SoK: A Systematic Review of Context- and Behavior-Aware Adaptive Authentication in Mobile Environments

Vyoma Harshitha Podapati[0009−0001−1353−711X], Divyansh Nigam[0009−0001−4765−9449], and Sanchari Das[0000−0003−1299−7867]

George Mason University
{vpodapat,dnigam,sdas35}@gmu.edu

Abstract. As mobile computing becomes central to digital interaction, researchers have turned their attention to adaptive authentication for its real-time, context- and behavior-aware verification capabilities. However, many implementations remain fragmented, inconsistently apply intelligent techniques, and fall short of user expectations. In this Systematization of Knowledge (SoK), we analyze 41 peer-reviewed studies since 2011 that focus on adaptive authentication in mobile environments. Our analysis spans seven dimensions: privacy and security models, interaction modalities, user behavior, risk perception, implementation challenges, usability needs, and machine learning frameworks. Our findings reveal a strong reliance on machine learning (64.3%), especially for continuous authentication (61.9%) and unauthorized access prevention (54.8%). AI-driven approaches such as anomaly detection (57.1%) and spatio-temporal analysis (52.4%) increasingly shape the interaction landscape, alongside growing use of sensor-based and location-aware models.

Keywords: Adaptive Authentication · Mobile Security

1 Introduction

As mobile devices become the primary access point to digital services, growing threats such as credential theft and unauthorized access demand authentication methods that go beyond static credentials [14, 16, 30]. Adaptive authentication has emerged as a promising solution, dynamically adjusting security mechanisms based on contextual signals such as user behavior, device state, and environmental risk [6, 8, 32]. However, current implementations remain fragmented, often relying on inconsistent design principles and failing to address human-centered concerns. As a result, many systems lack responsiveness to user expectations and contextual nuances [13, 41, 43]. Technical advancements frequently outpace improvements in transparency, user control, and trust [24].

To address these gaps, we present a Systematization of Knowledge (SoK) on adaptive authentication in mobile environments, analyzing 41 peer-reviewed studies published since 2011. We identify recurring themes such as continuous and passive authentication, behavioral modeling, and risk-aware decision-making [38, 42], along with emerging approaches like gesture- and image-based techniques tailored to mobile contexts [4, 12]. Our **contributions** are twofold: (1) a structured synthesis of over a decade of research on adaptive authentication in mobile environments; and (2) a systematic identification of key challenges, including privacy-preserving models, scalability issues, and the development of a seven-dimension analysis framework.

2 Methodology

To structure our review of adaptive authentication on mobile platforms, we adopted the study designs used in prior systematization efforts [15, 17–19, 26, 29, 33, 34, 44, 51–53, 55–57, 60]. Drawing on recurring technical, behavioral, and ethical themes identified during our preliminary analysis, we formulated the following RQs:

- **RQ1:** How do adaptive authentication systems incorporate contextual and behavioral signals to enhance security and user experience?
- **RQ2:** What ML techniques support real-time decision-making in adaptive authentication, and how are they applied across different systems?
- **RQ3:** What are the primary technical and human-centered challenges that affect the design, deployment, and adoption of adaptive authentication in mobile settings?

2.1 Paper Retrieval and Screening

Search Strategy: We performed a keyword-based search on Google Scholar using combinations of terms such as “adaptive authentication” and “mobile devices.” Our search covered publications since 2011 that returned 342 papers across the fields of cybersecurity, mobile computing, AI, and HCI. We then collected relevant papers from a variety of digital libraries and repositories. Table 1 shows the distribution of papers we gathered from each digital library source.
Screening Process: We applied a multi-phase filtering process involving title, abstract, and full-text screening. We removed 68 papers for being non-English, inaccessible, duplicates, or lacking core metadata, retaining 274 for further analysis. Abstract screening eliminated studies unrelated to adaptive authentication in mobile contexts such as those focused only on static biometrics or general security, resulting in 52 papers.
Full-Text Review: We then evaluated each of the 52 papers in detail, selecting 41 that aligned with our criteria: peer-reviewed, English-language, and focused on adaptive authentication for mobile platforms. The final corpus included works addressing system architecture, adaptive mechanisms, user behavior modeling, and risk-based control strategies. The first authors of the paper went through the paper collection and screening process.

Table 1. Distribution of Collected Papers by Publisher

Publisher	**Number of Papers**
ieeexplore	57
dl.acm.org	11
Springer	28
Elsevier	17
academia.edu	10
arxiv.org	6
search.proquest.com	16
researchgate.net	9
mdpi.com	12
Other	86
Unknown Source	22
Total	**274**

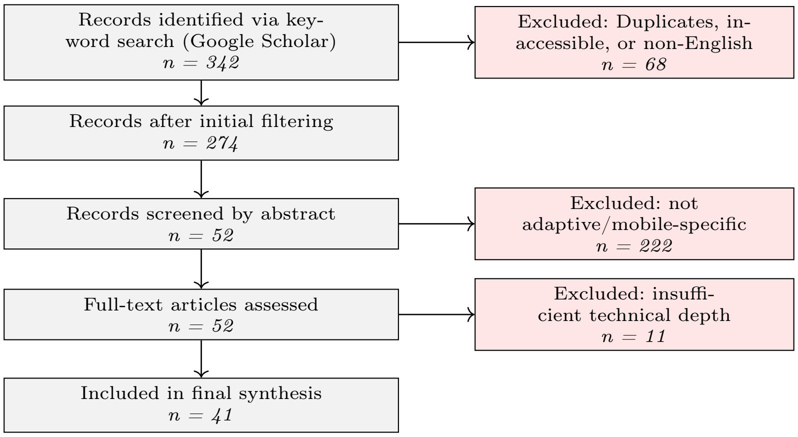
Records identified via keyword search (Google Scholar)
n = 342
Excluded: Duplicates, inaccessible, or non-English
n = 68
Records after initial filtering
n = 274
Records screened by abstract
n = 52
Excluded: not adaptive/mobile-specific
n = 222
Full-text articles assessed
n = 52
Excluded: insufficient technical depth
n = 11
Included in final synthesis
n = 41

Fig. 1. Overview of the Paper Retrieval and Filtering Stages Used in the Systematic Review of Adaptive Authentication Studies in Mobile Environments.

2.2 Analysis

To guide our analysis, we developed a comprehensive codebook combining insights from prior surveys with themes that emerged during our review. We organized the codebook around seven core dimensions. Each dimension includes subcodes that capture specific technical strategies and user interaction patterns. The first dimension, *Privacy and Security Models*, focuses on the foundational goals of authentication system design, such as risk-aware mechanisms, continuous behavioral tracking, and device-level access control [10, 11, 39, 49]. The second dimension of *Interaction Modalities* explores how users engage with authentication systems, including gesture-based inputs [46, 50], sensor-triggered responses [20, 45], passive background verification [40, 54], and adaptive prompts based on perceived risk [21, 47].

Through the third dimension, *User Behavior* we capture when and how authentication is triggered, encompassing continuous background authentication [12, 25], event-based triggers [4, 48], and spatio-temporal strategies responsive to location and time [10, 47]. In the fourth dimension of the *Risk Perception*, we address how users and systems assess cybersecurity threats, covering trust, privacy trade-offs, and concerns over false positives and negatives [3, 39, 49, 54].

In the *Implementation Challenges* we document the barriers to effective deployment, including user resistance to frequent prompts, lack of algorithmic transparency, and hardware or sensor limitations [1, 20]. Via the sixth dimension of *Usability Needs* we examine how systems accommodate user expectations, focusing on interface design [21, 28], adaptive security behaviors [4, 40], and multimedia-based authentication [48, 59]. Finally, in the *Machine Learning Frameworks* we cover the algorithms supporting adaptive authentication, including behavioral modeling [4, 12], real-time risk scoring [25, 49], anomaly detection [2, 45], and hybrid AI architectures [4, 49]. From a total of 175 subcategories, we report the 35 most impactful based on their contribution to key thematic dimensions (Table 2). We collaboratively refined the codebook and piloted it on ten papers using axial and thematic coding, achieving strong intercoder reliability (Cohen's Kappa = 0.85) before applying it to the full dataset.

3 Results and Discussion

3.1 Behavioral Security Architectures and Risk-Based Control

Our analysis reveals a significant shift from traditional rule-based security towards behavior-driven and risk-adaptive models. One of the most common feature among the 41 studies was *Unauthorized Access Prevention*, cited in 54.8% of papers. These implementations emphasize active threat detection through monitoring behavioral deviations or unauthorized context switching (e.g., unusual app access or device handoff). Machine Learning-Based Authentication, found in 64.3% of the papers, highlighting the field's strong interest in adaptive, environment-aware authentication methods. *Risk-Based Access Control* is a suggested access-control and authentication mechanism, however it was only applied in 40.5% of papers, where the researchers' didn't use real-time scoring models to elevate access restrictions.

A notable trend was the adoption of *Context-Aware Authentication* (42.8%), in which the authentication mechanism adapts based on user location, activity state, or network conditions. Systems that paired this with *Passwordless Authentication* (40.5%) and *Continuous Authentication* (61.9%) emphasizing the importance of ongoing identity verification. These behavior-aware security models form the backbone of most modern adaptive authentication architectures. They often operate in tandem with environmental sensing modules, continuously evaluating biometric, kinetic, and spatio-temporal patterns to determine access legitimacy with minimal friction. This progression reflects an increasing emphasis on dynamic, user-centric security frameworks that respond to real-time

Table 2. Distribution of Subcategories Of the Seven Focus Areas Based on their Impact Vector

Category	Sub-Code	Percentage (%)
Privacy and Security Models	Machine Learning-Based Authentication	64.29
	Continuous Authentication	61.90
	Unauthorized Access Prevention	54.76
	Multi-Factor Authentication (MFA)	45.24
	Context-Aware Authentication	42.86
Interaction Modalities	AI-Based Anomaly Detection	57.14
	Spatio-Temporal Analysis	52.38
	Background Validation	50.00
	Adaptive Security Models	40.48
	Sensor-Based Authentication	40.48
Usage Behavior	Location-Based Adjustments	47.62
	Risk-Adaptive Authentication Frequency	45.24
	Movement Validation	40.48
	Real-Time Interaction-Based Security	40.48
	Seamless Reauthentication	33.33
Implementation Challenges	Privacy-Preserving Models	66.67
	Fatigue Mitigation	52.38
	Authentication Complexity Scaling	50.00
	Frictionless Authentication	40.48
	Regulatory Compliance	28.57
Usability Needs	Context-Aware Prompts	54.76
	Passive Biometric Integration	52.38
	Non-Intrusive Authentication Mechanisms	47.62
	Movement Recognition	28.57
	Hybrid Biometric & Behavioral Authentication	21.43
Risk Perception	Privacy-Preserving Authentication Solutions	76.19
	Behavioral Tracking Concerns	50.00
	False Positives in ML Authentication	38.10
	Ethical AI Practices	23.81
	Surveillance Concerns	19.05
Machine Learning Frameworks	Access Control Decisions	45.24
	Behavioral Classification	35.71
	Risk Score Computation	33.33
	Context-Aware Frameworks	30.95
	Behavioral Analysis	30.95

behavioral and contextual cues. By integrating multiple signals, these architectures aim to balance robust security measures with seamless user experience.

3.2 Sensor Fusion and Passive User Interaction

On the interaction layer, adaptive systems rely on multimodal passive input to evaluate user authenticity. *Sensor-Based Authentication* was the one of the cited technique in this category (40.5%), leveraging IMU sensors (accelerometer, gyroscope, magnetometer) to extract implicit motion signatures associated with legitimate users. *Continuous Biometric Verification* was used in 26.2% of systems, combining facial analysis, gait recognition, keystroke dynamics, and touch interaction patterns for persistent authentication. Systems often employed local caching and edge-based analysis to ensure low-latency performance while respecting computational limits on mobile devices.

Motion-Based Authentication (26.2%) and *Behavioral Deviation Alerts* (14.3%) played a supplementary role in risk escalation protocols, primarily serving as secondary triggers for additional verification such as challenge prompts or multi-factor authentication when deviations from routine usage patterns were detected. *Seamless Reauthentication Mechanisms* were present in 23.8% of the systems. These mechanisms continuously updated user state in the background and revoked or adjusted access policies without interrupting workflows. Combined with *Real-Time Interaction-Based Security* (40.5%), these systems ensured that authentication adapted fluidly to user activity with minimal manual input. The convergence of gesture, movement, and environmental sensing illustrates a shift toward pervasive, real-time verification models in mobile security, designed to operate ubiquitously and invisibly within the mobile ecosystem. This highlights the growing emphasis on continuous, context-aware user validation strategies to enhance both usability and security in adaptive authentication systems.

3.3 Machine Learning Models for Context and Threat Inference

Machine learning emerged as the core engine for context classification, behavioral profiling, and threat detection in adaptive authentication. *Context-Aware Authentication Frameworks* were used in almost all of reviewed systems, enabling devices to synthesize multi-source input including app usage, motion, and temporal behavior into a continuously updating user trust model. This was obvious given the nature of the studies we evaluated. *Real-Time Risk Score Computation* was used in 33.3% of studies, typically employing supervised learning classifiers to infer session trustworthiness from time-series features. These scores modulate authentication stringency on a continuous scale, enabling frictionless access in low-risk contexts while invoking challenge mechanisms in high-risk conditions.

Multi-Factor Risk Analysis (14.3%) and *Fraud Detection in Authentication Requests* (11.9%) applied ensemble techniques, combining spatial location, sensor activation patterns, biometric traits, and usage trends to detect anomalies indicative of spoofing or unauthorized access attempts. *Longitudinal Behavioral*

Category	Name	Machine Learning-Based Authentication	Continuous Authentication	Unauthorized Access Prevention	Multi-Factor Authentication (MFA)	AI-Based Anomaly Detection	Spatio-Temporal Analysis	Background Validation	Adaptive Security Models	Location-Based Adjustments	Risk-Adaptive Authentication	Location-Based Authentication Adjustments	Risk-Adaptive Authentication Frequency	Movement-Based User Validation	Real-Time Interaction-Based Security	Privacy-Preserving Authentication Models	Authentication Fatigue Mitigation	Continuous, Non-Intrusive Authentication	Gesture & Proximity-Based Authentication	Privacy-Preserving Authentication Solutions	User Concerns Over Behavioral Tracking	Resilient to Physical Observation	False Positives in Authentication	Ethical AI Practices	Permission Mismanagement Risks	Behavioral Classification	Real-Time Risk Score Computation	Context-Aware Authentication Frameworks
Impln. Challenges	ML-Based [6]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Review [8]	●	❍	●	●	❍	●	❍	●	●	●	❍	-	●	❍	●	❍	●	❍	●	●	❍	❍	❍	❍	●	❍	●
	Risk-Aware [35]	●	●	❍	❍	❍	●	❍	●	❍	●	❍	●	❍	●	❍	●	❍	●	●	❍	❍	●	●	❍	●	❍	●
	ML-Based [7]	●	❍	●	●	●	●	❍	●	●	❍	-	●	❍	●	●	❍	❍	-	❍	●	❍	❍	●	❍	●	❍	●
	IoT-Security [5]	❍	❍	●	❍	❍	●	❍	❍	❍	❍	●	❍	❍	●	●	●	❍	●	❍	❍	❍	❍	❍	●	❍	❍	❍
	ML-Based [31]	●	❍	●	❍	●	❍	❍	●	●	❍	●	❍	●	●	❍	❍	●	❍	❍	❍	●	●	●	❍	❍	❍	●
	Continuous [42]	●	●	❍	●	●	❍	❍	❍	●	❍	❍	❍	❍	●	❍	●	●	❍	❍	●	❍	●	●	❍	❍	❍	●
	Survey [22]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	ML-Based [49]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Conceptual [21]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Fusion [40]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Hardware-Based [45]	●	❍	●	●	❍	●	❍	❍	●	●	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Multi-Factor [48]	●	❍	●	●	❍	❍	●	●	❍	❍	-	❍	●	●	●	❍	❍	-	●	❍	❍	❍	●	●	●	❍	●
	Malware [2]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	❍	❍	●	●
	Factors [27]	●	❍	●	●	❍	❍	❍	❍	❍	●	-	❍	❍	●	●	●	❍	●	❍	❍	❍	❍	●	❍	●	❍	❍
	Identity-Based [28]	●	●	❍	●	❍	●	❍	❍	●	❍	-	●	●	●	●	❍	❍	-	❍	❍	❍	❍	●	●	❍	❍	●
	Location-Based [10]	●	❍	●	●	●	❍	●	❍	●	●	❍	-	❍	❍	❍	❍	●	❍	❍	●	●	❍	❍	●	❍	●	●
	ZeroTrust [39]	❍	❍	❍	●	❍	●	❍	❍	●	❍	❍	●	❍	❍	●	❍	❍	❍	●	●	❍	●	❍	❍	❍	❍	●
	Biometric [12]	●	❍	●	❍	●	❍	❍	●	●	❍	-	❍	●	❍	●	●	●	❍	●	❍	●	❍	❍	❍	●	❍	●
Privacy & Security Models	Context-Aware [32]	●	❍	❍	❍	●	●	❍	●	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	Privacy [11]	●	❍	●	●	❍	❍	●	●	❍	●	-	❍	●	●	●	❍	❍	❍	❍	❍	●	❍	●	❍	❍	❍	●
	Profiling [9]	●	❍	●	❍	●	❍	❍	●	●	❍	-	❍	●	❍	●	❍	❍	-	❍	❍	●	●	❍	●	❍	❍	●
Risk Perception	Risk-Aware [13]	❍	❍	❍	❍	●	❍	❍	❍	●	●	●	❍	●	❍	❍	❍	❍	❍	❍	❍	❍	●	●	❍	❍	❍	●
	Risk-Based [36]	●	❍	●	❍	❍	●	●	❍	❍	●	❍	●	●	❍	❍	❍	❍	●	●	❍	❍	●	❍	❍	●	❍	●
	Survey [37]	●	❍	●	❍	❍	●	❍	●	●	❍	●	❍	●	●	❍	●	❍	●	❍	❍	●	❍	●	❍	❍	❍	●
Mobile Interaction	Behavior-Based [41]	●	●	●	●	❍	●	●	❍	❍	●	❍	❍	❍	❍	●	●	❍	❍	●	●	❍	❍	●	❍	❍	❍	●
	Biometrics [1]	❍	●	❍	●	●	❍	❍	●	●	❍	-	❍	●	❍	●	●	❍	❍	●	●	●	❍	●	❍	❍	●	❍
	Biometric [50]	❍	❍	●	●	●	❍	❍	●	●	❍	-	●	❍	●	❍	❍	●	-	❍	●	●	❍	❍	●	❍	❍	●
	Face-Based [59]	●	●	❍	●	❍	●	❍	●	●	●	❍	●	❍	❍	●	●	❍	❍	●	❍	❍	●	●	❍	●	❍	●
ML Techniques	Continuous [58]	❍	●	❍	●	❍	❍	❍	●	●	●	❍	●	❍	❍	●	❍	●	●	❍	❍	●	❍	❍	●	❍	●	❍
	ML-Based [4]	●	❍	●	●	❍	●	●	❍	●	●	❍	❍	❍	❍	❍	●	●	❍	❍	●	●	❍	●	❍	●	❍	●
	ML-Based [25]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
	ML-Based [3]	●	❍	●	●	●	●	❍	❍	●	❍	-	❍	❍	●	●	❍	●	-	❍	●	❍	❍	●	●	❍	❍	●
Usage Patterns	Transparent [54]	●	●	❍	❍	●	❍	❍	❍	❍	●	-	❍	●	❍	●	❍	❍	●	❍	❍	●	❍	●	●	❍	❍	●
	Habit-Based [47]	●	❍	●	❍	●	●	❍	❍	●	❍	-	❍	●	❍	●	❍	●	❍	❍	❍	●	●	❍	❍	❍	❍	●
User Needs Assessment	Engineering [23]	●	❍	●	❍	●	❍	●	❍	●	●	❍	●	❍	❍	❍	●	❍	●	●	❍	●	●	❍	❍	●	❍	❍
	Biometric [43]	●	❍	●	❍	●	●	❍	●	❍	●	●	❍	❍	❍	❍	●	❍	●	❍	❍	●	❍	❍	●	❍	❍	●
	Usability [38]	❍	❍	●	●	●	❍	●	❍	●	●	❍	●	❍	●	❍	●	●	●	❍	❍	●	❍	●	❍	❍	❍	●

Names: The mechanism's title as stated in the paper.
Evaluation: ● = method fulfills criterion; ❍ = method quasi-fulfills criterion; – = method does not fulfill criterion;

Table 3. Impact-Oriented Paper-Wise Distribution of Subcategories Within the Seven Core Focus Areas of Adaptive Authentication.

Data Analysis featured in 31.0% of systems, particularly those aiming to establish long-term user baselines. These systems improved detection precision by recognizing gradual changes in usage patterns due to behavioral drift or device sharing. Many papers reported hybrid model architectures: Support Vector Machines (SVMs) were often used for binary classification tasks (e.g., authorized vs. unauthorized), while Random Forests were favored for feature importance modeling. Deep Learning model such as Convolutional Neural Networks (CNNs) for image-based biometrics and Recurrent Neural Networks (RNNs) for time-series modeling were increasingly integrated for multi-modal prediction. This underscores the role of real-time risk scoring as a dynamic mechanism for balancing usability with proactive threat mitigation.

3.4 Systemic Challenges in Adaptive Implementation

Adaptive authentication introduces a complex design space requiring trade-offs between performance, accuracy, usability, and trust. One of the cited challenge was *Adaptive Authentication Complexity Scaling*, observed in 50.0% of studies. Systems often overcompensated for risk, leading to false positives or over-authentication, which impacted user experience. *Privacy-Preserving Authentication Models* appeared in 66.7% of studies, particularly those emphasizing edge-based inference, federated learning, or differentially private model training to minimize exposure of behavioral and biometric data. *False Positives in Authentication Decisions* were reported in 47.7% of papers. This issue was most pronounced in systems relying on hard thresholds or static models that failed to accommodate behavioral variability, such as changes in device handling or physical mobility due to injury or environment.

Regulatory Compliance in Behavioral Tracking and *User Consent & Transparency Measures* were inconsistently implemented across studies, raising ethical questions about silent tracking and unprompted data capture. Papers that addressed these concerns often relied on transparent UI mechanisms or opt-in biometric calibration periods. *Edge Computing for Localized Data Processing* was explored, indicating that its adoption in adaptive authentication remains relatively low. This reflects the continued dominance of cloud-based models, with on-device processing for privacy-preserving authentication yet to achieve widespread implementation. Privacy-preserving models, particularly those using federated learning, offer a promising pathway by enabling collaborative model training across devices without transferring sensitive data to centralized servers.

3.5 User-Centric Considerations and Ethical Design

User trust and system transparency emerged as critical factors in determining adoption. *Continuous, Non-Intrusive Authentication Mechanisms* and *Passive Biometric Integration* were present in over 50.0% of the studies. These approaches prioritized background verification to reduce friction and prevent workflow interruption. *Movement-Based Authentication Recognition* and *Routine-Based Authentication Learning* were used to tailor the system to individual users, allowing the authentication pipeline to learn and adapt to personal routines while maintaining responsiveness. From a permission standpoint, *Risk-Based Permission Allocation* and *Automated Permission Escalation* were employed in 7.0% of studies, automating access rights based on risk context or app behavior rather than static declarations. However, usability enhancements also introduced privacy tensions. *User Concerns Over Behavioral Tracking* and *Surveillance Concerns* were present in over half of the studies. These concerns were especially prominent in systems collecting fine-grained motion or voice data, such as continuous gait recognition or background audio sampling. These findings highlight the delicate balance between delivering seamless authentication and preserving user autonomy, underscoring the importance of ethical design in adaptive systems that learn from behavioral patterns.

3.6 Perceptions of Risk and Ethical AI in Authentication

Risk perception plays a pivotal role in the design and acceptance of adaptive authentication. *Privacy-Preserving Authentication Solutions* were explicitly implemented in 76.2% of the studies, using cryptographic protocols, on-device inference, and anonymous identity vectors to minimize user profiling. Concerns about explainability and bias were also prominent. *False Positives in Authentication Decisions* were reported in 38.1% of the studies, often due to rigid models that failed to adjust thresholds in real time. These errors not only increased user frustration but also eroded system trust. *Ethical AI Practices* were addressed in only 23.8% of papers, indicating a gap in the responsible deployment of machine learning in security contexts. Where mentioned, these practices focused on explainable decisions, demographic fairness, and post-deployment auditing.

User Control Over Permission Revocation and *Opt-Out & Privacy-Safe Alternatives* appeared sporadically, suggesting the need for greater emphasis on transparency and consent in future research. The lack of such controls may hinder the adoption of otherwise technically sound systems, particularly in sensitive sectors like healthcare and border security. Table 3 provides overview of the papers that focused on the different aspects of our studied elements. The limited focus on ethical AI practices reveals a critical research gap, emphasizing the need for adaptive authentication systems that not only perform accurately but also align with evolving societal expectations around fairness, accountability, and transparency.

4 Implications

In this work, we report on adaptive authentication research for mobile platforms and highlights key implications for design, user trust, policy, and future development. Based on our analysis, we offer the following recommendations.

4.1 Designing Context-Aware Security Frameworks

The convergence of passive biometric sensing, spatio-temporal data, and machine-learned behavior profiling presents a powerful design paradigm for adaptive authentication. However, the overreliance on static decision thresholds and rigid rule-based triggers (as seen in 47.7% of systems encountering false positives) underscores the need for adaptive threshold calibration mechanisms that dynamically evolve based on longitudinal usage and contextual cues. Moreover, the frequent adoption of real-time risk-based access control (found in over 40.5% of systems) illustrates the transition away from one-size-fits-all security models. Developers and system architects should prioritize modular risk engines that integrate seamlessly with mobile OS-level services, offering scalable protection with granular, behavior-conditioned control.

4.2 Balancing Privacy, Utility, and Transparency

While over 66.6% of systems implemented some form of privacy-preserving authentication model, our review highlights a persistent gap in transparency and user agency. Less than 40% of studies explicitly addressed mechanisms for user-informed consent, opt-out paths, or permission revocation interfaces. This exposes a critical trust bottleneck in the deployment of always-on security systems. Future implementations must address this by incorporating explainable authentication pipelines communicating what data is collected, how risk is assessed, and when access decisions are altered. Integrating user-adjustable sensitivity profiles and visual feedback mechanisms may mitigate behavioral surveillance concerns while improving user acceptance.

4.3 Operationalizing Adaptive Authentication at Scale

Despite the promising use of hybrid ML models including CNNs, RNNs, and ensemble methods, practical deployment remains hindered by edge limitations, battery constraints, and inconsistent sensor reliability. Only 50% of papers addressed on-device inferencing strategies, despite growing user concerns over cloud-based behavioral profiling. This implies a critical need for lightweight, on-device ML architectures, particularly in resource-constrained mobile environments. Federated learning, compressed neural networks, and edge-optimized anomaly detection present viable avenues for future research. In tandem, system developers should engineer fail-safe reauthentication fallbacks to ensure robustness in case of model failure or sensor dropout.

4.4 Policy and Standardization for Ethical Security AI

The review identifies inconsistent regulatory compliance across studies, less than 30% of systems acknowledged frameworks like GDPR, HIPAA, or CCPA, despite their relevance to biometric and behavioral data. As adaptive authentication increasingly relies on sensitive spatio-temporal and motion data, adherence to evolving legal standards becomes essential. To align system design with public interest, researchers and policymakers must co-develop standardized audit frameworks and accountability protocols for AI-based mobile authentication systems. Moreover, only 28.6% of systems discussed fairness, explainability, or bias mitigation, highlighting an urgent call for algorithmic transparency guidelines and periodic ethical reviews of deployed models, especially in high-risk domains such as border control, finance, and health access systems.

5 Future Work and Limitations

We focused our review on English-language, peer-reviewed literature, which may have excluded valuable research in other languages. To broaden the scope, we will incorporate multilingual sources and perspectives from underrepresented regions. We also found that many studies relied on pre-collected datasets or simulations rather than real-world deployments. To address this, we will prioritize in-situ evaluations and contribute to the development of standardized benchmarks.

6 Conclusion

We conducted a systematic review of 41 peer-reviewed studies on adaptive authentication in mobile environments and identified clear trends in technical design, user interaction, and ethical integration. Our results show that while 64.3% of systems incorporated machine learning-based authentication, only 33.3% implemented real-time risk score computation. Continuous authentication appeared in 61.9% of papers, yet only 23.8% supported seamless re-authentication mechanisms, revealing gaps in usability and workflow integration. We observed that 52.4% of studies utilized spatio-temporal analysis, and 57.1% applied anomaly detection techniques. However, only 30.95% developed context-aware frameworks capable of adaptive response to user behavior. Privacy-preserving authentication models were reported in 66.7% of systems, but less than one-third addressed regulatory compliance or user transparency. Additionally, while false positives impacted 38.1% of implementations, few systems introduced mechanisms for dynamic threshold calibration or behavioral drift adaptation. Our analysis highlights a field advancing in technical sophistication, yet limited by inconsistent support for user consent, explainability, and deployment scalability.

7 Acknowledgement

We gratefully acknowledge the anonymous reviewers for their valuable feedback and insightful suggestions, which have significantly enhanced the clarity and rigor of this systematization of knowledge. We extend our thanks to George Mason University for its institutional support and the resources that facilitated this comprehensive literature review. In addition, we express our gratitude to the researchers whose foundational work on adaptive authentication has been critical to this study; their pioneering contributions continue to shape and advance the evolving landscape of mobile security.

References

1. Agrawal, R., Sharma, P.: A study of touch dynamics biometrics authentication. International Journal of Scientific Research in Engineering and Management (IJSREM) **6** (2022)

2. Ahmad, N.: Navigating evolving mobile malware threats: Advanced strategies for defense adaptation (2024)
3. Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K.: Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications **61**, 59–80 (2016)
4. Anand, S., Miglani, S.: Ai-enhanced multi-layer security: Implementing a 3-level image-based authentication system on mobile devices. International Journal of Computer Applications **975**, 8887 (2024)
5. Arab, A., Jaber, G., Bouabdallah, A.: Towards adaptive security for mobile iot. In: Proceedings of TS3 (2024)
6. Arias-Cabarcos, P., Krupitzer, C., Becker, C.: A survey on adaptive authentication. ACM Computing Surveys (CSUR) **52**, 1–30 (2019)
7. Ayyal Awwad, A.M.: An adaptive context-aware authentication system on smartphones using machine learning. International Journal of Safety & Security Engineering **13** (2023)
8. Bakar, K.A.A., Haron, G.R.: Adaptive authentication: Issues and challenges. In: Proceedings of WCCIT (2013)
9. Baseri, Y., Hafid, A.S., Makrakis, D.: Privacy-enhanced adaptive authentication: User profiling with privacy guarantees. arXiv preprint arXiv:2410.20555 (2024)
10. Berbecaru, D.: Lrap: A location-based remote client authentication protocol for mobile environments. In: Proceedings of PDP Conference (2011)
11. Bonazzi, R., Fritscher, B., Liu, Z., Pigneur, Y.: From “security for privacy” to “privacy for security”. In: Proceedings of ICNGN (2011)
12. Caudill, S.M.C.: The Wyatt Facial Recognition Algorithm: A Constructive Study. Ph.D. thesis, Northcentral University (2023)
13. Chen, J., Hengartner, U., Khan, H.: Mraac: a multi-stage risk-aware adaptive authentication and access control framework for android. ACM Transactions on Privacy and Security **27**, 1–30 (2024)
14. Das, S.: A risk-reduction-based incentivization model for human-centered multifactor authentication. Indiana University (2020)
15. Das, S., Kim, A., Tingle, Z., Nippert-Eng, C.: All about phishing exploring user research through a systematic literature review. In: Proceedings of HAISA (2019)
16. Das, S., Wang, B., Kim, A., Camp, L.J.: Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies. In: Proceedings of HICSS (2020)
17. Das, S., Wang, B., Tingle, Z., Camp, L.J.: Evaluating user perception of multifactor authentication: A systematic review. In: Proceedings of HAISA (2019)
18. Das, S., et al.: Sok: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review. In: Proceedings of USEC (2022)
19. Düzgün, R., Noah, N., Mayer, P., Das, S., Volkamer, M.: Sok: A systematic literature review of knowledge-based authentication on augmented reality head-mounted displays. In: Proceedings of ARES (2022)
20. Gong, N.Z., Payer, M., Moazzezi, R., Frank, M.: Forgery-resistant touch-based authentication on mobile devices. In: Proceedings of ACM (2016)
21. Gupta, S., Buriro, A., Crispo, B.: Demystifying authentication concepts in smartphones: Ways and types to secure access. Mobile Information Systems **2018**, 2649598 (2018)
22. Hasan, S.S.U., Ghani, A., Daud, A., Akbar, H., Khan, M.F.: A review on secure authentication mechanisms for mobile security. Sensors **25**, 700 (2025)

23. Hassan, A., Nuseibeh, B., Pasquale, L.: Engineering adaptive authentication. In: Proceedings of ACSOS-C (2021)
24. Hebbes, L., Chan, C.: 2-factor authentication with 2d barcodes. In: Proceedings of HAISA (2011)
25. Hossain, G., Palaniswamy, P., Challoo, R.: Pattern of success vs. pattern of failure: Adaptive authentication through kolmogorov–smirnov (ks) statistics. (IJARAI) International Journal of Advanced Research in Artificial Intelligence (2016)
26. Huang, Y., Grobler, M., Ferro, L.S., Psaroulis, G., Das, S., Wei, J., Janicke, H.: Systemization of knowledge (sok): Goals, coverage, and evaluation in cybersecurity and privacy games. In: Proceedings of CHI (2025)
27. Jayabalan, M., O'Daniel, T.: A study on authentication factors in electronic health records. Journal of Applied Technology and Innovation (e-ISSN: 2600-7304) **3** (2019)
28. Kamarudin, N.H., Yussoff, Y.M.: Authentication scheme interface for mobile e-health monitoring using unique and lightweight identity-based authentication. In: Proceedings of AIP. vol. 1774. AIP Publishing (2016)
29. Kishnani, U., Madabhushi, S., Das, S.: Blockchain in oil and gas supply chain: a literature review from user security and privacy perspective. In: Proceedings of HAISA (2023)
30. Kishnani, U., Noah, N., Das, S., Dewri, R.: Assessing security, privacy, user interaction, and accessibility features in popular e-payment applications. In: Proceedings of EuroUSEC (2023)
31. Liu, K., Guan, J., Hu, X., Zhang, J., Liu, J., Zhang, H.: Aeaka: An adaptive and efficient authentication and key agreement scheme for iot in cloud-edge-device collaborative environments. arXiv preprint arXiv:2411.09231 (2024)
32. Liu, Z., Bonazzi, R., Pigneur, Y.: Privacy-based adaptive context-aware authentication system for personal mobile devices. Journal of mobile multimedia pp. 159–180 (2016)
33. Majumdar, R., Das, S.: Sok: An evaluation of quantum authentication through systematic literature review. In: Proceedings of USEC (2021)
34. Noah, N., Das, S.: Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. Computer Animation and Virtual Worlds **32**, e2020 (2021)
35. Papaioannou, M., Mantas, G., Essop, A., Cox, P., Otung, I.E., Rodriguez, J.: Risk-based adaptive user authentication for mobile passenger id devices for land/sea border control. In: Proceedings of CAMAD (2021)
36. Papaioannou, M., Mantas, G., Essop, A., Sucasas, V., Aaraj, N., Rodriguez, J.: Risk estimation for a secure & usable user authentication mechanism for mobile passenger id devices. In: Proceedings of CAMAD (2022)
37. Papaioannou, M., Pelekoudas-Oikonomou, F., Mantas, G., Serrelis, E., Rodriguez, J., Fengou, M.A.: A survey on quantitative risk estimation approaches for secure and usable user authentication on smartphones. Sensors **23**, 2979 (2023)
38. Papaioannou, M., Zachos, G., Essop, I., Mantas, G., Rodriguez, J.: Toward a secure and usable user authentication mechanism for mobile passenger id devices for land/sea border control. IEEE Access **10**, 38832–38849 (2022)
39. Park, J.H., Park, S.C., Youm, H.Y.: A proposal for a zero-trust-based multi-level security model and its security controls. Applied Sciences (2076-3417) **15** (2025)
40. Rahman, F., Gani, M.O., Ahsan, G.M.T., Ahamed, S.I.: Seeing beyond visibility: A four way fusion of user authentication for efficient usable security on mobile devices. In: Proceedings of IEEE (2014)

41. Rocha, C.C., Lima, J.C.D., Dantas, M.A., Augustin, I.: A2best: An adaptive authentication service based on mobile user's behavior and spatio-temporal context. In: Proceedings of ISCC (2011)
42. Rybnicek, M., Lang-Muhr, C., Haslinger, D.: A roadmap to continuous biometric authentication on mobile devices. In: Proceedings of IWCMC (2014)
43. Ryu, R., Yeom, S., Herbert, D., Dermoudy, J.: The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. ICT Express **9**, 1183–1197 (2023)
44. Saka, S., Das, S.: Safeguarding in the internet of things age: A comprehensive review of security and privacy risks for older adults. Innovation in Aging **7**, 819 (2023)
45. Salomatin, A.: Method of user identification based on dynamic characteristics of mobile device hardware. In: Proceedings of E3S. vol. 548 (2024)
46. Sejjari, A., Moujahdi, C., Assad, N., Abdelfatteh, H.: Dynamic authentication on mobile devices: Evaluating continuous identity verification through swiping gestures. Signal, Image and Video Processing **18**, 9095–9103 (2024)
47. Seto, J., Wang, Y., Lin, X.: Toward secure user-habit-oriented authentication for mobile devices. In: Proceedings of IEEE (2014)
48. Shah, Y., Choyi, V., Schmidt, A.U., Subramanian, L.: Multi-factor authentication as a service. In: Proceedings of IEEE (2015)
49. Shahzadi, A., Ishaq, K., Nawaz, N.A., Mustafa, G., Khan, F.A.: Enhancing security in mobile cloud computing: An analysis of authentication protocols and innovation. International Journal of Innovations in Science & Technology (2024)
50. Shih, D.H., Lu, C.M., Shih, M.H.: A flick biometric authentication mechanism on mobile devices. In: Proceedings of ICCSS (2015)
51. Shrestha, S., Das, S.: Exploring gender biases in ml and ai academic research through systematic literature review. Frontiers in artificial intelligence **5**, 976838 (2022)
52. Shrestha, S., Irby, E., Thapa, R., Das, S.: Sok: a systematic literature review of bluetooth security threats and mitigation measures. In: Proceedings of EISA (2022)
53. Surani, A., Das, S.: Understanding privacy and security postures of healthcare chatbots. In: Proceedings of CHI (2022)
54. Tanviruzzaman, M., Ahamed, S.I.: Your phone knows you: Almost transparent authentication for smartphones. In: Proceedings of IEEE (2014)
55. Tazi, F., Nandakumar, A., Dykstra, J., Rajivan, P., Das, S.: Sok: Analysis of user-centered studies focusing on healthcare privacy & security. arXiv preprint arXiv:2306.06033 (2023)
56. Tazi, F., Nandakumar, A., Dykstra, J., Rajivan, P., Das, S.: Sok: Analyzing privacy and security of healthcare data from the user perspective. ACM Transactions on Computing for Healthcare **5**, 1–31 (2024)
57. Tazi, F., Shrestha, S., De La Cruz, J., Das, S.: Sok: An evaluation of the secure end user experience on the dark net through systematic literature review. Journal of Cybersecurity and Privacy **2**, 329–357 (2022)
58. Valero, J.M.J., Sánchez, P.M.S., Celdran, A.H., Pérez, G.M.: Machine learning as an enabler of continuous and adaptive authentication in multimedia mobile devices. In: Handbook of Research on Multimedia Cyber Security, pp. 21–47. IGI Global (2020)
59. Vazquez-Fernandez, E., Gonzalez-Jimenez, D.: Face recognition for authentication on mobile devices. Image and Vision Computing **55**, 31–33 (2016)
60. Zezulak, A., Tazi, F., Das, S.: Sok: Evaluating privacy and security concerns of using web services for the disabled population. In: Proceedings of ConPro (2023)