GlobeIS International Journal of Global Information Systems
globeisjournal.com

Comparing Multi-Factor Authentication Methods from SMS and TOTP to FIDO2/WebAuthn and Passkeys: A Qualitative Study of Practitioner Perspectives

Femi Emmanuel Folorunsho [1*], Zubair Odeleye [2]

[1] Ball State University, Muncie, Indiana, United States

[2] Wale University, Lagos, Nigeria

*Corresponding author: ffolorunsho30@gmail.com

ABSTRACT

The escalation of cyber-attacks has intensified the need for stronger multi-factor authentication (MFA), motivating a shift from traditional knowledge- and possession-based factors, such as SMS one-time passwords (OTP) and time-based one-time passwords (TOTP), toward FIDO2/WebAuthn credentials and passkeys. This study qualitatively compares five widely deployed MFA methods, grouped as traditional (SMS-based OTP, TOTP, and push-based authentication) and advanced (FIDO2 security keys and platform biometric authenticators), across four criteria: usability, security, cost, and implementation challenges. Adopting an interpretive qualitative design, the study draws on semi-structured interviews with four identity-and-access-management (IAM) practitioners, analysed through Braun and Clarke's six-phase reflexive thematic analysis. Coding produced an initial framework of 30 codes that was consolidated into four themes corresponding to the study criteria. Practitioners consistently characterised traditional methods as more affordable and broadly familiar but weaker in security and more prone to operational reliability problems, whereas FIDO2 security keys and platform biometrics were described as offering stronger phishing resistance and smoother day-to-day operation at a higher initial and maintenance cost. The study situates these accounts within organisational governance and cross-regional regulatory drivers of adoption and recommends a risk-based migration toward FIDO2/WebAuthn and passkeys.

Keywords: FIDO2/WebAuthn, identity and access management, multi-factor authentication, passkeys, phishing resistance, usability

1. INTRODUCTION

The rise in cyber-attacks conducted through phishing, data breaches, and ransomware has made multi-factor authentication (MFA) a core control for protecting digital identities (Nallainathan, 2021; Suleski et al., 2023). Personal email, online learning platforms, corporate email, social media, and e-banking systems are all routinely targeted by attackers seeking access to personal or confidential data (Gupta, 2025). MFA methods can be grouped broadly into traditional and advanced approaches (Abduhari et al., 2025). Traditional MFA typically verifies a user through a knowledge or possession factor delivered as an SMS-based one-time password (OTP) or a time-based one-time password (TOTP) generated by applications such as Google Authenticator or Authy (Prabha et al., 2025). These delivery channels have increasingly been exposed to interception and social-engineering attacks as adversary techniques have matured (Almass & Chowdhary, 2024). Advanced MFA, by contrast, relies on public-key

cryptography and passwordless verification (Ferdous et al., 2026; Shukla et al., 2025), in which a user is authenticated through a device-bound or synced credential unlocked by a local gesture, such as a PIN or biometric, under the WebAuthn and Fast Identity Online 2 (FIDO2) standards (Yusop et al., 2025). Despite their known weaknesses, traditional methods remain widely used because of their low cost and broad compatibility, even though they are less secure than modern passwordless approaches (Mondal & Sarkar, 2025).

This study compares selected traditional and advanced MFA methods on four criteria: usability, security, cost of use, and implementation challenges. The traditional methods examined are SMS-based OTP, TOTP, and push-based authentication; the advanced methods are FIDO2 security keys and platform biometric authenticators.

1.1 Objectives

The objectives of this study are:

- To evaluate the selected MFA methods on usability;
- To evaluate the security of the selected MFA methods;
- To determine the cost of using the selected MFA methods; and
- To identify the challenges associated with implementing the selected MFA methods.

2. RELATED WORK

2.1 Traditional MFA Methods

Traditional MFA is a security model that combines two or more factors, most commonly a password with a time-limited code or a security question, to prevent unauthorised third-party access to user data on digital platforms such as websites and banking applications (Acemyan et al., 2018; Ang et al., 2025; Eko-Davies, 2025; Reese et al., 2019).

- **SMS-based OTP:** SMS-based OTP delivers a time-limited code (typically a six-digit code) to a user by text message during sign-in, strengthening security beyond username and password (Kaur & Jain, 2025; Zhao et al., 2025). It is popular because of its wide compatibility and convenience (Jubur et al., 2025; Zou et al., 2025), and codes can also be received through applications without a SIM (Kavitha et al., 2025; Maryniuk et al., 2025). However, the absence of end-to-end encryption in the cellular signalling infrastructure and the prevalence of SIM-swapping make SMS codes vulnerable to interception (Abbas et al., 2025; Bartłomiejczyk & El Fray, 2024; Peeters et al., 2022).
- **TOTP:** TOTP generates short-lived codes locally on the user's device using a shared secret and the current time, through applications such as Google Authenticator or Authy (Almeida et al., 2023; Ikram et al., 2024; Kalash et al., 2025). Because codes are generated offline and are typically valid for only about 30 seconds, they are harder for attackers to intercept than SMS codes (Bianchi & Valeriani, 2023; Huseynov, 2020). Authentication can nonetheless fail when the clock on the user's device and the server drift out of alignment (Kasse & Mboup, 2025).

- **Push-based authentication:** Push-based authentication sends a notification to a registered device asking the user to approve or deny a sign-in attempt, rather than requiring manual entry of a code (Lassak et al., 2024). It is generally less susceptible to interception than conventional OTPs (George, 2024), but it is vulnerable to "MFA fatigue" attacks, in which repeated push spam leads a user to approve a fraudulent request accidentally (Bicakci et al., 2026).

2.2 Advanced (Passwordless) MFA Methods

Advanced MFA authenticates users through passwordless, public-key methods, in which a private key stored on an authenticator signs a challenge and a local gesture, such as a PIN or biometric, unlocks that key under WebAuthn/FIDO2 (Angelogianni et al., 2024; Obulose & Agu, 2024).

- **FIDO2 security keys (roaming authenticators):** FIDO2 security keys are portable hardware authenticators that store a private key and use public-key cryptography, rather than a shared password, to verify identity (Matzen et al., 2025; Mitra & Sethuraman, 2025). Common examples include the YubiKey 5 series, Google Titan Security Key, and Feitian ePass K9 NFC/USB-A (Karim et al., 2023; Papaspirou et al., 2023). They provide strong, origin-bound resistance to phishing that OTP-based methods cannot match (Qian, 2024). Their principal limitations are usability barriers arising from user unfamiliarity and a comparatively high per-unit and provisioning cost for individuals and organisations (Burda, 2025; Clarke & Furnell, 2025).
- **Platform biometric authenticators:** Platform biometric authenticators verify a user through fingerprint, facial, iris, retina, or voice recognition, most often as the local user-verification gesture that unlocks an on-device FIDO2 credential (Aramide, 2023; Ganmati et al., 2025; Sriman et al., 2024). They are convenient and generally reliable, but presentation attacks, such as fingerprint duplication, photographs, and voice mimicry, remain a concern where liveness detection is weak (Arora & Bhatia, 2022).

2.3 Clarifying the FIDO2/WebAuthn Ecosystem

Because reviewers and practitioners frequently conflate the components of passwordless authentication, this section clarifies the terminology used throughout the study. FIDO2 comprises two specifications: the W3C Web Authentication (WebAuthn) API and the Client-to-Authenticator Protocol (CTAP). Within this ecosystem, several concepts are distinct but related:

- Authenticator type. A roaming (cross-platform) authenticator is an external device such as a USB, NFC, or Bluetooth security key; a platform authenticator is built into a phone or computer and typically uses the device's biometric sensor.

- Passkeys. A passkey is a FIDO2 credential (a discoverable WebAuthn credential). Device-bound passkeys never leave the authenticator (as on a security key), whereas synced passkeys are backed up and synchronised across a user's devices through a platform provider's cloud keychain.

- Biometrics. In FIDO2, a biometric is not itself the authenticating secret; it is the local user-verification gesture that unlocks the private key. The biometric template does not leave the device.

Accordingly, this study treats "FIDO2 security keys" as roaming hardware authenticators and "platform biometric authenticators" as platform authenticators unlocked by biometrics. The label "physical passkeys" used in earlier drafts is replaced by "FIDO2 security keys" to avoid conflating a hardware form factor with the credential type.

3. MATERIALS AND METHODS

3.1 Research Design

This study adopted an interpretive qualitative design centred on semi-structured expert interviews. The design is exploratory and descriptive: it seeks to understand how experienced IAM practitioners perceive, weigh, and articulate the trade-offs among five MFA methods across four criteria, rather than to measure those methods numerically or generalise to a defined population. A qualitative approach was chosen because authentication decisions in organisations are shaped by professional judgement, contextual constraints, and lived operational experience that are best surfaced through practitioners' own accounts. Reflexive thematic analysis was selected as the analytic strategy because it is well suited to identifying patterned meaning across a small, information-rich set of expert accounts.

3.2 Participants and Recruitment

Four identity-and-access-management (IAM) practitioners took part in semi-structured interviews conducted between January and February 2026. Participants were selected purposively for their direct professional experience of deploying or managing authentication systems. To protect confidentiality, and because their individual identities are not material to the analysis, participants are reported by role and sector rather than by name or employer, and are labelled E1–E4:

- E1 – a senior executive at a fintech company;
- E2 – an experienced IT security practitioner;
- E3 – a senior product leader at an identity-management provider; and
- E4 – a product-marketing manager specialising in identity and access management.

Participants were approached by email or professional-network message and provided informed consent before participating. Recruitment prioritised depth and relevance of expertise over breadth; the small sample is consistent with an interpretive study whose aim is analytic insight rather than statistical representativeness.

3.3 Data Collection

The four participants took part in two audio-recorded interview sessions. Session 1 was held on 17 January 2026 with E1 and E2, and Session 2 on 7 February 2026 with E3 and E4; each recorded segment ran for approximately twelve minutes. Both sessions were transcribed with the participants' consent. All participants were told the purpose of the study, that participation was voluntary, and that their responses would be de-identified. A semi-structured interview guide directed the conversation around

the four criteria: usability, security, cost, and implementation challenges for the five MFA methods, while leaving room for participants to raise issues they considered important.

3.4 Data Analysis

Interview data were analysed using Braun and Clarke's six-phase reflexive thematic analysis: familiarisation, initial coding, theme generation, theme review, theme definition, and reporting. Coding was primarily deductive, structured around the four a priori criteria (usability, security, cost, and challenges), while remaining open to inductive sub-codes arising from the data. An initial codebook of 30 codes was generated (Table 1) and then organised into the four overarching themes reported in the Findings (Table 2). Coding was performed by the lead researcher and independently reviewed by a second member of the research team, who checked the code-to-theme assignments; disagreements were resolved through discussion until consensus was reached. The full codebook, mapping the 30 codes to the four themes, is available from the corresponding author on request.

Trustworthiness was addressed with reference to the criteria of Lincoln and Guba. Credibility was supported by drawing on practitioners with direct operational experience and by grounding every interpretation in verbatim quotations. Dependability and confirmability were supported by maintaining an audit trail of transcripts, codes, and theme definitions, and by independent review of the coding. Transferability was supported by providing sufficient contextual description of participants' roles and sectors to allow readers to judge the relevance of the findings to their own settings. Reflexivity was maintained throughout, with the research team remaining attentive to how their prior familiarity with passwordless authentication might shape interpretation.

3.5 Ethical Considerations

Participation was voluntary and based on informed consent. Interview participants were de-identified and are reported only by role and sector (E1–E4); no directly identifying information is published. The study protocol was reviewed by the Ball State University institutional research ethics committee and granted an exemption determination, protocol no. 2197107-3 as it involved anonymous, voluntary participation by adults, collected no sensitive personal data, and posed minimal risk to participants.

Table 1. Initial Coding Framework Derived from the Interview Data

No.	Initial code	Description / meaning	Evidence
1	Traditional authentication use	Continued organisational reliance on conventional verification methods	E1
2	User technological diversity	Users have different levels of technological knowledge	E1
3	Username and password authentication	Continued use of usernames and passwords as a primary mechanism	E1
4	Awareness of alternative authentication	Awareness of technologies beyond passwords	E1
5	Biometric authentication adoption	Consideration of face and fingerprint recognition	E1
6	Security-key adoption	Planned or preferred use of physical security keys	E1, E4

7	Gradual authentication transition	Movement to advanced authentication occurring progressively	E1
8	Ease of biometric verification	Facial verification perceived as straightforward	E2
9	Password familiarity	Familiarity makes passwords easy to operate	E2
10	User memorability	Users create passwords from personally memorable information	E2
11	Professional usability	Methods usable for professional applications such as banking	E2
12	Security-key preference in banking	Security keys preferable to OTPs in banking contexts	E2
13	OTP service downtime	OTP affected by service availability	E2
14	Perceived authentication security	Existing authentication perceived as adequately secure	E1
15	Additional transaction verification	Extra verification for higher-value transactions	E1
16	Authentication maintenance cost	Maintaining authentication is an organisational expense	E1
17	Customisation cost	Tailoring authentication increases expenditure	E1
18	Financial barrier to upgrading	Cost influences decisions to adopt advanced methods	E1
19	OTP delivery delay	Users experience delays receiving codes	E1
20	Network dependency	OTP depends on network conditions for delivery	E2
21	Duplicate OTP codes	Delayed codes result in multiple codes	E2
22	User confusion from delayed codes	Multiple or delayed codes cause uncertainty	E2
23	Biometric environmental limitations	Environmental conditions interfere with biometrics	E3, E4
24	Biometric recognition limitations	Physical conditions interfere with fingerprint recognition	E3
25	Authentication method vulnerabilities	Every method has some form of weakness	E3
26	Phishing resistance of passkeys	Passkeys particularly resistant to phishing	E3
27	OTP affordability	OTP perceived as more affordable than advanced methods	E3
28	High hardware security-key cost	Physical security keys require significant investment	E4
29	Layered authentication	Combining mechanisms strengthens protection	E4
30	Preference for advanced authenticators	Advanced authenticators viewed as the preferred future option	E4

Note. Codes were generated during initial coding and later consolidated into the four themes reported in Table 2.

Table 2. Organisation of the Initial Codes into Four Themes

Overarching theme	Contributing codes
Theme 1: Usability	Traditional authentication use; user technological diversity; username and password authentication; awareness of alternatives; biometric adoption; security-key adoption; gradual transition; ease of biometric verification; password familiarity; user memorability; professional usability; security-key preference in banking

DOI: https://doi.org/10.66395/globeis.19
ISSN: 3108-7213

Theme 2: Security	Perceived authentication security; additional transaction verification; authentication method vulnerabilities; phishing resistance of passkeys; layered authentication; biometric authentication security; security-key security; passkey security
Theme 3: Cost	Authentication maintenance cost; customisation cost; financial barrier to upgrading; OTP affordability; high hardware security-key cost
Theme 4: Implementation Challenges	OTP service downtime; OTP delivery delay; network dependency; duplicate OTP codes; user confusion from delayed codes; biometric environmental and recognition limitations

4. FINDING

Four themes were developed from the interview data, each corresponding to one of the study's criteria: usability, security, cost, and implementation challenges. Across all four, practitioners consistently distinguished the three traditional methods (SMS-based OTP, TOTP, and push-based authentication) from the two advanced, passwordless methods (FIDO2 security keys and platform biometric authenticators). The following sections present each theme in turn, grounded in participants' own words.

4.1 Theme 1: Usability

Practitioners portrayed usability as having two faces: the familiarity that keeps traditional methods in place, and the efficiency and reliability that draw organisations toward advanced methods. Traditional credentials were valued for accommodating users with varied levels of technological knowledge, and passwords in particular were seen as easy because they are familiar and often saved by browsers. At the same time, participants described a deliberate, staged movement toward security keys and biometrics. E1 explained that the organisation was actively planning this transition:

> *"Though we currently verify users with usernames and passwords, we are looking to strengthen security by offering security keys to those who can afford them, and verifying existing users through face or fingerprint ID, and having new users register their face or fingerprint at sign-up."* –- E1

For learnability, practitioners agreed that all methods can be learned quickly, but they distinguished everyday convenience in professional settings. E2 noted that although OTPs are simple to adopt, security keys are frequently preferred in banking because they are not exposed to the delivery delays that affect codes:

> *"All of the methods are easy to learn and can be used for professional work such as banking, but tokens (security keys) are preferred in banks over OTPs because of the service downtime that can affect code delivery."* –- E2

Reliability at the moment of need was a further usability concern. While participants stressed that every method is broadly dependable, they ranked biometrics and security keys highest. E3 captured this graded view:

> *"All the authentication methods are strong, but biometric verification is the most dependable, and you can rely on security keys too."* –- E3

DOI: https://doi.org/10.66395/globeis.19
ISSN: 3108-7213

Taken together, these accounts suggest that traditional methods retain a usability advantage rooted in familiarity, but that practitioners increasingly associate genuine day-to-day usability –- speed, fewer steps, and dependable operation –- with passwordless authenticators. This is consistent with Lyastani et al. (2020), who found passwordless methods more usable than passwords and OTPs.

4.2 Theme 2: Security

Security was the theme on which practitioners converged most strongly. All participants accepted that every method carries some weakness, yet they consistently positioned FIDO2 security keys and biometrics as the most resistant to compromise. E3 emphasised the origin-bound, phishing-resistant nature of passkeys, framing phishing as the dominant threat:

> *"Virtually every method has a weakness – some to forgery, some to phishing – but passkeys have very strong resistance to phishing."* –- E3

Practitioners also reasoned about the cryptographic and biometric strength of the underlying factors. E4 contrasted the shared-secret logic of OTPs with the key-based and biometric logic of advanced methods:

> *"An OTP strengthens a username and password with a code; a passkey requires a key-generated credential that is hard to compromise; and my face, fingerprint, or typing behaviour can only authenticate me, which keeps my secrets safe."* –- E4

Layered verification emerged as a practical security pattern, particularly in payments, where an additional factor is added to an existing one. E4 and E1 both described this arrangement:

> *"Some methods are layered onto an existing one –for example, some payment platforms require facial verification in addition to a PIN."* –- E4

> *"A second check is sometimes required for large transfers on digital-banking platforms."* –- E1

Participants were candid about the limits of biometrics, noting that oily fingerprints or poor lighting can impede recognition, and that OTP codes remain exposed to interception and delivery problems. On balance, however, the security accounts pointed clearly toward passwordless methods as offering the strongest protection, echoing Ravilla et al. (2023), who reported that FIDO2 passwordless authentication offers the strongest protection against credential compromise.

4.3 Theme 3: Cost

Cost was the clearest counterweight to the security and usability advantages of advanced methods. Practitioners agreed that all authentication carries expense, but they consistently identified passwordless methods, and hardware security keys in particular, as the most costly to acquire and maintain. E3 drew the direct-cost contrast plainly:

> *"Adopting OTPs is far more affordable than WebAuthn/FIDO2 and passkeys, which use more advanced technology."* –- E3

E4 acknowledged the higher outlay for hardware keys while still recommending them, tying cost to the value of stronger protection:

> *"Organisations spend more to obtain and maintain hardware security keys, but they are the most secure and are highly recommended."* –- E4

Beyond acquisition, participants highlighted continuing maintenance and customisation costs. E4 pointed to the ongoing financial commitment required for passwordless infrastructure, while E1 noted that tailoring authentication to specific needs raises the bill further:

> *"Managing OTPs is not as expensive as WebAuthn/FIDO2; organisations need strong financial capacity to keep up with maintenance."* –- E4

> *"Maintaining an authentication method is expensive, and tailoring it to what an individual or organisation specifically needs can raise the cost further."* –- E1

The cost theme thus frames adoption as a trade-off: practitioners see clear security and reliability gains in passwordless methods but recognise that their direct, indirect, and user-specific costs can constitute a real barrier, especially for smaller or resource-constrained organisations. This mirrors Bindel et al. (2023), who found that FIDO2 offers the strongest security but can be costly to implement.

4.4 Theme 4: Implementation Challenges

The final theme concerned the operational problems practitioners encountered in practice, which they associated overwhelmingly with OTP-based methods. Delays in code delivery, dependence on network conditions, duplicate codes, and resulting user confusion recurred across the interviews. E2 linked OTP delays directly to network quality and described the confusion that follows:

> *"OTP verification is usually smooth, but code arrival can be delayed by poor networks caused by bad weather. Users sometimes receive duplicate codes when they retry after a delayed first code."* –- E2

E1 corroborated this from the organisation's support experience, and E4 framed the same reliability problems as a driver of the wider industry shift toward biometric and behavioural verification:

> *"Users reporting errors often describe delays in receiving codes."* –- E1

> *"Because atmospheric conditions hinder sending and receiving OTP codes, the industry is moving toward behavioural and biometric verification."* –- E4

By contrast, practitioners reported that FIDO2 security keys and biometrics ran comparatively smoothly, being free of the network-dependent delivery on which OTPs rely. Where advanced methods encountered difficulty, it was environmental –- lighting or fingerprint condition –- rather than infrastructural. This pattern is consistent with Kim et al. (2020), who identified vulnerabilities in OTP authentication linked to network faults, and it reinforces the broader account of passwordless methods as more operationally dependable.

5. DISCUSSION

VOL. 2, NO. 1, June 2026
DOI: https://doi.org/10.66395/globeis.19
ISSN: 3108-7213

Across all four themes, the two passwordless methods, FIDO2 security keys and platform biometrics, were consistently described by practitioners as outperforming the three traditional methods on security, usability, and operational reliability, while carrying higher direct and indirect costs. The accounts were notably coherent: origin-bound public-key credentials remove the shared secrets that make SMS and TOTP interceptable, which explains both their superior phishing resistance and their freedom from the network-dependent delays that drive OTP fatigue and downtime. The same feature that makes passwordless methods more secure the absence of a transmittable code also makes them, in practitioners' experience, more reliable in everyday use.

The cost theme provides the principal tension in this picture. Practitioners did not dispute the superiority of passwordless methods; rather, they framed adoption as a question of financial capacity and organisational readiness. This suggests that the barrier to migration is less technical than economic and managerial, a point with direct implications for how organisations should plan and budget for authentication upgrades.

5.1 Governance and Regulatory Drivers of Adoption

Technical superiority alone does not determine adoption; organisational governance and regional regulation strongly shape which methods are deployed. In the European Union, the revised Payment Services Directive (PSD2) mandates strong customer authentication for electronic payments (European Parliament & Council of the European Union, 2015), and the eIDAS framework governs cross-border electronic identity (European Parliament & Council of the European Union, 2014), both of which push regulated entities toward phishing-resistant methods. In the United States, NIST SP 800-63B discourages SMS as an out-of-band authenticator and rates cryptographic authenticators at the highest assurance levels, influencing federal and contractor practice (Grassi et al., 2017). Sectoral regimes such as PCI DSS for payment card data further raise the baseline, now requiring multi-factor authentication for all access into the cardholder data environment (PCI Security Standards Council, 2022). For multinational organisations, these divergent requirements make MFA selection a governance decision about assurance levels, auditability, and cross-regional interoperability, not merely a usability or cost trade-off. Framed this way, the migration toward FIDO2/WebAuthn and passkeys is as much a response to compliance and risk-governance pressure as to technical merit, which situates this study within the broader agenda of global information-systems governance and digital transformation.

6. LIMITATION

Several limitations should be borne in mind. First, the study rested on four expert interviews conducted in two sessions, which constrains the depth and comparability of the data and means the findings are analytically rather than statistically generalisable; they are best read as an information-rich account of experienced practitioner reasoning rather than as a representative survey of the field. Second, the participants were drawn from fintech, IT security, and identity-management roles, so perspectives from other sectors, such as healthcare or the public sector, are not represented. Third, self-reported perceptions of security and cost

may diverge from measured technical performance and actual expenditure. Fourth, while the coding was independently reviewed and an audit trail maintained, interpretation inevitably reflects the research team's prior familiarity with passwordless authentication, which reflexive practice sought to surface but cannot eliminate. These limitations motivate the future-research agenda below.

7. FUTURE RESEARCH

Future qualitative work should broaden and deepen the practitioner base, drawing on larger and more sector-diverse samples, including healthcare, education, and the public sector, to test the transferability of the four themes developed here. Longitudinal case studies of organisational passkey migration, including the lived trade-offs between synced and device-bound credentials and the security of recovery flows, would add valuable process insight. Ethnographic and observational methods could complement interview self-reports by capturing authentication behaviour as it actually unfolds, and further studies could examine how specific regulatory regimes accelerate or impede adoption across regions. Where appropriate, future research might also triangulate these qualitative accounts with instrumented measures of authentication latency, failure rates, and total cost of ownership.

8. CONCLUSION

Protecting users' data on digital platforms requires reliable verification of identity, and MFA has become central to that task. This study qualitatively compared three traditional methods (SMS-based OTP, TOTP, and push-based authentication) with two advanced, passwordless methods (FIDO2 security keys and platform biometric authenticators) across usability, security, cost, and implementation challenges, drawing on the accounts of four IAM practitioners. Practitioners consistently described traditional methods as affordable and familiar but less secure and more prone to network-related operational problems, whereas FIDO2 security keys and biometrics were seen as offering stronger phishing resistance and smoother operation at a higher cost. Weighed against these higher initial and maintenance costs, the perceived security and reliability advantages support a risk-based migration toward FIDO2/WebAuthn and passkeys, guided by organisational governance and the relevant regional regulatory frameworks.

Ethics Statement

The study protocol was reviewed by the Ball State University Institutional Review Board, which granted an exemption determination (protocol no. 2197107-3). Participation in the interviews was voluntary and based on informed consent. Interview participants were de-identified and are reported only by role and sector (E1–E4).

Funding Statement

This research received no external funding.

Author Contributions

Femi Emmanuel Folorunsho: conceptualization, methodology, investigation, formal analysis, writing, original draft, writing, review and editing. Zubair Odeleye: methodology, formal analysis (independent review of the qualitative coding), writing, review and editing. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The interview consent records and correspondence, and the full qualitative codebook mapping the 30 codes to the four reported themes, are retained by the corresponding author and are available on reasonable request.

Acknowledgments

The authors thank the four identity-and-access-management practitioners who generously shared their time and expertise in the interviews.

REFERENCES

1. Abbas, W., Joshua, S. R., Abbas, A., & Lee, J. H. (2025). An end-to-end GSM/SMS encrypted approach for smartphone employing advanced encryption standard (AES). *arXiv*. https://arxiv.org/abs/2503.18859
2. Abduhari, E. S., Shaik, T. C., Adidul, A. B., Ladja, J. H., Saliddin, E. S., Adin, A. J., Rumbahali, F. A., Sali, A. B., Jemser, J. M., & Tahil, S. K. (2025). Access control mechanisms and their role in preventing unauthorized data access: A comparative analysis of RBAC, MFA, and strong passwords. *Natural Sciences Engineering and Technology Journal, 5*(1), 418–430. https://doi.org/10.37275/nasetjournal.v5i1.62
3. Abiew, N. A. K., Jnr, M. D., & Banning, S. O. (2020). Design and implementation of cost effective multi-factor authentication framework for ATM systems. *Asian Journal of Research in Computer Science, 5*(3), 7–20.
4. Acemyan, C. Z., Kortum, P., Xiong, J., & Wallach, D. S. (2018). 2FA might be secure, but it's not usable: A summative usability assessment of Google's two-factor authentication methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62*(1), 1141–1145.
5. Almass, S., & Chowdhary, S. K. (2024). Comprehensive study on cyber security and cyber attacks. In *Proceedings of the 1st International Conference on Electronics, Communication and Signal Processing (ICECSP)* (pp. 1–6). IEEE.
6. Almeida, L. E., Fernández, B. A., Zambrano, D., Almachi, A. I., Pillajo, H. B., & Yoo, S. G. (2023). One-time passwords: A literary review of different protocols and their applications. In *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability* (pp. 205–219). Springer Nature.
7. Ang, K. W., Chekole, E. G., & Zhou, J. (2025). Unveiling the covert vulnerabilities in multi-factor authentication protocols: A systematic review and security analysis. *ACM Computing Surveys*.
8. Angelogianni, A., Politis, I., & Xenakis, C. (2024). How many FIDO protocols are needed? Analysing the technology, security and compliance. *ACM Computing Surveys, 56*(8), 1–51.
9. Aramide, O. O. (2023). AI-driven identity verification and authentication in networks: Enhancing accuracy, speed, and security through biometrics and behavioral analytics. *Adhyayan: Journal of Management Sciences, 13*(2), 60–69.
10. Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective, 31*(1), 28–48.
11. Bartłomiejczyk, M., & El Fray, I. (2024). Device risk analysis protocol for SMS-based OTP authentication. *IEEE Access*.
12. Bianchi, G., & Valeriani, L. (2023). Time is on my side: Forward-replay attacks to TOTP authentication. In *International Symposium on Security and Privacy in Social Networks and Big Data* (pp. 109–126). Springer.
13. Bicakci, K., Varli, F. M., Korkmaz, M. E., & Uzunay, Y. (2026). QES-backed virtual FIDO2 authenticators: Architectural options for secure, synchronizable WebAuthn credentials. *arXiv*. https://arxiv.org/abs/2601.06554
14. Bindel, N., Cremers, C., & Zhao, M. (2023). FIDO2, CTAP 2.1, and WebAuthn 2: Provable security and post-quantum instantiation. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)* (pp. 1471–1490). IEEE.
15. Burda, K. (2025). Electronic identification of persons and objects – current status. *International Journal of Computer Science and Network Security, 25*(6), 1.
16. Clarke, N., & Furnell, S. (2025). Usable authentication: Are we there yet? *Computers & Security*, 104823.
17. Duy, P. T., Minh, V. Q., Dang, B. T. H., Son, N. D. H., Quyen, N. H., & Pham, V. H. (2024). A study on adversarial sample resistance and defense mechanism for multimodal learning-based phishing website detection. *IEEE Access*.

18. Eko-Davies, O. (2025). Emerging trends in user authentication tools: Innovations, challenges, and future directions. In *Proceedings of the IEEE International Conference on Electro Information Technology (eIT)* (pp. 51–55). IEEE.
19. European Parliament & Council of the European Union. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)*. Official Journal of the European Union, L 257, 73–114. http://data.europa.eu/eli/reg/2014/910/oj
20. European Parliament & Council of the European Union. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)*. Official Journal of the European Union, L 337, 35–127. http://data.europa.eu/eli/dir/2015/2366/oj
21. Ferdous, M. S., Ali, M. Y., Chowdhury, F. R., Nahid, M. A., Ionita, A., & Prinz, W. (2026). A passwordless authentication mechanism for the web using self-sovereign identity. *ACM Transactions on the Web*.
22. Ganmati, A., Afdel, K., & Koutti, L. (2025). Deep learning-based multi-factor authentication: A survey of biometric and smart card integration approaches. *arXiv*. https://arxiv.org/abs/2510.05163
23. George, A. S. (2024). The dawn of passkeys: Evaluating a passwordless future. *Partners Universal Innovative Research Publication, 2*(1), 202–220.
24. Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b
25. Gupta, S. (2025). Hacking the system: A deep dive into the world of e-banking crime. In *Techno-Legal Dynamics of Cyber Crimes in Industry 5.0* (pp. 121–148).
26. Huseynov, E. (2020). Improving user experience with TOTP hardware tokens by implementing QR codes and HID keyboard emulation. In *Proceedings of the IEEE International Conference on Application of Information and Communication Technologies (AICT)* (pp. 1–5). IEEE.
27. Idrus, Z. S. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences, 7*(5), 95–107.
28. Ikram, M., Sentana, I. W. B., Asghar, H., Kaafar, M. A., & Kepkowski, M. (2024). More than just a random number generator! Unveiling the security and privacy risks of mobile OTP authenticator apps. In *International Conference on Web Information Systems Engineering* (pp. 177–192). Springer.
29. Jubur, M., Shrestha, P., & Saxena, N. (2025). An in-depth analysis of password managers and two-factor authentication tools. *ACM Computing Surveys, 57*(5), 1–32.
30. Kalash, Ghosh, B. C., & Addya, S. K. (2025). Enhancing security in smart contract wallets: An OTP-based two-factor authentication approach. In *Proceedings of the International Conference on Distributed Computing and Networking* (pp. 211–220).
31. Kamaruddin, N. H. C., & Zolkipli, M. F. (2024). The role of multi-factor authentication in mitigating cyber threats. *Borneo International Journal, 7*(4), 35–42.
32. Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A. K. (2023). Online banking user authentication methods: A systematic literature review. *IEEE Access, 12*, 741–757.
33. Kasse, M. C., & Mboup, E. H. M. (2025). Post-quantum secure authentication protocol based on OTP and TEE. *The Journal of Supercomputing, 81*(16), 1–33.
34. Kaur, K., & Jain, A. K. (2025). A survey on phishing attack taxonomy, detection techniques, datasets, and security measures. *Journal of Applied Security Research*, 1–52.
35. Kavitha, L., Ashwitha, K., Dharshana, P. K., & Elakkiyaa, M. (2025). Wireless locking system through OTP. In *Proceedings of the International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)* (pp. 1795–1799). IEEE.
36. Kim, H., Han, J., Park, C., & Yi, O. (2020). Analysis of vulnerabilities that can occur when generating one-time passwords. *Applied Sciences, 10*(8), 2961.
37. Lassak, L., Pan, E., Ur, B., & Golla, M. (2024). Why aren't we using passkeys? Obstacles companies face deploying FIDO2 passwordless authentication. In *33rd USENIX Security Symposium* (pp. 7231–7248).
38. Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? A comparative usability study. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)* (pp. 268–285). IEEE.
39. Maryniuk, M. D., Dalbo, A., Stanitski, J., & Khan, Y. (2025). Using text messaging to reach, reinforce, remind, and support. *ADCES in Practice, 13*(1), 16–19.
40. Matzen, A., Rüffer, A., Byllemos, M., Heine, O., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Challenges and potential improvements for passkey adoption – a literature review with a user-centric perspective. *Applied Sciences, 15*(8), 4414. https://doi.org/10.3390/app15084414
41. Mitra, A., & Sethuraman, S. C. (2025). Verifiable passkey: The decentralized authentication standard. *arXiv*. https://arxiv.org/abs/2512.21663
42. Mondal, P. C., & Sarkar, P. P. (2025). A novel risk-based multi-factor authentication approach for card-not-present transactions. *International Journal of Research and Innovation in Social Science, 9*(3), 3062–3076.
43. Muir, A., Brown, K., & Girma, A. (2024). Reviewing the effectiveness of multi-factor authentication methods in preventing phishing attacks. In *Proceedings of the Future Technologies Conference* (pp. 597–607). Springer.
44. Nallainathan, S. (2021). Analysis onto the evolving cyber-attack trends during COVID-19 pandemic. *International Journal of Science and Research, 10*(4), 139–144.
45. Obulose, C., & Agu, P. C. (2024). *The future of passwordless authentication: Trends, predictions, and emerging technologies*.
46. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1.
47. Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., & Gerla, M. (2019). Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Network, 33*(2), 82–88.
48. Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems. *Mesopotamian Journal of Cybersecurity*, 115–133.
49. Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrag, M. A., & Janicke, H. (2023). A novel authentication method that combines honeytokens and Google Authenticator. *Information, 14*(7), 386. https://doi.org/10.3390/info14070386
50. PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and testing procedures* (Version 4.0). https://www.pcisecuritystandards.org

51. Peeters, C., Patton, C., Munyaka, I. N., Olszewski, D., Shrimpton, T., & Traynor, P. (2022). SMS OTP security: Hardening SMS-based two-factor authentication. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS)* (pp. 2–16).
52. Pietrzak, K. (2020). Delayed authentication: Preventing replay and relay attacks in private contact tracing. In *International Conference on Cryptology in India* (pp. 3–15). Springer.
53. Prabha, R. S., Dharaneesh, C. K. V., & Reshekkaesh, K. A. (2025). Bio secure authentication framework. In *Proceedings of the International Conference on Electronics, Computing, Communication and Control Technology (ICECCC)* (pp. 1–6). IEEE.
54. Qian, Y. (2024). Applying combined one-time passwords to prevent phishing attacks in electronic banking. *Journal of Artificial Intelligence and Systems Modelling, 2*(4), 32–46.
55. Ravilla, H., Sayal, R., & Kulkarni, P. (2023). Study and analysis of FIDO2 passwordless web authentication. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 375–386). Springer.
56. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)* (pp. 357–370).
57. Senapartha, I. K. D., & Nendya, M. B. (2024). Usability evaluation of mobile multi-factor authentication based on face authentication, geolocation and QR code. *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer), 10*(2), 425–432.
58. Shukla, S., Varshney, G., Singh, S., & Goel, S. (2025). A passwordless MFA utilizing biometrics, proximity, and contactless communication. *Information Security Journal: A Global Perspective, 34*(6), 633–654.
59. Sriman, J., Thapar, P., Alyas, A. A., & Singh, U. (2024). Unlocking security: A comprehensive exploration of biometric authentication techniques. In *Proceedings of the IEEE Confluence* (pp. 136–141).
60. Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health, 9*, 20552076231177144.
61. Vorakulpipat, C., Pichetjamroen, S., & Rattanalerdnusorn, E. (2021). Usable comprehensive-factor authentication for a secure time attendance system. *PeerJ Computer Science, 7*, e678.
62. Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review. *IEEE Access*.
63. Zhao, J., He, F., Yang, Y., & Zhang, Y. (2025). Identifying implementation flaws of SMS OTP authentication. *IEEE Transactions on Mobile Computing*.
64. Zou, F., Zhang, Z., & Hu, Y. (2025). OTP-Hunter: An app-based fuzzing framework to discover one-time password vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*.