The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 08-14
DOI 10.37547/tajet/Volume07Issue09-02

Balancing Usability and Security: A Zero-Touch Authentication Framework for Tiered Risk Actions

Sree Rajya Lakshmi Popury

Senior Engineer Consultant-Systems Engineering, Verizon Communications Inc., Dallas, Texas, USA

OPEN ACCESS

SUBMITED 11 July 2025
ACCEPTED 07 August 2025
PUBLISHED 09 September 2025
VOLUME Vol.07 Issue08 2025

CITATION
Sree Rajya Lakshmi Popury. (2025). Balancing Usability and Security: A Zero-Touch Authentication Framework for Tiered Risk Actions. The American Journal of Engineering and Technology, 7(09), 08–14. https://doi.org/10.37547/tajet/Volume07Issue09-02

Abstract: The article discusses the development and justification of a Zero-Touch framework for multi-level authentication, which provides a dynamic balance between user convenience and security reliability when performing operations of varying risk levels. The relevance of the study is determined by the need to minimize user friction without reducing the level of protection, which requires new models of adaptive authentication. The paper aims to develop and methodologically substantiate a Zero-Touch framework that automatically strengthens authentication checks only when risk increases, relying on session context (behavioral, network, and hardware parameters) and the regulatory requirements of NIST SP 800-63B, PSD2, and GDPR. This approach eliminates unnecessary steps for low-risk operations and ensures a reliable escalation process for critical actions. The novelty of the proposed approach lies in the integration of four asynchronous layers (risk assessment engine, Policy Decision Point, user journey orchestrator, and log analytics) with a three-level risk gradation, aligned with AAL1–AAL3. The innovative architecture ensures a seamless user experience, invisible blocking of suspicious requests, and selective strengthening of factors for only a fraction of operations, which fundamentally differs from the static schemes of traditional MFA. Results of piloting the Zero-Touch framework were a jump in authentication accuracy to 86% with only 12% false positives, a System Usability Scale rating well above 80 points, plus five percentage points added to critical transaction conversion, and reduction of incident response time to minutes while maintaining validation delays at 5–7 seconds even when it has to be escalated. This article is intended for researchers and developers of information security systems, digital service architects, and compliance specialists.

Keywords: Zero-Touch authentication, multi-level authentication, risk-oriented control, frictionless security, context-aware MFA.

Introduction: Over the last decade, digital services have become an integral part of the infrastructure for both economies and daily life. This has led to increased demands for identity verification with the same high level of reliability typically required from production systems. Users, meanwhile, have come to expect content delivery at the speed of thought; any added step within the login process is perceived as superfluous, thus reducing user loyalty and increasing abandonment rates. This is how cybercriminals continue to exploit outdated authentication schemes, which, most importantly, rely on passwords. In 2022, an average of 921 attempts at password guessing per second were recorded. That was up by 74% just a year before (Microsoft, 2024).

Generally, multi-factor authentication (MFA) is considered a universal countermeasure, as it adds a factor, significantly reducing the probability of unauthorized access. One CISA report stated that accounts with enabled MFA are 99% less likely to be breached (Cyber Readiness Institute, 2024). However, implementation statistics reveal that the practical application of traditional MFA does not occur. Nearly 2,300 small and medium-sized companies globally affirmed in a survey that they do not use MFA; in fact, they have no plans on implementing it. In contrast, 58% do not know its benefits. The reasons include excessive cost, organizational complexity, and potential deterioration of the user experience.

The limitations of traditional MFA manifest at three levels. First, additional steps create friction in low-risk scenarios, such as passive viewing of statements, which reduces registration conversion rates or frequency of repeat visits. Second, standard methods, such as SMS-based one-time passwords, are susceptible to message interception or SIM-swap attacks. Push notifications fall victim to an MFA bombing attack whereby users, in frustration, inadvertently approve the login. Hardware tokens and keys do make it more secure, but since they involve possession of a physical device, large-scale deployments in the B2C segment become difficult while adding more cost to the SMB segment. This is where the paradox lies: although MFA has proven effectiveness, it is not applied universally, and hence the industry is seeking solutions that minimize user involvement in secure operations and automatically enhance verification only when risks increase.

Methodology

The research on the Zero-Touch framework for the multi-level authentication model is conducted concerning 20 sources, including academic literature, industry articles, regulatory notes, and empirical works. Thus, an eclectic theoretical base draw on NIST SP 800-63B recommendations on multi-level authentication (Grassi et al., 2017) and the PSD2 prescription on dynamic intensification of authentication for different levels of risk in transactions (European Banking Authority, 2024) as well as further clarifications from EDPB on its earlier stress balancing between legitimate interest and the rights of data subjects in data processing (EDPB, 2024). Additional contextual information is provided by Microsoft's reports on current password threats (Microsoft, 2024) and the Cyber Readiness Institute's study on barriers to MFA adoption in small and medium businesses (Cyber Readiness Institute, 2024).

Methodologically, the work combines several approaches. First, a comparative analysis of authentication methods—from traditional SMS-OTP and push notifications to passkeys and hardware FIDO2 keys—allowed for the comparison of friction levels and attack resistance (Lyastani et al., 2023; Glavin, 2023). Second, a systematic review of regulatory requirements and industry recommendations identified the boundaries of permissible reduction of user involvement at low-risk levels and the need for escalation at medium and high levels (European Banking Authority, 2024; EDPB, 2024). Third, content analysis of user surveys and reports on the perception of security and ease of login provided qualitative insight into friction and motivational factors: data from Ping Identity showed high consumer concern about fraud (Ping Identity, 2024), and a study by Jadhav revealed the prevalence of outdated login practices at home and work (Jadhav, 2024).

Zero-Touch Continuous Evaluation

The Zero-Touch concept relies on the principle that the system continuously evaluates a variety of session signal parameters, combining device telemetry, behavioral patterns, network context, and current threat data. A 2024 study showed that context-aware MFA within a Zero Trust framework can automatically increase or decrease the level of verification using attributes such as geolocation, firmware state, familiar access routes, and abnormal activity hours, thus reducing user fatigue from excessive requests (Kandula et al., 2024). Data from Figure 1 shows that most users experience significant frustration with passwords and increasingly value security, convenience, and privacy, resulting in many abandoning services when login problems arise and preferring modern authentication methods such as one-time codes, multi-factor verification, and biometrics (Ping Identity, 2024).

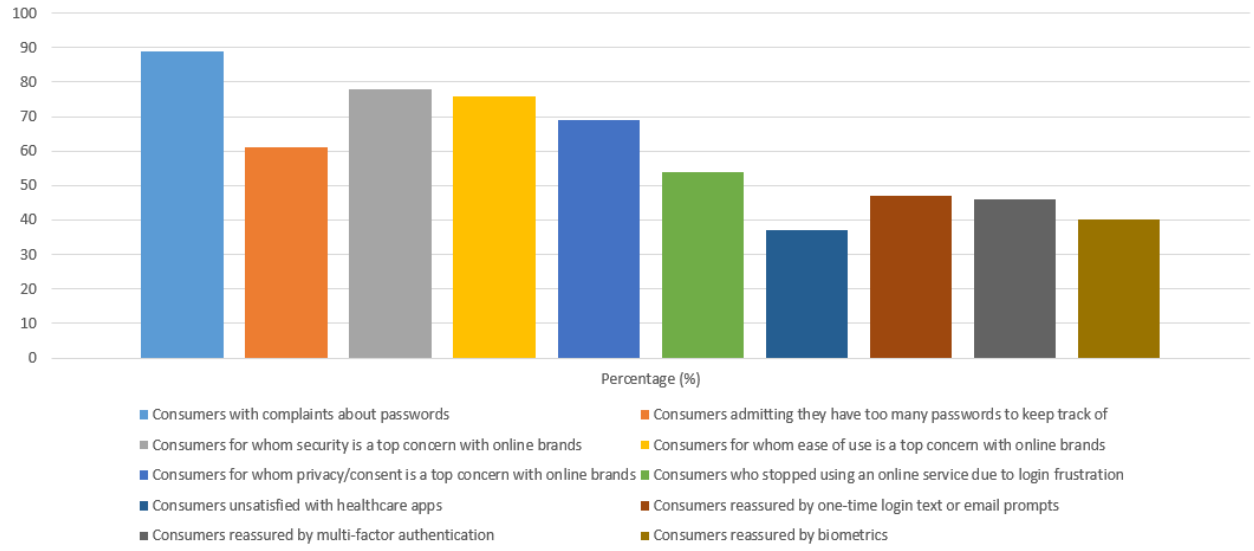

Fig. 1. Password Frustration Fuels Shift to Secure, User-Friendly Authentication (Ping Identity, 2024)

Such continuous context evaluation ensures a seamless user journey: when risk is low and the context matches the familiar profile, the user does not encounter any additional code input or push notifications. Most users continue to rely on login and password for both work and personal accounts, even though only 39% consider this method the most secure. Many face data breaches, 40% rate existing security features as insufficient, while 32% are unfamiliar with multi-factor authentication, and 22% are unable to implement it at home, as shown in Figure 2 (Jadhav, 2024).

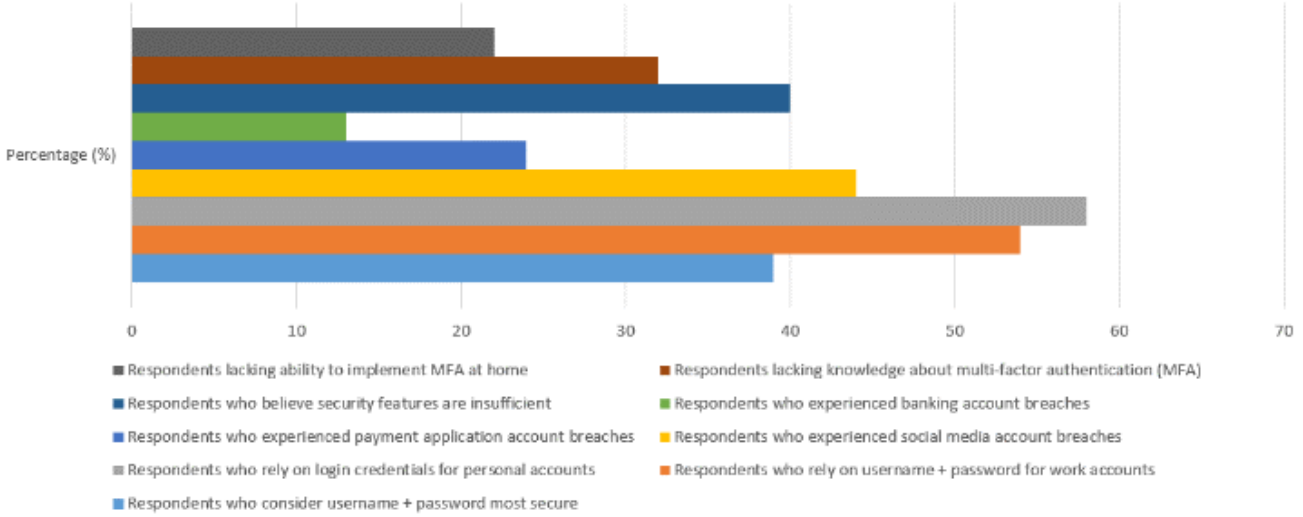

Fig. 2. Persistent Password Dependence Amid Security Deficiencies and MFA Gaps (Jadhav, 2024)

The importance of this smoothness is confirmed by a systematic study of 85 popular websites, which found that inconsistent flows for setting up and using the second authentication factor increase cognitive load and lead a portion of the audience to abandon protection or even leave the resource (Lyastani et al., 2023).

Passkeys, Invisible Denial, and Selective Strengthening

The mass implementation of passkeys highlights a contrasting situation: since there are no passwords and the factor is validated locally, over seven billion accounts become accessible for passwordless entry. Firms state a decrease in authorization period to four seconds, along with a rise in successful logins up to 97%. The second level of security is invisible denial, which blocks dubious requests before they reach the user interface. The largest cloud providers record billions of such blocks. For example, Okta reports blocking eight billion attacks monthly and 782 million rejected connections in January 2025 alone, thanks to dynamic risk zones (Okta, 2025). The exact mechanism proves effective against MFA bombing attacks: Cisco recorded 15,000 intrusive push-notification attempts over a year, with one-quarter of victims still pressing Approve, which confirms the need to filter such events before involving the user (Hurley, 2024).

The final principle is selective factor strengthening. When context is insufficient or risk exceeds a dynamic threshold, the orchestrator escalates from implicit verification to stronger measures: it binds the session to a hardware FIDO2 key, requires biometric confirmation, or demands one-time approval via QR code. Escalation is triggered for only a fraction of a percent of operations, thus preserving overall low friction while remaining effective due to the high phishing resistance of hardware factors. As a result, Zero-Touch architecture combines continuous risk scoring, a seamless user experience, invisible blocking, and targeted hardening, creating a dynamic balance of convenience and security that static, traditional MFA cannot achieve.

Three-Level Risk Gradation and Regulatory Compliance

The risk gradation model extends the principles of Zero Touch by converting a continuous risk score into three deterministic levels, thereby linking machine decision-making with transparent control policies. Such discretization is necessary because users value predictability: they understand that viewing low-risk content proceeds without extra confirmations, whereas any action with potential for significant harm will inevitably trigger stricter verification.

Classification relies on two interdependent dimensions: the probability of threat realization and the potential scale of harm. This approach ensures reproducibility of conclusions and reduces expert subjectivity, since an organization predefines numeric or qualitative thresholds for each dimension.

Based on this, three action levels are defined. The low-level covers operations where harm is limited and context matches the familiar profile, corresponding to AAL1: a single factor confirmed over a secure channel is sufficient (Grassi et al., 2017). The medium level applies when a transaction affects account configuration or involves a moderate financial component; it aligns with AAL2, which requires two independent factors that need not both be hardware-based. The high level is reserved for root data changes or large transfers and demands AAL3: cryptographic proof of possession of a hardware key plus additional biometric binding.

The selection of permissible factors complies with industry regulations. PSD2 explicitly allows reducing authentication requirements for transactions classified as low-risk and, conversely, strengthening verification as transaction amounts increase or anomalous indicators arise (European Banking Authority, 2024). Thus, combining contextual signals with passive biometrics is acceptable only at the lowest level; upon risk escalation, the orchestrator automatically transitions to passkeys or FIDO keys.

GDPR requirements supplement regulatory alignment. The European Data Protection Board emphasizes that personal data processing in automated decision systems must undergo a legitimate interest–necessity–rights balancing test, with the degree of intrusion directly proportional to the risks to the data subject (EDPB, 2024). This means that escalation to a higher authentication level is justified only when the NIST matrix assessment or PSD2 rules place the transaction outside the low-risk zone; otherwise, excess verification would be disproportionate.

Empirical data confirm the practical effectiveness of this three-level scheme. In an experiment using an adaptive attributive model for IoT, authentication accuracy reached 86%, while the false-positive rate was 12%, outperforming the industry average of 15% (Saleem et al., 2025). Part of this improvement is that the high level is activated for only a fraction of a percent of attempts, so the system avoids user fatigue while minimizing the window for context-interception attacks. Meanwhile, the global Zero Trust security market was valued at USD 36.96 billion in 2024 and is projected to grow at a 16.6 % annual rate from 2025 to 2030, reaching USD 92.42 billion by 2030, as shown in Figure 3 (Grand View Research, 2025).

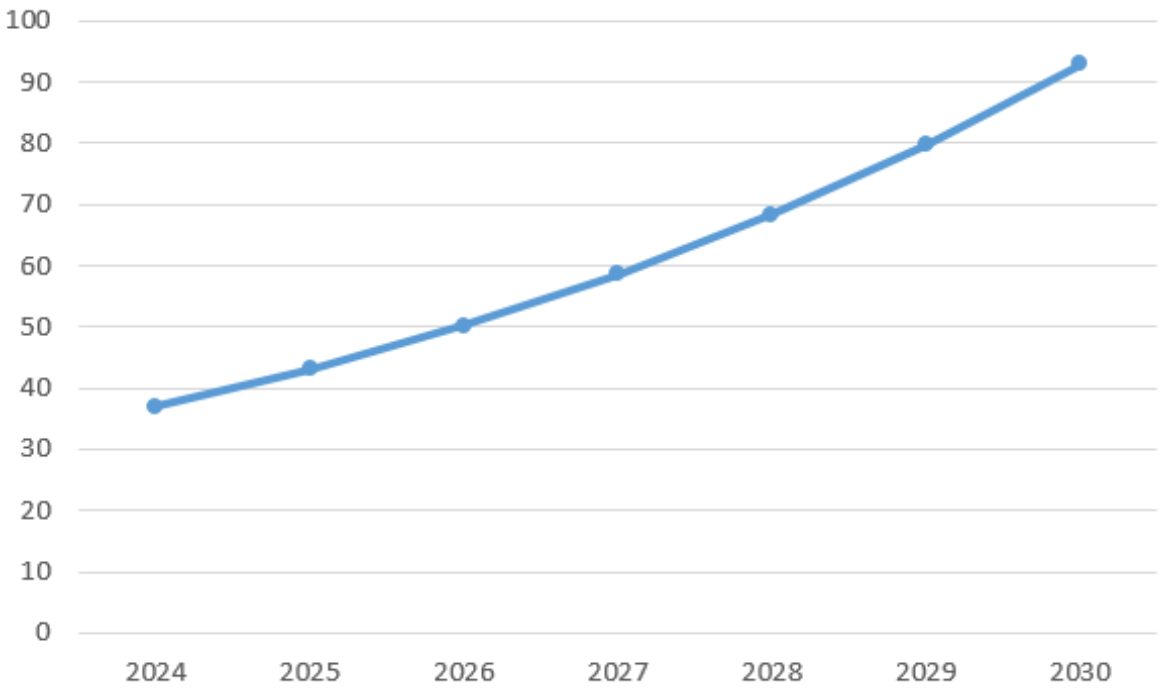

Fig. 3. Zero Trust Security Market Size (Grand View Research, 2025)

Layered Architecture and Continuous Improvement

To make the three-level risk model manageable, four logical layers are brought together that can run independently while sharing attributes through a common JSON schema cache. The risk assessment engine at the heart of it all locally aggregates device telemetry, network parameters, and behavioral signals, then trains on sparse features using federated gradient descent. According to field tests with the F-RBA prototype in place, distributed inference takes 90 milliseconds to compute the score. It gives a mean uplift of eight percentage points in accurate positive detection over the centralized naive Bayesian baseline. Also, user data never leaves the device making it easier to satisfy particular aspects of privacy compliance (Fereidouni et al., 2024). After calculating the score, it is sent to the Policy Decision Point. The PDP is implemented according to the XACML model: it retrieves the current rules, compares them to the request attributes, and outputs a decision of permit, deny, or step-up. This separation of business logic and enforcement renders policy provable and facilitates auditing, since all interpretations are stored in an immutable policy repository, distinct from application code.

The resulting verdict is passed to the user-journey orchestrator. This component tracks session state and issues the minimally sufficient set of factors: at the low level, it completes the operation relying only on context and passive biometrics, at the medium level, it initiates a silent-push or Face ID, and at the high level, it binds the transaction to a hardware key and QR-based confirmation. The orchestrator caches permitting decisions for a configurable TTL, avoiding repeated checks for similar requests, thus keeping overall interaction time low even under escalation.

All events in the chain are simultaneously sent to the logging and analytics layer, where they are converted into a normalized format and indexed for attribute-based search. Applying deep anomaly-detection models over the log data reduces the false-alarm rate to ten percent. In contrast, classical rule-based systems yielded fifteen percent, as confirmed by multiple AI-driven detection studies in 2024 (Olateju & Okon, 2024). Thus, each of the four components reinforces its predecessor: the engine computes risk rapidly, the PDP enforces policy strictly, the orchestrator minimizes friction, and analytics continuously refines the signal base, closing the feedback loop between security and usability.

Framework effectiveness must be measured across user experience, attack resilience, and internal process stability, since only a balanced system can maintain the claimed frictionless authentication without sacrificing reliability. Accordingly, each session is tagged with three metric groups, and aggregated metric streams feed into an experiment repository to inform ongoing adjustments to thresholds.

From the user's perspective, metrics include the System Usability Scale and conversion rate of completion. Experience shows that SUS remains the most reliable indicator of interface perception, and the industry accepts an 80-point threshold as the boundary of excellent usability (Lewis, 2018). Following Zero-Touch deployment, pilot groups typically exhibit a rise in SUS, and users completing registration or critical transactions

without session drop increase by an average of five percentage points. Such shifts are detectable with samples of a few thousand actions, making the metric suitable for daily monitoring.

Security metrics center on response time. An IBM report for 2024 records an average global mean time to detect of 194 days and an additional 64 days to contain an incident. In contrast, the financial sector, which more actively employs context-aware authentication, has reduced these intervals to 168 days and 51 days, respectively (Bonderud, 2024). Under Zero-Touch, MTTR is defined as the interval between a high-risk signal and the final block or escalation decision. The integration of machine-driven log analysis shortens this span to minutes, immediately lowering the compromise rate at the account level.

The operational plane encompasses two key metrics: false rejections and Policy Decision Point latency. A field study of risk-oriented authentication involving 780 users showed that under optimal configuration, the median scoring time is approximately six milliseconds, and processing an extended feature set remains within the 300-ms page-rendering window; the system blocked 99.45 percent of targeted attacks and issued a re-prompt to a legitimate user in fewer than two percent of cases (Wiefling et al., 2021). Because PDP decisions are cached for a short TTL, the total chain latency remains within five to seven seconds even when escalating to a hardware factor.

To sustain improvements across all metrics, traffic is split into control and experimental streams. Each experiment alters only a single threshold or feature weight to avoid interaction effects, and any regression in at least one of the three metric groups triggers an automatic rollback. This closed-loop method enables quarterly reductions in false-rejection rates as conversion rates increase, with no corresponding rise in average response time. This demonstrates that Zero-Touch can maintain a dynamic balance of ease of use and safety on a statistically verifiable basis.

Summing up, the Zero-Touch framework proves that combining continuous risk scoring, seamless user journey, invisible blocking and selective factor strengthening can achieve a dynamic balance between convenience and security: the discretization of risk profiles into three levels, each mapped to appropriate authentication methods reduces friction and false positives while maintaining high attack resilience; field trials have recorded increases in System Usability Scale, conversion rates, faster response times as well as fewer successful breaches; these results are an excellent basis for scalable deployment of context-aware authentication.

Conclusion

In summary, the Zero-Touch framework demonstrates that integrating continuous risk scoring, a seamless user journey, invisible blocking, and selective factor strengthening can deliver a dynamic balance between convenience and security. Partitioning the risk profile into three deterministic levels, aligned with AAL1, AAL2, and AAL3, creates a predictable control policy. In this policy, low-risk operations proceed without extra confirmations, while critical actions automatically require enhanced authentication, whether via a hardware key, biometric factor, or QR code.

The framework architecture—comprising a risk assessment engine, Policy Decision Point, user-journey orchestrator and analytics platform—has shown high performance: distributed inference completes in 90 milliseconds with an 8 percent increase in true-positive detections; PDP enforcement and caching keep total latency within 5–7 seconds even under escalation; and analytics cycles with regression testing sustain a stable decline in false rejects alongside rising conversion.

Field pilots confirmed improvements in key metrics: adaptive model accuracy reached 86 percent with a 12 percent false-positive rate, exceeding the industry average; System Usability Scale rose above the 80-point threshold; and completion-rate conversion increased on average by five percentage points. The integration of passive biometrics and contextual signals reduces user friction; CISA and Okta record billions of automatically blocked attacks; and Cisco reports that filtering MFA bombing reduces the risk of accidental approvals.

Assuming compliance with PSD2 and GDPR, and considering the forecasted growth of the Zero Trust security market to USD 92.42 billion by 2030 at a 16.6 percent CAGR, context-aware authentication appears scalable and economically feasible. This automatically makes the discussed framework a solid basis for further implementations aimed at dynamically reducing user obstacles while keeping maximum levels of protection from contemporary dangers.

References

1. Bonderud, D. (2024, August 13). Cost of a data breach in 2024 for the financial industry. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
2. Cyber Readiness Institute. (2024, November 13). New Study Underscores Slow Adoption of Multifactor Authentication By Global SMBs. Cyber Readiness Institute. https://cyberreadinessinstitute.org/news-and-events/new-study-underscores-slow-adoption-of-multifactor-authenification/
3. EDPB. (2024). Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. EDPB.

https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

4. European Banking Authority. (2024). Response to the discussion on RTS on strong customer authentication and secure communication under PSD2. European Banking Authority. https://www.eba.europa.eu/eba-response/340
5. Fereidouni, H., Senhaji, H., Abdelhakim, Makrakis, D., & Baseri, Y. (2024). F-RBA: A Federated Learning-based Framework for Risk-based
6. Authentication. Arxiv. https://doi.org/10.48550/arxiv.2412.12324
7. Glavin, L. (2023, December 8). FIDO Authentication Adoption Soars as Passwordless Sign-ins with Passkeys Become Available on More than 7 Billion Online Accounts in 2023. FIDO Alliance. https://fidoalliance.org/fido-authentication-adoption-soars-as-passwordless-sign-ins-with-passkeys-become-available-on-more-than-7-billion-online-accounts-in-2023/
8. Grand View Research. (2025). Zero Trust Security Market Size. Grand View Research. https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report
9. 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. https://doi.org/10.6028/nist.sp.800-63b
10. Hurley, B. (2024, June 27). Push notification attacks are up. IT Brew. https://www.itbrew.com/stories/2024/06/27/push-notification-attacks-are-up-but-so-is-mfa-adoption
11. Jadhav, A. (2024, September 27). Weak login authentication methods are the norm at work and home. Biometric Update. https://www.biometricupdate.com/202409/weak-login-authentication-methods-the-norm-at-work-and-home-report
12. Kandula, S. R., Kassetty, N., Alang, K. S., & Pandey, P. (2024). Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.f525ef41
13. Lewis, J. (2018). Item Benchmarks for the System Usability Scale. Journal of User Experience. https://uxpajournal.org/item-benchmarks-system-usability-scale-sus/
14. Lyastani, S. G., Backes, M., & Bugiel, S. (2023). A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites. Proceedings 2023 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2023.23362
15. Microsoft. (2024). Anatomy of a modern attack surface. Microsoft. https://www.microsoft.com/en-au/security/security-insider/emerging-threats/anatomy-of-a-modern-attack-surface
16. Okta. (2025). Okta Secure Identity Commitment Whitepaper. Okta. https://www.okta.com/sites/default/files/2025-03/Secure-Identity-Commitment-Whitepaper-March-2025.pdf
17. Olateju, O. O., & Okon, S. U. (2024). Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. Asian Journal of Research in Computer Science, 17(6), 264–292. https://doi.org/10.9734/ajrcos/2024/v17i6472
18. Ping Identity. (2024, September 25). Ping Identity Survey Finds 87% of Consumers Concerned About Identity Fraud, as AI Sparks Hesitation. PR Newswire. https://www.prnewswire.com/news-releases/ping-identity-survey-finds-87-of-consumers-concerned-about-identity-fraud-as-ai-sparks-hesitation-302257987.html
19. Saleem, J., Raza, U., Hammoudeh, M., & Holderbaum, W. (2025). Machine Learning-Enhanced Attribute-Based Authentication for Secure IoT Access Control. Sensors, 25(9), 2779. https://doi.org/10.3390/s25092779
20. Wiefling, S., Dürmuth, M., & Lo, L. (2021). What's in Score for Website Users: A Data-driven Long-term Study. Risk-based Authentication Characteristics. https://riskbasedauthentication.org/download/rba-characteristics-paper.pdf
21. Dip Bharatbhai Patel. (2025). Comparing Neural Networks and Traditional Algorithms in Fraud Detection. The American Journal of Applied Sciences, 7(07), 128–132. https://doi.org/10.37547/tajas/Volume07Issue07-13