Scientific Research Publishing

International Journal of Intelligence Science, 2026, 16(3), 248-258
https://www.scirp.org/journal/ijis
ISSN Online: 2163-0356
ISSN Print: 2163-0283

Measuring Adoption and Security Impact of Passwordless Authentication in Large-Scale Identity Systems

Sadab Qureshi

San Jose State University, San Jose, USA
Email: qureshi.sadab2488@gmail.com

How to cite this paper: Qureshi, S. (2026) Measuring Adoption and Security Impact of Passwordless Authentication in Large-Scale Identity Systems. *International Journal of Intelligence Science*, **16**, 248-258.
https://doi.org/10.4236/ijis.2026.163013

Received: June 30, 2026
Accepted: July 21, 2026
Published: July 24, 2026

Abstract

The number of credentials stolen is increasing steadily, largely because they are generally not changing across accounts. It has been proven that previous authentication methods were lacking. Unshared secrets still have a couple of drawbacks, so passwordless authentication is still a tantalizing option that relies on public-key cryptography, biometrics, and hardware-based authenticators to facilitate identity verification. The focus of this review is on the use pattern and measurable security impact of passwordless authentication in a scalable enterprise and consumer identity system. It highlights the theory behind the use of the TAM and how users adopt it. The usability-security ratio plays a key role in implementations. The study extrapolates from the empirical studies of practical implementations, suggesting that passwordless solutions have the potential to substantially decrease the use of traditional password-based authentication. Those sorts of credential AND password reset requests are extremely high. However, it poses interoperability issues, device administration issues, regulatory issues, and user trust issues. The next-generation concepts would include the combination of decentralized identity and artificial intelligence for flexible and scalable security positions and identity lifecycle management. Passwordless authentication is a new obsession to build a secure, easy, and scalable digital identity system.

Keywords

Authentication, Identity, FIDO2, Adoption, Cybersecurity Metrics

1. Introduction

As the most popular means of user verification in digital identities, for decades,

user verification was a password system with several issues, mostly stemming from the risk of credential dumping, password reuse, and large-scale credential breaches, as well as from the possibility of phishing attacks [1]. But even with so many holes exposed, small, medium, and large-sized organizations are struggling with continuous security issues because of poor credential security management practices and poor security practices of employees. Cloud computing, Internet of Things (IoT) devices, mobile apps, and digital distributed services are rapidly expanding in number, a growth that requires scalable, secure, and user-friendly authentication mechanisms. In this regard, among the various possibilities that are emerging, there is authentication based on a public-key cryptographic system, authentication by a biometric feature, authentication by an authentication hardware key pair, and authentication based on the authenticator located in the device. This is called passwordless authentication as it does not involve sharing of secrets. The FIDO2 and WebAuthn standards provide enhanced security and protection against phishing, credential hijacking, and replay attacks and are more convenient and efficient to use for authentication [2]. For this review, the term "large-scale identity systems" refers to enterprise, government, and consumer identity systems that are able to prove the identity of thousands to millions of users in a set of distributed identity worlds. They are the percentage changes of user/organisation between the switch from being password authenticated to passwordless, and the impact of security, which is measurable in terms of activity, for example, reduction in the number of phishing events, number of credentials stolen, number of password reset attempts, user/authentication failure, operation failure, overhead, etc. [3] [4]. A key gap in the literature is the limited empirical evidence on how passwordless authentication performs at scale in real-world settings and in multi-factor authentication (MFA) systems. This review aims to identify the adoption rates and security performance of passwordless authentication in large-scale identity solutions.

2. Review Methodology

In this research, a structured literature research method was chosen to collect a variety of literature sources related to security in the system of "without password" authentication in enterprise and consumer identity systems. Comprehensive electronic searches were conducted in IEEE Xplore, ACM Digital Library, Scopus, Springer Link, ScienceDirect, and Google Scholar, and relevant publications in the last 8 years (2018-2025) were identified. Searching was done with some of the combinations, such as passwordless authentication, FIDO2, WebAuthn, passkeys, authentication security, identity management, biometric authentication, multi-factor authentication (MFA), search for Technology Acceptance Model (TAM), search for enterprise authentication, and search for consumer identity systems. A preliminary search was made to identify ~185 publications, which was made possible by this. The full text of 112 papers was analyzed; 28 papers were duplicate studies, and 28 papers were screened on the basis of their title and abstract. Of the

publications selected, based on the inclusion/exclusion criteria, 52 were analyzed in more depth using a qualitative analysis method. The papers surveyed included presented papers from peer-reviewed journals, conference proceedings, industrial case studies, standards papers, or technical reports that provided empirical data, implementation experiences, usability studies, trends, or information about the adoption of a security outcome that has some relevance to the use of passwords. Studies that just included the traditional password system, opinion articles or editorials, duplicate studies, non-English publications, and studies where the method used was not described in enough detail to be used were excluded. Data gathered from the studies included: Deployment-Enterprise vs Consumer, Authentication Technology-FIDO2, WebAuthn, Passkeys, Windows Hello; Evaluation Methodology, Security Characteristics, Challenges Faced, and Metrics Obtained.

Studies were compiled across five themes: authentication technologies and standards, acceptance and adoption by users, measurable impacts of security, concerns during deployment and interoperability, and the directions of future studies. The studies were categorized into the following broad categories: technologies and standards for authentication, technologies and standards for user acceptance and adoption, measurable impacts of security, deployment challenges and interoperability, and future research directions. The values of **Table 1** and of **Figure 2** were synthesized; the other values, from representative results reported throughout the literature, presently in use, and from case studies in the public domain for the industry, were used for comparative analyses. These studies are not a formal meta-analysis, but rather they are listed to indicate a general trend: they had varying sizes, types of evaluation, developmental levels of evaluations, and whether they reported metrics of the evaluations. The framework approach makes it easy to ensure a clear, repeatable, and unbiased review, thereby allowing a thorough review of the state of the art, how passwordless authentication development can be implemented, and future opportunities.

3. Background and Theoretical Framework

Digital authentication has traversed amazing cycles, each of which is driven by a distinct technology. Digital authentication has come a long way over the years as cybersecurity issues have evolved, and the importance of secure digital identity credentialing has increased. For decades, for ease of use, low implementation expense, and compatibility, traditional username-and-password authentication was the prevailing method of authentication. But passwords have become a weak security measure in the face of the growing number of phishing attacks, credential stuffing, password reuse, and big data breaches [5]. To reduce these risks, organizations came up with Multi-Factor Authentication (MFA), which combines passwords with other authentication factors (one-time password (OTP), biometric, hardware security tokens, or mobile authenticators). MFA is a very good solution to prevent credential-based attacks, but it is also more complex, burdening the

admin and causing user friction, particularly in an enterprise environment with thousands or millions of users requiring access to a resource. Passwordless authentication is the next step in authentication evolution, as hidden secrets can be replaced by cryptographic credentials, which are not vulnerable to phishing and credential theft. Public-key techniques like FIDO2, WebAuthn, and Passkeys use public-key cryptography where the private part is securely kept on user devices and only the public part is registered to the service provider [6]. They use trusted representations from the area, such as biometrics or PIN codes of devices for authentication, and they don't send reusable representations over communications pathways. This design significantly decreases the potential for password cracking and provides increased ease of login, turnaround time, and efficiency during operations. Based on the Technology Acceptance Model (TAM), people's acceptance of a particular technology is mainly driven by two factors: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). Some aspects of passwordless authentication include perceived usefulness, which means users feel that the use of an authentication tool where they don't have to remember their own passwords provides them additional security, reduces authentication failure rates, increases ease of use when dealing with the management of authentication credentials, and blocks phishing attacks. The Ease of Use concept is a measure of how easily biometric authentication, passkeys, and hardware security devices are used when used normally in the system [7]. These are concepts that are applied throughout this review as a guideline for art analysis. The businesses featured in Section 4 prove that companies that saw fewer password resets, less complex management, and higher phishing protection had a higher adoption rate. Likewise, seamless authentication experiences and the lack of doubts in device-bound credentials have a positive impact on usage, as seen by consumer deployments. Yet privacy concerns, loss of interoperability and recovery of credentials, and device limitations have lowered the perceived value and trust, despite the technical advantages of the passwordless authentication paradigm, reducing the uptake of implementations. As seen in **Figure 1**, over the years, different kinds of authentication technologies have evolved, starting with passwords and moving to multi-factor authentication, and on to the newer passwordless authentication technologies. It illustrates the gradual development from knowledge-based authentication techniques to more cryptographic, biometric, and hardware-based authentication techniques to address increasing security demands, user-friendliness, and scalability requirements for enterprise and consumer identity systems.

While not using TAM is the first concept to keep in mind when implementing the concept of no password, there's another concept that can't be overstated: usability. The authentication mechanisms need to be secure enough not to be a burden on cognitive load, as well as the amount of time or effort it takes to log in to the system, and would need to be easily recoverable in case of lost device/replacement of authentication elements. Empirical research has shown that passwordless authentication can help decrease password reset rates [8] and the time needed to

fulfill the authentication process, increase satisfaction among users, and is less tedious than the traditional password authentication process. But true deployment challenges include cross-platform support, dealing with the various legacy systems, recouping credentials (when lost), putting hardware in place, and local legislation. They are different challenges, depending on the context: enterprise: access to locking is less of a focus than it should be; it's more about being efficient and useful to them; consumer: less about locking than it should be about being convenient and being usable; it's about privacy and about syncing cross devices. Technically robust deployment integrity is acceptable; however, the scale of deployment, user interest, and organization readiness play significant roles in deployment considerations. The user authentication schemes used have changed from simple password-based schemes to schemes that involve some cryptographic elements, or schemes that require no password, and have gotten more involved in what they consider the "right" level of security, all the while maintaining some reasonable level of usability and operating efficiency, as in Figure 1. These are "flavored" views and concepts which provide the context to interpret the conceptualization of the process of enterprise and consumer adoption of the patterns discussed in Section 4 and the measurement of security outcomes in Section 5.

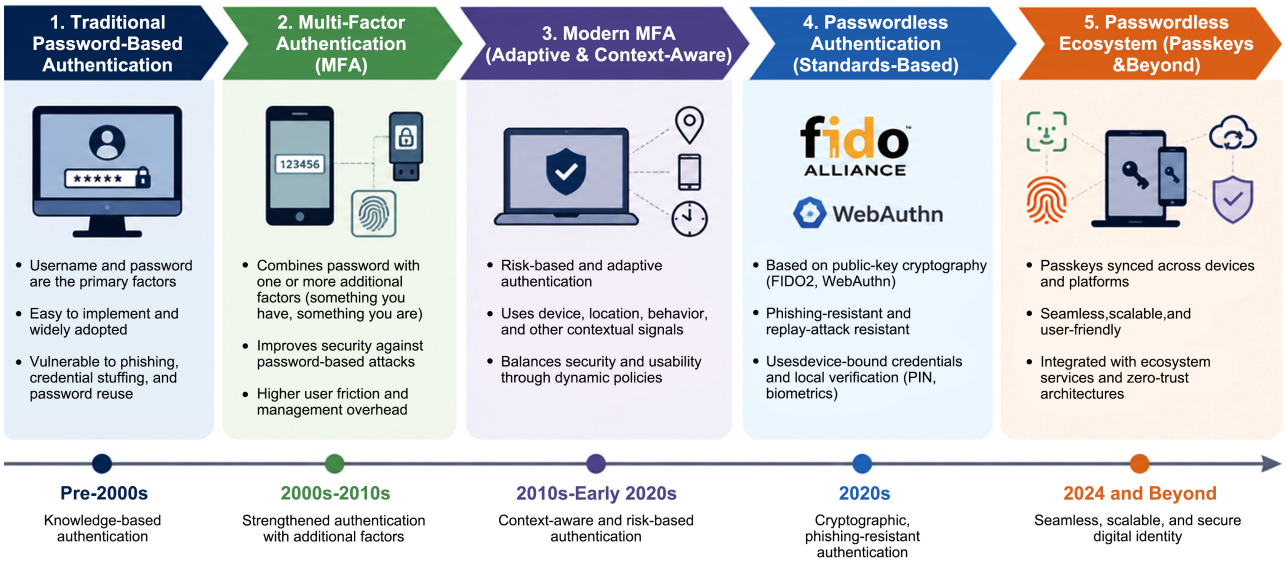

Figure 1. Evolution of authentication methods.

4. Adoption Metrics and Case Studies

Over the last five years, the trend of eliminating passwords has picked up significantly, as many organisations recognize the failure of password-based authentication to keep up with the challenges of today's digital infrastructures. With the ubiquity of FIDO2, WebAuthn and Passkeys, people can log in without relying on more vulnerable password-based logins without any risk of them being compromised or stolen, and without risk from phishing, credential theft or account takeover attacks [9]. Adoption patterns vary, though, from one business tier to another

(enterprise versus consumer) because goals for deployment, constraints, and regulations differ from tier to tier and expectations differ among consumers and users, as well.

4.1. Enterprise Adoption

The need to protect cloud and hybrid identity infrastructures, operational efficiency, regulatory compliance, and cybersecurity needs have been the key factors underpinning enterprise adoption. Enterprise organizations have been investing in passwordless authentication solutions via enterprise identity and access management (IAM) platforms to cut support costs associated with dealing with passwords and provide more protection to prevent credential-based attacks. Microsoft has rolled out Windows Hello for Business and FIDO2 authentications, claiming that around 70% of its employees have enrolled in selected enterprise deployments during 2022 and that practically 90% fewer passwords were reset, compared to standard password-based authentication [10]. Likewise, for enterprise deployments, integration with Single Sign-On (SSO) (some 55% of enterprise clients that enrolled) led to a higher success rate of logon completion before and after Okta integration, with ~25% cited as the improvement figure [11]. Industries with higher security and regulatory demands such as banking, healthcare, education, and government have a relatively higher adoption rate since they have more rigorous authentication and identity assurance criteria.

4.2. Consumer Adoption

Secure and seamless cross-device authentication and user-friendliness are among the primary factors driving consumer adoption. Platform vendors like Google, Apple, and other tech vendors are rolling Out Passkeys, allowing people to use their biometrics or familiar gadget to verify themselves without having to recollect a password after a security breach. Google estimated that in 2023, some 60 percent of the eligible users of the passkey functionality in selected workforce deployments and those that deployed passkeys with consumers successfully adopted the technology; almost half (49 percent) of users in phishing attacks using the passkeys functionality with available user data were also the unsuccessful users when compared with users that did not use passkeys in their logon, according to Google's study of implementation [9]. This is not only improving the security of financial institutions' mobile Banking products, but also the usability of their customer-facing applications that use passwords. For example, the Bank of America recently offered biometric passkey login for eligible mobile banking customers, which led to their subscription and was appreciated by customers, and it also contributed to an increase in mobile authentication security for mobile banking customers; 45% of the Bank of America's mobile banking customer base subscribed to passkey login [12]. The convenience of use, the possibility of securing with biometrics, compatibility with devices, and trust in its security are the top issues in driving consumer desire, while challenges like privacy and account recovery issues are

further factors slowing the rate of consumer adoption. The beliefs, attitudes, and intentions to use software systems as described by the Technology Acceptance Model (TAM) in Section 3 can account for these representations of software adoption. Regarding enterprise organisations, passwordless authentication could prove to be beneficial as it reduces the perceived risk of cybersecurity, password management and operating costs, and increases perceived usefulness. Perceived ease of use is more likely to drive consumer users—anything that can be easily identified using biometric methods and easily integrated into trusted devices is more appealing. On the other hand, its drawbacks of interoperability and recovery of credentials, privacy and compatibility issues do not promote adoption and trust in the technical features. An overview of selected and representative enterprise and consumer case studies found in published literature is provided in Table 1. The figures given for adoption rates refer to the percentage of users (or organizational deployments) identified as such in the studies and do not allow for statistical comparison to indicate the true rate of adoption. Values are representative evidence and should not be viewed as standardized benchmark measurements because the studies that underlie these values vary in the way they have been deployed, type of assessment, and reporting metrics used.

Table 1. Representative passwordless authentication adoption across enterprise and consumer deployments.

Organization	Deployment Context	Authentication Method	Adoption Population	Year	Reported Outcome	Reference
Microsoft	Enterprise	Windows Hello/FIDO2	Approximately **70% of eligible employees** in selected enterprise deployments	2022	Approximately **90% reduction** in password reset requests	[10]
Google	Enterprise/ Consumer	Passkeys (WebAuthn)	Approximately **60% of eligible users/workforce** in reported deployments	2023	Around **50% reduction** in successful phishing attempts	[9]
Okta	Enterprise	WebAuthn with Single Sign-On	Approximately **55% of enrolled enterprise clients**	2021	Approximately **25% improvement** in login success rate	[11]
Bank of America	Consumer Banking	Biometric Passkeys	Approximately **45% of eligible mobile banking customers**	2022	Improved mobile authentication security and customer satisfaction	[12]

5. Measuring Security Impact

Assessing the security effect of passwordless authentication goes beyond just the technical aspects of enhanced security and involves quantifying with performance metrics and then using qualitative metrics to assess results. Phishing instances and reports of credential theft, requests for password reset, authentication success

rates, login completion time, account takeover attempts, and the cost of support transactions to the helpdesk are among the more popular quantitative statistics. Qualitative statistics focus on usability, trust, accessibility, and administrative efficiency of users. When moving towards passwordless authentication, other factors like cryptographic assurance, device integrity validation, phishing resistance, and resiliency to replay attacks have become necessary to evaluate the effectiveness of the system [13]. Every enterprise deployment of FIDO2, WebAuthn, and Passkeys speaks to the fact that reusables are being removed from the authentication process, and the results have measurable positive effects on improving authentication security. In the large-scale deployments reported by studies involving Microsoft, Google, Okta, and others, the number of phishing attacks, password reset requests, credential compromises, and authentication failures has been reduced after adopting passwordless authentication [10]-[12] [14]. The improvements are explained by the fact that public-key cryptography keeps the private keys in trusted hardware where they are never delivered or revealed in authentication, which greatly diminishes the chances for both credential capture and replay (recording and replaying an authentication) from occurring. Furthermore, comparative studies show that passwordless authentication is more resistant to phishing attacks, adverse in-the-middle attacks, and credential stuffing attacks than traditional password-based Multi-Factor Authentication (MFA) methods, and that it enhances user convenience and reduces the administrative burden [15]. Even though passwordless authentication can offer technological benefits, it also presents new implementation issues such as representation attacks, loss of device, synchronization, and recovery, along with security mechanisms like adaptive authentication, behavioral analytics, continuous device trust assessment, and risk-based access policies [16]. The authors were able to distill some representative security enhancements from the reviewed enterprise and consumer case studies into an overall summary (**Figure 2**). Where published literature and industrial deployment data exist, the comparative values are used to illustrate overall security

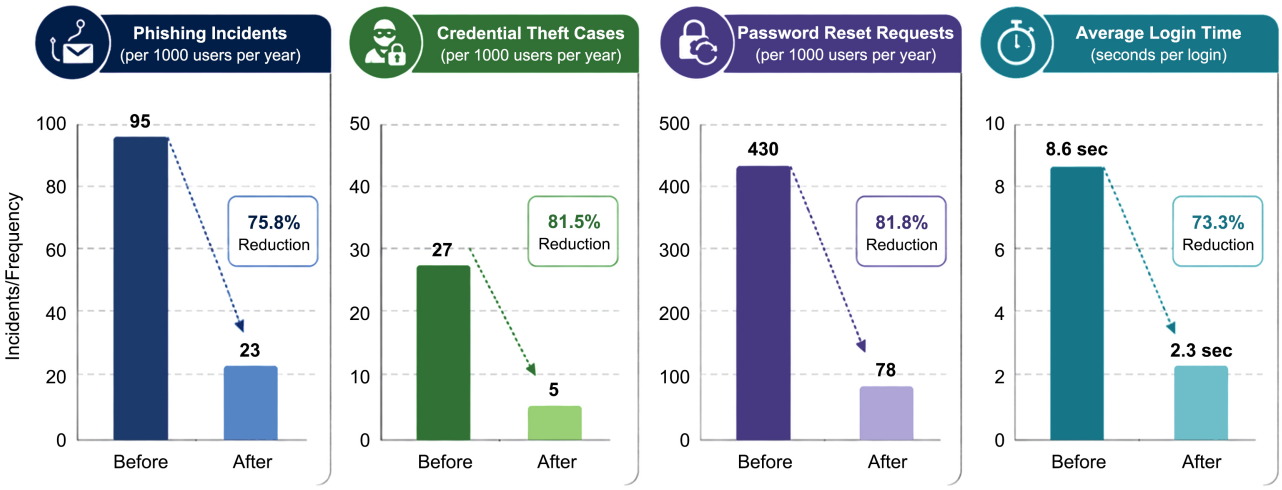

Figure 2. Representative security impact comparison before and after passwordless authentication deployment.

trends, and not results from a single experimental data set. As each of the reviewed studies has varying levels of deployments, evaluation approaches, numbers of evaluators, and the duration of the lift period, the values presented herein are intended to provide a foundation for evidence that, overall, passwordless authentication can reduce the incidence of compromises and enhance an organization's security and operational efficiency.

6. Problems and Future Projections

In the absence of global identity systems, there are some challenges in making passwordless authentication more convenient for users to perform what they need. The most critical issue is how to handle devices and keys. In a passwordless system, a private key is typically stored on trusted local machines. This re-enrolment/recovery process will be difficult if these types of devices are lost or replaced due to user actions, and it will affect their usability and security [17]. Furthermore, legacy solutions become hard to interoperate with other passwordless authentication solutions, such as Single Sign-On (SSO) and Federated ID. Protocols like FIDO2 and WebAuthn will offer privacy and security, but there are inconsistencies in their ability to be used across browsers, platforms and devices that pose a range of challenges for interoperability [18]. Other sets of stringent rules include User consent, data minimisation and authentication levels under regulatory frameworks like GDPR, HIPAA and PSD2. These are conflicting legal and technical obligations, and can be difficult to meet in order to increase uptake. Biometric systems and biometric hardware authenticators prove to be more convenient to use. So, there are certain types of people who aren't persuaded by biometric systems and hardware authenticators. The issue of perceived transparency and of users' confidence in the use of new authentication technologies has been identified as one of the most important topics [19]. So it's not just technically possible; it can't be effectively applied on a large scale unless there's an effort to educate people on the subject of making their personal data more secure with passwordless systems. Comparable to that, services and solutions that use AI, such as passwordless authentication and new solutions like DID decentralized identity, have tremendous potential in ushering us towards a passwordless world. Using AI, adaptive authentication can rely on contextual data to make more accurate decisions by analyzing how the user is using the device, verifying device integrity, and identifying anomalies on the network. A blockchain-based identity management architecture can enable decentralized identity platforms to help humans manage their identity without relying on a centralized entity, thereby reducing vulnerability [20]. The changes mentioned above will be future developments in the elaboration of Passwordless systems. It's already smart, privacy-enabling, and autonomous identity systems, transcending the whole world of authentication.

7. Conclusion

The digital identity system can offer a couple of handy enhancements to the basic

flaws of passwords: passwordless authentication and passwordless authentication keys. Businesses and research have made significant advancements in user satisfaction and credential security, and in measurable resistance to phishing attacks. Problems with interoperability, equipment costs, and more stringent security and privacy protocols have restricted the use of the field. If an appropriate quantified solution can be developed and conscientiousness can be created among users so that digital transformation can be scaled, then cooperation between the technology providers in both the discourse space and at the organizational level is crucial. Alongside passwordless security, these possible technologies like artificial intelligence and decentralized identity architectures will enable flexible and self-sovereign authentication as well. The passwordless user experience, its robust security features and convenience, makes it a promising solution for securing and authenticating users in the future of authentication and security management.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Bonneau, J., Herley, C., Oorschot, P.C.V. and Stajano, F. (2012) The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 *IEEE Symposium on Security and Privacy*, San Francisco, 20-23 May 2012, 553-567. https://doi.org/10.1109/sp.2012.44

[2] Alqahtani, A.A.S., Almuairfi, S., Hammad, M. and Alamleh, H. (2026) A Systematic Review of FIDO2 Security, Usability, and Deployment Evidence. SSRN, 34 p.

[3] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018) Multi-Factor Authentication: A Survey. *Cryptography*, **2**, Article 1. https://doi.org/10.3390/cryptography2010001

[4] Arias-Cabarcos, P., Krupitzer, C. and Becker, C. (2019) A Survey on Adaptive Authentication. *ACM Computing Surveys* (*CSUR*), **52**, 1-30. https://doi.org/10.1145/3336117

[5] Aloul, F., Zahidi, S. and El-Hajj, W. (2009) Two Factor Authentication Using Mobile Phones. 2009 *IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, 10-13 May 2009, 641-644. https://doi.org/10.1109/aiccsa.2009.5069395

[6] Balfanz, D., Czeskis, A., Hodges, J., Jones, J.C., Jones, M.B., Kumar, A., *et al.* (2019) Web Authentication: An API for Accessing Public Key Credentials Level 1. *W3C Recommendation*, **4**.

[7] Zimmermann, V., Schäfer, S., Dürmuth, M. and Marky, K. (2025) Authenticate as You Go: From Exploring Smart Home Authentication with Daily Objects to Authenticating with Primary Tasks. *ACM Transactions on Computer-Human Interaction*, **32**, 1-69. https://doi.org/10.1145/3702318

[8] Mustafa, G., Nizamani, S.Z., Memon, I., Wagan, A.A., Fedushko, S. and Hejaili, A.A. (2026) Usability Evaluation of a Push-Based Passwordless Authentication Model Using Public-Key Cryptography. *IET Biometrics*, **2026**, Article ID: 5462893. https://doi.org/10.1049/bme2/5462893

[9] Dharavath, K., Talukdar, F.A. and Laskar, R.H. (2013) Study on Biometric Authenti-

cation Systems, Challenges and Future Trends: A Review. 2013 *IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, 26-28 December 2013, 1-7. https://doi.org/10.1109/iccic.2013.6724278

[10] Yusop, M.I.M., Kamarudin, N.H., Suhaimi, N.H.S. and Hasan, M.K. (2025) Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity. *IEEE Access*, **13**, 13919-13943. https://doi.org/10.1109/access.2025.3528960

[11] Holtgrave, J.U., Klivan, S., Marky, K. and Fahl, S. (2025) A Qualitative Study of Adoption Barriers and Challenges for Passwordless Authentication in German Public Administrations. Proceedings of the 2025 *CHI Conference on Human Factors in Computing Systems*, Yokohama, 26 April 2025-1 May 2025, 1-16. https://doi.org/10.1145/3706598.3713252

[12] Chitta, S. (2024) Continuous Behavioral Biometrics for Passwordless Authentication: A Trust Engine-Privacy Preserving, on Device Trust Engine for Mobile and Wearables. *International Journal of Emerging Trends in Computer Science and Information Technology*, **5**, 161-173. https://doi.org/10.63282/3050-9246.ijetcsit-v5i3p116

[13] Ghorbani Lyastani, S. (2023) Studying User Experience and Acceptance of Web Authentication Solutions. https://publikationen.sulb.uni-saarland.de/bitstream/20.500.11880/37474/1/Dissertation_finalprint.pdf

[14] Karuppiah, S.P. (2025) Understanding the Behaviour of Business Users in Multi-Factor Authentication Adoption. https://lutpub.lut.fi/bitstream/handle/10024/169612/Masterthesis_Karuppiah_SivamPrasath.pdf?sequence=1

[15] Hashmi, T.H., Tang, G., Liu, X. and Zhang, Z. (2025) Multi-Dimensional Identity Construction and Continuous Authentication Methods: A Survey. *Journal of Networking and Network Applications*, **5**, 176-197.

[16] Al Kabir, M.A. and Elmedany, W. (2024) Adaptive Risk-Based Passwordless Authentication: A Fido2 Integrated Approach for Enhanced Security and Usability. Social Science Research Network, 46 p.

[17] Papadamou, K., Gevers, S., Xenakis, C., Sirivianos, M., Zannettou, S., Chifor, B., *et al.* (2020) Killing the Password and Preserving Privacy with Device-Centric and Attribute-Based Authentication. *IEEE Transactions on Information Forensics and Security*, **15**, 2183-2193. https://doi.org/10.1109/tifs.2019.2958763

[18] Yasasve, P. (2026) Enhancing Secure Identity Management: A Systematic Review of Passwordless Authentication Techniques. *Anusandhanvallari*, **1**, 1324-1331.

[19] Hien, L.M. and Thai, N.D. (2024) Developing a Passwordless Authentication Solution Using Asymmetric Cryptography and Device Fingerprint Technology. 2024 *RIVF International Conference on Computing and Communication Technologies* (*RIVF*), Danang, 21-23 December 2024, 227-231. https://doi.org/10.1109/rivf64335.2024.11009081

[20] Aramide, O.O. (2024) Zero-Trust Identity Principles in Next-Gen Networks: Ai-Driven Continuous Verification for Secure Digital Ecosystems. *World Journal of Advanced Research and Reviews*, **23**, 3304-3316. https://doi.org/10.30574/wjarr.2024.23.3.2656