographic challenges are computationally infeasible	Removes systematic attack feasibility
Database Breach Mitigation	Centralized credential storage targeting	Distributed authentication factors across devices	Reduces high-value attack targets
Replay Attack Prevention	Captured authentication attempt reuse	Asymmetric cryptography with unique challenges	Intercepted communications cannot be exploited

Table 2: Security Benefits and Attack Vector Mitigation [5, 6]

4. USER EXPERIENCE AND OPERATIONAL BENEFITS

Apart from security improvements, passwordless authentication creates significant benefits for user experience and operational efficiency, as shown through widespread enterprise use and research studies. Users no longer struggle with creating, remembering, and tracking numerous complex passwords for personal and work accounts—a problem that gets worse as people use more services and applications. Research watching how people actually use passwords in real situations has revealed major pain points, including frequent password recall failures, unsafe

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

shortcuts like writing passwords down, and frustration with password reset procedures that interrupt work [7]. Passwordless methods make authentication faster and simpler, cutting friction through biometric scans that finish in seconds or hardware token taps that need almost no effort, likely boosting user engagement and satisfaction while reducing login abandonment. For organizations, removing passwords means lower IT support costs since password-related help desk requests—password resets, account lockouts, synchronization problems—make up a big chunk of IT service desk work and labor expenses. Financial analysis of passwordless authentication shows strong returns through several channels: direct savings from fewer help desk tickets, productivity increases from faster authentication and fewer interruptions, and risk reduction from lower breach likelihood and incident response costs [8]. Streamlined authentication is also more productive for the employees in terms of total hours saved by the entire workforce because they do not have to spend a lot of time working on credentials, waiting to use passwords again, and dealing with lockouts that restrict access to key business systems. Passwordless authentication is also beneficial to those who are not able to use the traditional password entry as a hindrance, such as people with motor challenges who cannot use keyboards, vision issues that make it difficult to read complex password guidelines, or cognitive challenges that lead to the forgetting of multiple passwords. The technology also eases authentication on devices with few input options smart TVs, IoT devices, gaming systems, and car entertainment systems, where typing on the remote control or having limited interfaces are annoying experiences and frequent errors.

Benefit Category	Specific Advantage	Quantifiable Impact	Affected Stakeholders
User Convenience	Elimination of the password memory burden	Faster authentication completion	End users across all demographics
IT Support Reduction	Fewer password reset and lockout tickets	Decreased help desk workload and costs	IT service desk teams and budgets
Productivity Gains	Reduced time managing credentials	Aggregate hours saved across the workforce	Employees and organizational efficiency
Accessibility Enhancement	Alternative input methods for disabilities	Improved access for motor, visual, and cognitive impairments	Users with disabilities and special needs
Device Compatibility	Simplified authentication on limited-input devices	Better experience on IoT, smart TVs, and gaming consoles	Consumer electronics users

Table 3: Organizational and User Benefits of Passwordless Authentication [7, 8]

5. IMPLEMENTATION CHALLENGES AND CONSIDERATIONS

With many advantages, passwordless authentication brings implementation challenges that need careful handling through smart planning, gradual rollouts, and thorough change management. Device dependency creates serious problems when users lose smartphones with biometric data or authentication apps, misplace hardware security tokens, or deal with broken devices that block system access until administrators complete alternative verification. Passwordless authentication organizations experience significant design challenges in that account recovery requires a careful balance between being infused with security, ensuring that unauthorized access is not achieved, and usability that ensures that legitimate users get back in as soon as authentication factors are lost or damaged [9]. This needs robust account recovery mechanisms that are secure and convenient at the same time; they are accessible with multiple verification procedures, but commonly use alternative authentication means, identity validation, or administrative approval mechanisms that restore access without leaving any security vulnerability. Implementation gets complicated, especially for organizations with older systems built before current authentication standards, varied technology using multiple platforms and programming languages, and complex integration needs spanning local infrastructure, cloud services, and third-party applications with different levels of

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

standard support. Transition phases when passwordless and password systems run together need careful handling to avoid security gaps, maintain consistent experiences, and keep operations running while reducing confusion as users navigate different authentication methods across systems. Research on authentication evolution and ongoing challenges in moving past passwords has found basic conflicts between security and usability that keep shaping authentication design, with each new technology bringing its own compromises and implementation issues [10]. Another significant issue is the privacy concern, especially when it comes to the storage and processing of biometric data, where organizations must have another major concern when users become worried about the way the fingerprints, face scans, or other biological data are collected, saved, and potentially shared with a third party or a state institution. The cost considerations of provision of hardware tokens to a high number of users or updating hardware to handle more modern authentication may require significant investment of capital that cannot be met by small organisations, bearing in mind that full ownership cost includes purchasing of devices, enrollment systems, routine maintenance, and eventual replacement of hardware. Their adoption issues may also arise particularly with the less technologically advanced categories who do not know much about the benefits of using biometrics to enroll and to exist in the new authentication security, or those who fear change and prefer to stay with long practiced work processes that do not fully embrace change may also become a problem and organizations may have to invest a lot in user training, effective communication on the advantages of the new system and provision of supportive mechanisms to the employee to ease the transition stress.

Challenge Area	Specific Issue	Organizational Impact	Mitigation Strategy Required
Device Dependency	Lost or malfunctioning authentication devices	User lockout and access disruption	Robust account recovery mechanisms
Implementation Complexity	Legacy system integration difficulties	Extended deployment timelines and costs	Phased rollout with hybrid authentication
Privacy Concerns	Biometric data storage and processing	User anxiety and regulatory compliance	Local device storage and transparent policies
Capital Investment	Hardware token distribution and infrastructure upgrades	Significant upfront costs	Total cost of ownership assessment
User Adoption Resistance	Unfamiliarity with new authentication methods	Slower adoption rates and support burden	Comprehensive training and change management

Table 4: Implementation Challenges and Mitigation Strategies [9, 10]

CONCLUSION

Passwordless authentication is one of the most significant innovations in the field of cybersecurity that provides organizations and users with a solid alternative to the weaknesses of password-based systems that have haunted them for decades. This authentication paradigm will greatly improve the security postures by removing the use of static credentials and instead using biometrics, cryptographic tokens one one-time codes, and other innovative authentication mechanisms in addition to increasing user convenience and minimizing operational overheads. The technology is useful in combating some of the most common attack vectors, such as phishing programs, credential stuffing activities, and brute force attacks, by use of cryptographic defenses and by simply eliminating the fixed secret keys that attackers have historically used. The organizations that have adopted passwordless authentication have reported significant returns, such as the reduction of account breaches by a huge percentage, reduction in the IT support expenses as a result of fewer password-related help desk calls, increased employee productivity due to the simplification of the login process, and greater accessibility to users with disabilities or those who use a device with limited input capabilities. Nonetheless, successful implementation requires prudent consideration of the issues associated with implementation, like the dependency of the device that may pose potential access

discontinuity, privacy issues, especially with biometric data management, integration problems with the existing infrastructure, and reluctance of users to adopt new authentication methods, more so when the populace has not yet mastered the new authentication system. To implement the strategy, the choice of the right approach is necessary based on the specific security needs, user demographics, and technical infrastructure, and the creation of a set of effective account recovery techniques that are both security-wise safe and user-friendly. With the increased accuracy of biometric sensors, standardized authentication systems such as FIDO2 and WebAuthn gain wider ecosystem coverage, and most major technology platforms are starting to offer passwordless access options, this type of authentication will probably become the new standard in the access control industry. The issue regarding progressive organizations has moved beyond the question of whether or not to implement passwordless authentication to how quickly and efficiently deployment can occur, since it has become clear that the traditional password protection measures are not keeping pace with the level of cyber threats currently prevalent in the digital arena.

REFERENCES

[1] Verizon, "2025 Data Breach Investigations Report," Verizon Solutions. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] Vasu Jakkal, "The passwordless future is here for your Microsoft account.", Microsoft Security Blog, 2021. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/

[3] Davide Maltoni et al., "Handbook of Fingerprint Recognition," SpringerNature, 2009. [Online]. Available: https://link.springer.com/book/10.1007/978-1-84882-254-2

[4] Javed Shah, "What Is Magic Link Authentication? Benefits & Challenges," 1Kosmos, 2023. [Online]. Available: https://www.1kosmos.com/authentication/magic-link-authentication/

[5] RF IDEAS, "2023 State of Passwordless Security". [Online]. Available: https://www.rfideas.com/sites/default/files/2023-08/rfIDEAS_2023_State_of_Passwordless_Report_WP_702.pdf

[6] Maximilian Golla and Markus Dürmuth, "On the Accuracy of Password Strength Meters," Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018. [Online]. Available: https://dl.acm.org/doi/10.1145/3243734.3243769

[7] Sarah Pearman et al., "Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3133973

[8] Forrester, "The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory", A Forrester Total Economic Impact™ Study Commissioned By Microsoft, 2020. [Online]. Available: https://f.hubspotusercontent40.net/hubfs/2762090/M365%20SECURITY%20AUTOMATION/Docs%20%C3%A0%20t%C3%A9l%C3%A9charger/TEI%20of%20Microsoft%20Azure%20Active%20Directory.pdf

[9] Deepak Gupta, "The Economics of Authentication: Why Passwordless Pays," Authentication Security Blog, 2025. [Online]. Available: https://guptadeepak.com/the-economics-of-authentication-why-passwordless-pays/

[10] Joseph Bonneau et al., "Passwords and the evolution of imperfect authentication, "Communications of the ACM, 2015. [Online]. Available: https://dl.acm.org/doi/10.1145/2699390