AIPA's International Journal on Artificial Intelligence: Bridging Technology, Society and Policy
ISSN: 3062-097X
Published: 2025

Through the Eyes: A Survey on Gaze-Based Biometric Authentication Systems

Nadir İbrahimoğlu[1*], Furkan Yıldız[2], and Mustafa Kahraman[3]

[1]MSDC Department, Huawei R&D Center, Ankara, Türkiye, ORCID:0000-0003-1189-3054
[2]Papilon Savunma, Ankara, Türkiye, ORCID:0009-0003-1334-1613
[3]MSDC Department, Huawei R&D Center, Ankara, Türkiye, ORCID:0000-0002-7218-9311

ORIGINAL RESEARCH PAPER

Abstract

Eye-based biometric authentication leverages distinctive patterns in users' gaze movements to provide secure, continuous verification and addresses escalating challenges in cybersecurity. This comprehensive review surveys 222 peer-reviewed publications and introduces the first three-dimensional taxonomy of the field spanning: (i) authentication approaches (physiological, behavioral, hybrid), (ii) system platforms (hardware/software/cloud/edge/embedded), and (iii) evaluation aspects (accuracy measures, spoofing resistance, usability). Departing from conventional Human-Computer Interaction (HCI) surveys, our study employs a security-oriented framework informed by adversarial insight alongside a systematic comparative analysis. We evaluate methodologies across deployment platforms ranging from desktop infrared (IR) tracking to Extended Reality (XR) head-mounted displays, using well-crafted datasets (GazeBase, GazeBaseVR, Gaze360, LPW). The analysis yields three central insights. First, physiological cues exhibit temporal stability and strong spoofing resistance; behavioral cues offer adaptive performance that remains robust to calibration on ordinary commodity sensors; and hybrid approaches attain superior performance at the cost of higher complexity. Second, system robustness requires robust liveness and Presentation Attack Detection (PAD) solutions, with multi-modal fusion and template protection essential against presentation, synthetic, and adversarial attacks. Third, cloud and edge architecture can effectively mitigate latency and privacy constraints via on-device inference and privacy-preserving learning methods. These results indicate substantial opportunities in enterprise, XR, automobile, mobile/IoT, and smart-environment applications. We conclude by outlining priority research directions: standardization protocols, privacy-preserving methods, optimization of multi-modal fusion, and longitudinal cross-cultural validation to ensure fairness and robustness in real deployments.

Keywords: gaze-based biometrics, eye movement authentication, behavioral gaze dynamics, hybrid fusion, security evaluation.

1 Introduction

Ongoing digital transformation and increasingly sophisticated cyber threats underscore the need for authentication systems that are both secure and usable. Conventional approaches face challenges: passwords suffer from poor practices and scalable attacks, while token-based systems create single points of failure [1, 2]. Biometric authentication directly associates credentials with individuals, reducing knowledge and possession risks [3]. Gaze-based methods leverage physiological properties and learned behaviors, creating unique signals difficult to impersonate while enabling continuous, transparent authentication [4, 5, 6]. Advances in eye-tracking, computer vision, and machine learning (ML) have enabled real-world gaze authentication across desktops, XR headsets, and cameras [7, 8]. However, challenges remain: individual gaze pattern variability, security-usability-accessibility trade-offs, and modern threats including presentation attacks, synthetic data, and adversarial ML [9, 10, 11]. Continuous data collection raises privacy concerns regarding cognitive and health inferences [12, 13].

This survey systematically reviews two decades of research across multiple academic sources including major databases (IEEE Xplore, Springer Link, ScienceDirect, ACM Digital Library, MDPI), conference proceedings, and preprint repositories. After deduplication and screening, 222 peer-reviewed papers on gaze-based authentication were retained and grouped along three axes: methodology (physiological/behavioral/hybrid), architecture (hardware/software/cloud/edge/embedded), and evaluation/security (metrics, PAD, usability). Unlike existing HCI-focused surveys, this work emphasizes engineering trade-offs, security threat models, and systematic comparative analysis [14]. Inclusion criteria prioritized gaze-based verification/identification

OPEN ACCESS
AIPAJ Vol:1, Issue:2

***Corresponding author**
nebrahimpour@ktu.edu.tr

***Submitted** 10 June 2025*

***Accepted** 28 August 2025*

Citation
İBRAHİMOĞU, N., Furkan, Y., Mustafa, K. (2025). Through the Eyes: A Survey on Gaze-Based Biometric Authentication Systems. AIPA's International Journal on Artificial Intelligence: Bridging Technology, Society and Policy, 1(2). DOI: 10.5281/zenodo.17191813

studies with clear protocols and metrics, plus system implementation and usability papers. Exclusion criteria removed gaze estimation-only works, non-peer-reviewed sources, and methodologically insufficient studies. Studies were mapped to datasets (GazeBase, GazeBaseVR, Gaze360, LPW) [15, 16, 17, 18] and attack models, enabling systematic comparisons and gap identification. Despite extensive research, the field lacks a comprehensive engineering-based taxonomy combining approaches, architectures, and security evaluations [5, 12]. This review addresses this gap with a three-dimensional framework encompassing methodologies, system architectures, and evaluation/security considerations, supported by practitioner-focused tables and a research agenda.

The main contributions of this review include a systematic literature review of 222 peer-reviewed articles from multiple academic sources including major databases, conference proceedings, and scholarly repositories, providing comprehensive coverage of the field. We present a tri-dimensional taxonomy structuring the field by authentication methods, system architectures, and security/evaluation frameworks, which enables systematic cross-approach comparisons. In addition, we conduct a capability analysis that maps existing technological capabilities, key constraints, and trade-offs, yielding an analytical perspective that extends beyond descriptive accounts. We identify research trends and future research directions through examination of latest developments and practical application requirements. Finally, we provide practical guidelines with recommendations for next-generation system development, including clear guidelines for constraint mitigation and methodology selection appropriate for specific deployment scenarios.

This survey offers comprehensive review of 222 peer-reviewed papers with three-dimensional categorization combining methodologies/architectures/evaluation, comparative analysis emphasizing trade-offs, and systematic design guidance incorporating emerging Artificial Intelligence (AI)/Augmented Reality (AR)/edge computing trends. We propose a taxonomy addressing literature fragmentation through three dimensions: (1) authentication techniques—physiological patterns, behavioral dynamics, and hybrid fusion systems; (2) architectures—hardware-based, software-based, cloud-based, and embedded systems; (3) evaluation methodologies—accuracy metrics, security assessment, and usability considerations. This framework enables systematic comparison, gap identification, and informed design choices across applications. The survey structure follows this framework: Section 2 reviews methodologies; Section 3 analyzes system architectures; Section 4 covers evaluation and security; Section 5 summarizes applications; Section 6 highlights challenges and future directions; Section 7 offers practitioner guidelines; Section 8 concludes.

Prior surveys examined gaze in security and HCI contexts, emphasizing interaction, privacy, and usability rather than unified engineering taxonomy [12]. Others focused on competitive evaluations or specific methodological threads [5], while broader XR/biometrics surveys discuss gaze within multimodal authentication but don't systematize gaze-only landscapes [19]. This survey differs by: (1) introducing three-dimensional taxonomy spanning methodology, architecture, and evaluation/security; (2) operationalizing security through threat-centric views (PAD, liveness, synthetic/generative, adversarial ML, template security); (3) connecting methodology to deployment constraints and usability; and (4) providing systematic comparative analysis supporting reproducibility and design choices.

2 Gaze-Based Authentication Methodologies

This section evaluates authentication schemes by our taxonomy's first dimension, examining physiological, behavioral, and hybrid methods for extracting biometric characteristics from gaze signals. We analyze theoretical foundations, real-world deployments, and comparative performance characteristics impacting suitability for various application domains.

2.1 Physiological Gaze Patterns

Physiological gaze patterns leverage stable anatomical and neural characteristics of the human visual system that are difficult to consciously manipulate, providing robust biometric features for authentication across various conditions [5, 20]. The human eye's anatomical structure provides distinctive, lifetime-stable biometric features. Modern eye-tracking technology enables anatomical feature extraction during routine gaze tasks, combining anatomical and behavioral analysis. The key challenge involves extracting sufficient detail from lower-resolution images while maintaining discriminatory power through advanced processing techniques compatible with commercial eye-trackers. Iris structure analysis preserves characteristic textural patterns from muscle fibers, crypts, furrows, and pigment variations. While accuracy remains lower than dedicated iris devices, combining iris analysis with gaze verification enables multi-modal systems integrating anatomical and behavioral features [4, 21, 22, 23]. Pupil morphology examination analyzes shape, size, and dynamic properties showing individual variability, with properties like baseline diameter, asymmetry, and response characteristics facilitating verification using standard eye-tracking equipment [24].

The oculomotor system's biomechanical and neurological properties create individual-specific eye movement patterns that are difficult to counterfeit. These physiological characteristics, including muscle fiber composition, neural organization, and sensory capabilities, form the basis for authentication features inherently resistant to conscious manipulation or behavioral mimicry [20]. The oculomotor system exhibits several distinctive characteristics suitable for authentication. Saccadic main sequence characteristics show significant individual differences in the velocity-amplitude relationship, with consistent slope, intercept, and variability patterns over time serving as effective authentication signatures [20]. Smooth pursuit gain and latency measurements reveal individual variability in tracking moving stimuli, where the pursuit gain (eye velocity to target velocity ratio) and onset latency provide biometric markers reflecting neural processing capacity that resist conscious manipulation [25].

Fixational eye movements (drift, tremor, microsaccades) reveal idiosyncratic characteristics difficult to control intentionally, exemplifying involuntary aspects of ocular movement. These movements maintain visual stability during fixation attempts, with individual differences in frequency, amplitude, directional bias, and temporal profiles providing unique biometric signatures. Microsaccades show particularly valuable authentication properties through interindividual differences in rate, amplitude distribution, and directional anisotropy. These properties exhibit intra-individual stability yet substantial inter-individual variability, making them well suited for authentication scenarios that require robustness against deliberate manipulation. However, authentication using fixational movements requires highly accurate measurement devices capable of discriminating small amplitude movements [20].

Pupil dynamics provide biophysiological information reflecting individual differences in autonomic nervous system function and cognitive processing. Pupil responses to light and cognitive demands create robust biometric signatures that are largely involuntary and difficult to manipulate [26]. Pupillary light reflex features (response latency, constriction amount, recovery time) show individual variability with temporal consistency. Direct and consensual light reflexes demonstrate inter-individual differences in amplitude, duration, and symmetry. These automatic responses resist conscious manipulation and remain robust to mental/emotional state variations, integrating easily into routine eye-tracking procedures [27]. Cognitive pupillary responses reflect mental effort and attentional demands, showing individual differences in dilation magnitude, latency, and recovery dynamics. These involuntary physiological responses to cognitive challenges resist conscious control while revealing individual cognitive processing patterns [28]. Hippus (spontaneous pupil fluctuations under stable illumination) exhibits individual oscillation frequencies, amplitudes, and temporal patterns reflecting neural regulation of pupillary function. These involuntary oscillations provide continuous biometric information resistant to conscious control, valuable for anti-spoofing applications. Analysis reveals distinctive features including oscillation frequency, amplitude distribution, and temporal regularity [29].

2.2 Behavioral Gaze Dynamics

Behavioral gaze dynamics encompass learned eye movement patterns shaped by individual experience, cognitive style, and attention strategies [5, 30]. While humans share basic oculomotor mechanisms, gaze deployment shows significant individual differences due to learning experiences, cultural factors, and cognitive processing strategies. Unlike physiological patterns reflecting anatomical traits, behavioral dynamics involve higher-level cognitive processes in attention allocation and visual navigation. Individuals develop specific visual exploration preferences for different stimuli and tasks, creating measurable behavioral profiles reflecting spatial attention preferences, temporal sequences, and task-specific strategies. Behavioral approaches offer hardware robustness, calibration tolerance, and compatibility with less accurate devices, making them suitable for consumer applications [31].

2.2.1 Fixation Pattern Analysis

Fixation pattern analysis reveals individual differences in visual attention allocation and information processing, creating biometric signatures [5]. This analysis quantifies spatial attention distribution and temporal allocation aspects including fixation duration, sequences, and attention transitions [32]. Patterns emerge from interactions between bottom-up visual saliency and top-down cognitive control. Spatial fixation allocation reveals individual preferences for attention distribution across visual stimuli, reflecting cognitive styles and exploratory strategies. Individuals show consistent tendencies: some exhibit center-biased patterns while others use peripheral exploration strategies. These spatial preferences demonstrate high inter-session consistency, providing reliable authentication features analyzable through heat maps, center-of-mass computation, and statistical modeling [33]. Fixation clustering analysis reveals individual attention distribution strategies. Some subjects exhibit tight clustering for detailed analysis, while others show diffuse patterns for broad scene exploration. Clustering amount, dimensions, inter-cluster distances, and formation dynamics provide quantitative measures of attentional styles. Metrics like Davies-Bouldin index and silhouette measures enable precise attention pattern characterization [34].

Fixation duration properties show individual differences reflecting cognitive processing time and information retrieval strategies. Duration statistics (mean, variance, skewness) create time-based biometric signatures The consistency found within-subjects is in contrast to variability between users. Some users exhibit a trend for shorter durations reflecting fast processing, whereas others have longer durations reflecting detailed information extraction. These distinguishable patterns are related to reading speed, processing ability, attentional control, and task-related strategies [35]. The temporal aspects involve cognitive processes and behavioral patterns difficult to intentionally modify, thus allowing consistent biometric identification from natural gaze behaviors [36]. Fixation duration patterns utilize statistical methods such as distribution fitting and machine learning models [37]. The analysis of sequential fixations reveals individual variability by changes in temporal dynamics and positional changes, reflecting higher-order cognitive processes such as planning and attentional control. Computational methods such as Markov chain modeling, sequence alignment, and transition probability matrices are applied to measure unique exploratory patterns reflecting higher-order cognitive processes difficult to manipulate [38]. Fixation density mapping generates heat map displays of distributions of attention, revealing unique spatial patterns by aggregating locations and durations to create holistic behavioral authentication profiles.

2.2.2 Saccadic Behavior Characteristics

Saccadic behavior varies systematically with exploration strategies, attentional control, and cognitive styles. Individuals show differences in amplitude distributions, directional biases, temporal dynamics, and coordination with other movements. These features integrate learned strategic components with biomechanical constraints, yielding distinctive exploration profiles that reflect cognitive styles and visual habits [39]. Saccadic amplitude preferences reflect individual information acquisition strategies. Some prefer frequent small saccades for detailed local analysis, while others use longer saccades for rapid scene exploration. Amplitude distribution characteristics (mean, variance, skewness) provide consistent individual attributes across viewing tasks, modulated by visual acuity, attention span, and processing rate [40]. Directional saccadic patterns reveal individual preferences in eye movement directionality during visual exploration, reflecting cognitive approaches and culturally transmitted behaviors. Examining saccade direction distributions—horizontal versus vertical preferences, clockwise versus counterclockwise tendencies, and visual field quadrant asymmetries—reveals individual biometric markers. These directional preferences result from reading habits, cultural spatial attention models, occupation-based exploration strategies, and inherent spatial cognitive differences, forming consistent behavioral signatures across viewing conditions and stimulus types [41].

Saccadic velocity profiles, although ultimately constrained by physiology, exhibit characteristic patterns with pronounced inter-individual differences that reflect the oculomotor system's biomechanical properties and associated neuronal control processes. Profile parameters—including acceleration and deceleration intervals, overall duration, and symmetry—vary across individuals in ways that are informative for authentication. These features capture automatic components of the eye-movement control system [42]. Inter-saccadic interval analysis examines the timing between successive saccades, revealing individual differences in visual processing speed, decision making, and cognitive control. Summary statistics such as means, variances, distributional skewness, and preferred interval ranges yield temporal identifiers that mirror processing capacity and control strategies. Such temporal variations indicate efficiency of visual processing, capacity to reorient attention, and choice of cognitive strategy, producing robust behavioral signatures that are difficult to willfully manipulate [43]. Overshoot and undershoot tendencies further expose individual accuracy in oculomotor control and motor strategy. Systematic propensities to overshoot or undershoot—quantified by frequency, magnitude, and the nature of corrective responses—form profiles that remain stable across sessions and tasks, providing distinctive attributes (e.g., error magnitude, directional consistency, compensation speed, and control strategy) that are particularly useful for authentication because they reflect automatically controlled oculomotor dynamics not amenable to intentional manipulation [44].

2.2.3 Scanpath and Visual Search Method Analysis

Scanpath analysis characterizes inter-individual differences in visual exploration by systematically examining sequences of eye movements during visual tasks. By integrating spatial, temporal, and sequential gaze features, it yields coherent behavioral profiles that describe cognitive strategies and perceptual biases. Emergent scanpath patterns arise from interactions among stimulus properties, task demands, and cognitive predispositions, capturing strategic visual behaviors that are difficult to modulate—including exploration style, cognitive bias, and variation in attentional control. The method produces broad behavioral signatures spanning spatial coverage, temporal dynamics, sequential structure, and adaptive processes that support information retrieval [45].

Scanpath similarity measures quantify visual search behavior across users and sessions to support construction of computational models. The Needleman–Wunsch algorithm computes optimal sequence alignments, revealing common subsequences and variations in exploratory behavior. The Levenshtein distance measures the minimum operations required to transform one scanpath into another, capturing structural similarity and discrepancies in exploration strategy. Specialized comparison techniques include dynamic time warping for temporal variability, string-based encodings for sequential structure, and graph-based methods for spatial relations. These approaches detect characteristic exploration patterns while accommodating timing variability and spatial imprecision. Similarity measures enable authentication mechanisms to discriminate among users while remaining robust to within-user session variability [46]. The effectiveness of visual search can be analyzed via the ratio of search effort to search information. In this work, we consider search effectiveness, coverage patterns, and completion rate to examine individual variation in visual search strategy. Variations in inattentional control and strategic search behaviors serve as individual behavioral signatures [47].

Patterns of attention transition investigate visual attention structure that controls gaze direction allocation and adjustment during exploration activities. These patterns consist of revisitation propensities, systematic or opportunistic exploration of novel regions, and strategic scene exploration that reflect individual cognitive profiles and perceptual styles. Patterns can be characterized by individual differences in working-memory utilization, curiosity levels, novelty-seeking tendencies, and preferences for global versus local exploration protocols. The exploitation–exploration trade-off leaves distinctive behavioral traces valuable for verification. Analyses extract time and rate of revisitation, the spatiotemporal organization of exploration sequences, and adaptive responses to exploratory demand or scene complexity, thereby revealing the cognitive processes governing visual attention control [48].

Temporal scanpath characteristics assess the timing of visual exploration, including exploration duration, information-gathering rate, and attention allocation. Analyses reveal inter-individual differences in processing speed, cognitive efficiency, and information-seeking strategies. Some participants exhibit rapid, effective exploration, whereas others adopt systematic, attentive approaches. These temporal descriptors delineate exploration rhythm, distributions of attentional concentration, transition rates, and the temporal organization of fixation sequences, thereby characterizing distinct cognitive processing styles [49]. Scanpath complexity metrics capture structural properties of visual exploration such as path length, convex hull area, and fractal dimension. These measures provide compact summaries of individual exploration strategies, highlighting spatial and organizational properties relevant for authentication. Path length indexes exploration speed and efficacy; convex hull area reflects spatial coverage (dense versus diffuse allocation); and fractal dimension indicates self-similar exploration patterns and hierarchical attention structure, reflecting cognitive processing propensities and learned strategies [17].

2.2.4 Task-Specific Gaze Behaviors

Task-specific gaze behaviors examine individual patterns of gaze motion within specialized visual tasks, yielding contextually interpretable biometric features rooted in expertise-oriented cognitive and perceptual structures optimized for those tasks. While general gaze patterns provide interpretable biometric content, the greatest discriminability typically arises when work-oriented tasks are designed to target particular cognitive processes or perceptual abilities [50].

Reading is one of the most thoroughly studied task-specific gaze paradigms for authentication [6, 28, 51]. It elicits highly structured eye-movement patterns with pronounced individual differences that reflect cognitive processing, linguistic competence, and practiced reading routines. Key biometric indicators include reading speed (visual processing and comprehension capacity), regression patterns (error-correction strategies), line-to-line transitions (spatial search and attention management), and word skipping (reading skill and lexical familiarity). Together, these behaviors expose individual strategies for information extraction and comprehension [51].

Research on visual search behavior examines individual differences in target-object identification within complex environments. It reveals characteristic patterns in attention allocation, spatial search strategies, and decision processes that reflect cognitive abilities and learned routines. Key factors include search efficiency (objective evaluation of information detection and exploration inhibition), the systematic–random search spectrum (stringently systematic versus adaptive, opportunistic methods), and the use of peripheral vision (attentional abilities and visual-field strategy). Collectively, these traits provide informative biometric indicators of cognitive abilities and search strategies [52].

Menu navigation structures in graphical user interfaces reflect individual interaction styles and reliance on spatial memory. This perspective is valuable for describing how users traverse large information hierarchies and make decisions from well-structured visual displays. Analyzing gaze during menu selection—covering exploratory behavior, decision strategies, and efficiency measures—yields contextually grounded biometric markers for interface authentication that accommodate individual differences in spatial comprehension, memory use, and interaction modes. Navigation methods further differentiate systematic versus opportunistic information gathering: some users employ structured, hierarchical exploration, whereas others exhibit goal-directed, direct navigation. Decision behavior exposes individual differences in the cognitive processes underlying evaluation and choice, including time spent considering alternatives, the criteria applied during evaluation, and confidence levels expressed during selection [53].

Free viewing of visual stimuli reveals inter-individual differences in aesthetic preferences, attention-allocation strategies, and visual processing styles shaped by personal interests, social context, and learned viewing habits. Gaze behavior during image viewing can therefore identify distinctive features linked to individual visual preferences and cognitive styles. Salient indicators include preferred visual attributes, attention distributions concentrated on specific scene components, and exploratory tendencies that mirror one's processing routines and aesthetic evaluation strategies. Examples include a preference for faces over objects or settings, a tendency toward fine-grained inspection rather than global scene comprehension, and characteristic temporal attention-allocation dynamics during unconstrained viewing, all of which reflect differences in visual interest, aesthetic sensitivity, and cognitive processing strategies [54]. Table 1 provides a comprehensive comparison of these methodological approaches.

Table 1. Comparative Analysis of Gaze-Based Authentication Methodologies

Methodology	Advantages	Disadvantages	Performance Characteristics	Use Cases
Physiological Gaze Patterns	High stability, Difficult to forge, Consistent across sessions	Limited by hardware precision, Requires calibration, Sensitive to eye conditions	Generally stable performance, Hardware-dependent accuracy	High-security applications, Laboratory settings
Behavioral Gaze Dynamics	Natural interaction, Continuous authentication, Context-aware	Variable performance, Learning required, Environmental sensitivity	Calibration-tolerant, Adaptive over time	Mobile devices, Interactive systems
Hybrid Approaches	Balanced performance, Adaptive capability, Robust to variations	Increased complexity, Greater computational demands, Integration challenges	Combined benefits of multiple approaches	Commercial systems, Multi-platform deployment

2.3 Hybrid Approaches

Hybrid approaches combine physiological and behavioral gaze features to outperform mono-modal systems. Physiological cues contribute stability, whereas behavioral cues provide environmental adaptability; together, their complementary strengths offset individual limitations [55]. The hybrid approaches require an understanding of feature synergies: physiological ones provide temporal stability, though susceptible to hardware variation, while behavioral ones provide flexibility, though prone to variation over time. The hybrid approaches stabilize such properties using fusion mechanisms and adaptive approaches, yielding enhanced security, usability, as well as flexibility in deployment [56].

2.3.1 Physiological-Behavioral Feature Fusion

Fusion of physiological and behavioral characteristics entails higher-level fusion methods juggling computational constraints and feature redundancies. Physiological characteristics operate in millisecond time scales, which require high-grade measurements, while behavioral characteristics allow longer time intervals in which measurement error is permitted. The difficulty is in integrating heterogeneous sources without losing unique feature properties of sources [57].

Efficient fusion requires feature normalization for measurement scale compatibility, dimensionality reduction for high-dimensional spaces, and temporal alignment for different acquisition scales. Fusion models must address feature redundancy and correlation while extracting complementary information to maintain discriminative capability [58]. Early fusion combines features at the feature level into unified vectors [59]. Late fusion maintains separate processing streams, combining outputs at the decision level through voting or meta-learning [60]. Hybrid fusion combines both approaches with intermediate junctions [61]. Adaptive fusion dynamically adjusts feature importance based on context, users, or environment [62].

2.3.2 Multi-modal gaze-based authentication

Multi-modal strategies extend beyond gaze-only features by incorporating additional biometric modalities for improved security and robustness. Combining gaze with other modalities enhances performance, strengthens spoofing resistance, and enables flexible deployment across various hardware configurations and user populations [63].

Multi-modal gaze authentication creates complex biometric profiles more difficult to imitate than single-modality systems while incorporating redundancy for steady performance when one modality is unavailable or under attack. Appropriate modality selection relies on hardware compatibility, computational requirements, user acceptance, and application-specific security requirements. Optimal multi-modal systems require thorough investigation of biometric characteristic interactions and sophisticated fusion methodologies [64]. Gaze-face fusion leverages simultaneous extraction of facial and gaze data through eye-tracking technology, strengthening security while utilizing available hardware without requiring additional sensors. This combination provides complementary biometric information, merging physiological facial structure aspects with behavioral gaze movement aspects.

An integrated single-camera setup can capture gaze and facial characteristics simultaneously, ensuring precise temporal alignment and reducing typical multimodal synchronization challenges. This configuration substantially improves robustness against spoofing, since concurrently reproducing facial characteristics and natural gaze behavior is difficult—especially under adverse conditions involving illumination changes, partial occlusions, or hardware variability [38, 65]. Gaze–voice fusion combines gaze-based verification with speaker recognition, providing a multimodal solution well suited to scenarios that involve spoken interaction. The approach leverages the intrinsic coupling between speech production and visual attention, thereby strengthening authentication and enhancing user experience. Empirical evidence shows that gaze behavior systematically varies during speech, reflecting cognitive load, linguistic formulation, and idiosyncratic communication patterns. This makes the framework attractive for voice-activated agents and interactive interfaces, enabling seamless authentication during natural use without explicit biometric capture. Joint use of voice and gaze further increases robustness by impeding simultaneous spoofing of vocal characteristics and concordant gaze behavior, while supporting continuous authentication over extended interactions [41, 66].

Integrating gaze with keystroke dynamics enables construction of behavioral profiles for computer authentication by exploiting the coupling between visual attention and motor coordination during text entry. Empirical studies show that individuals exhibit characteristic gaze patterns while typing that correlate with their typing style, visuo-motor coordination, and cognitive strategies for text production. This multimodal approach supports authentication in conventional computing workflows by accommodating natural typing variability and enabling transparent verification during routine interaction, without explicit biometric capture. Joint modeling of gaze and keystrokes strengthens security by making it difficult to simultaneously spoof typing dynamics and the corresponding attention profile, while supporting continuous authentication over prolonged text-entry sessions [67].

Gaze–gesture fusion pairs eye-movement patterns with hand-gesture detection to provide a multimodal authentication mechanism well suited to touchscreen devices and gesture-driven interfaces. It exploits the natural synchrony between visual attention and manual action during interaction. Studies show that users exhibit characteristic eye–hand coordination patterns indicative of motor control, spatial cognitive skills, and interaction habits acquired through experience with diverse devices and interfaces. This modality pairing is particularly relevant for phones, tablets, and interactive displays, enabling authentication during ordinary use without explicit biometric capture. Joint modeling of gaze and gestures improves security by making it difficult to reproduce both gesture dynamics and concordant gaze patterns, while permitting seamless, in-the-flow authentication [68].

2.3.3 *Adaptive Feature Selection*

Adaptive feature selection enables dynamic adjustment of feature deployment in hybrid authentication systems to accommodate changing conditions, user characteristics, or security demands, ensuring optimal performance across diverse contexts. Physiological and behavioral characteristics have different utility depending on environmental parameters, hardware capacity, temporal variations, and security requirements. Adaptive systems continuously assess feature performance, enabling deployment adjustments to maintain authentication effectiveness through dynamic selection strategies [5, 62].

Efficient adaptive feature selection involves detailed knowledge of a range of determiners such as environmental, user, time, and security factors. Monitoring frameworks are applied in systems for feature quality assessment, aided by machine learning methods to adapt selection in terms of specified measures of performance. Decision frameworks enable authentication accuracy, computational intensity, usability, and security limitations [62, 69]. Context-aware feature selection adjusts relevance of gaze features to environmental conditions, task demands, or user states, using monitoring methods to evaluate context and then adapt feature employment. For instance, systems prefer physiological features in adverse conditions where external factors obscure behavioral ones, or switch to use behavioral ones where hardware accuracy is low. These are applied as environmental sensors, instruments of performance measure, and machine learning methods to conduct optimal adaptation protocols [70].

User-adaptive methods enable authentication platforms to distinguish peculiar characteristics of individual users so as to adapt procedures to suit differences in gaze pattern feature attributes, stability, and distinctness. This adaptation improves effectiveness by considering that users have different levels of performance among different feature categories based on physiological attributes, interaction modes, and behavior patterns. User-adaptive platforms utilize learning methods to determine optimal feature combination sets in spite of protecting against vulnerabilities exploitable from personalized action [3].

Temporal adaptation dynamically adjusts feature selection to remain aligned with enduring changes in a user's gaze behavior—arising from aging, health status, experiential learning, or environmental shifts—over long deployment horizons. These mechanisms recognize that oculomotor and behavioral attributes evolve over time and therefore monitor trajectories of change. Temporally adaptive systems incorporate monitoring technologies that discriminate legitimate long-term drift from potential security incidents, adapting procedures to preserve security while accommodating genuine behavioral change. They employ machine-learning models that represent user attributes on longer time scales to defend against attacks [15, 16]. Security-focused adaptation tunes feature selection according to threat assessments and/or security policy directives, leveraging dynamic controls that modulate authentication strength with current risk. High-security contexts emphasize features robust to spoofing, whereas routine operation prioritizes user convenience, balancing security imperatives against usability considerations.

Security-oriented adaptation comprises threat assessment procedures that identify vulnerabilities, evaluate the security posture, and make pragmatic feature-selection decisions that preserve required protection while avoiding unnecessary user burden. These mechanisms build threat intelligence, perform behavioral anomaly detection, and conduct risk evaluation to dynamically adjust authentication workflows, enabling continuous responsiveness to evolving threat landscapes without compromising user acceptance or usability [9].

Table 2. Taxonomic Framework Application (Representative Examples)

Study (Year)	Methodology	Architecture	Evaluation Focus	Dataset/Subjects	Headline Metrics
Komogortsev et al. 2010 [7]	Physiological (OPC)	Hardware (desktop IR)	EER, liveness	Lab; tens	Low EER; OPC liveness feasibility
Holland & Komogortsev 2011 [6]	Behavioral (reading scanpaths)	Hardware (desktop IR)	Verification (EER/FRR)	Lab; tens	Distinctive scanpaths; mid EER
Yoon et al. 2014 [34]	Behavioral (medical imaging viewing)	Hardware (desktop IR)	Biometric feasibility	Medical imaging; 15	Gaze patterns as biometric
Lohr et al. 2023 (GazeBaseVR) [16]	Dataset contribution (VR)	HMD (embedded)	Dataset for longitudinal studies	407 subjects; VR tasks	Large-scale VR gaze dataset
Komogortsev et al. 2012 [71]	Physiological (OPC)	Hardware (desktop IR)	Verification + PAD	Lab; tens	Stable OPC features; PAD signals
Eberz et al. 2016 [29]	Behavioral (insider threat)	Hardware (desktop IR)	Insider detection	Lab; tens	Insider exposure via gaze
Sluganovic et al. 2016 [72]	Behavioral (challenge-response)	Hardware (desktop IR)	CR liveness; EER	Lab; tens	Fast CR; improved PAD
Song et al. 2016 (EyeVeri) [73]	Behavioral (mobile)	Software (smartphone)	Usability + EER	Field/lab; dozens	Practical mobile auth
Zhang et al. 2018 (IMWUT) [33]	Behavioral (implicit stimuli)	Software (mobile/ubiquitous)	Continuous auth	In-situ; tens	Feasible continuous auth
Boutros et al. 2020 (HMD fusion) [38]	Hybrid (periocular/iris+gaze)	HMD (embedded)	Fusion gains; PAD	HMD; variable	Fusion boosts robustness
Zhu et al. 2020 (BlinKey) [74]	Behavioral (blink + gaze)	HMD/VR (embedded)	Two-Factor Authentication (2FA); usability	Lab; dozens	Low friction; higher security
Jeon et al. 2025 (Pre-AttentiveGaze) [75]	Dataset contribution	Not specified	Dataset for auth research	Large-scale dataset	Momentary visual interaction data
Lohr et al. 2025 [76]	Hybrid (gaze + periocular fusion)	Software/Hardware	Authentication fusion	Methodology validation	Gaze-periocular fusion framework

The methodological framework delineates the complementary strengths and inherent limitations of physiological, behavioral, and hybrid approaches to gaze-based authentication. Figure 1 presents a comparative visualization of the three primary methods, highlighting distinctive attributes, performance trade-offs, and suitability across implementation contexts. Table 2 illustrates the application of the taxonomic framework to representative studies in the literature.

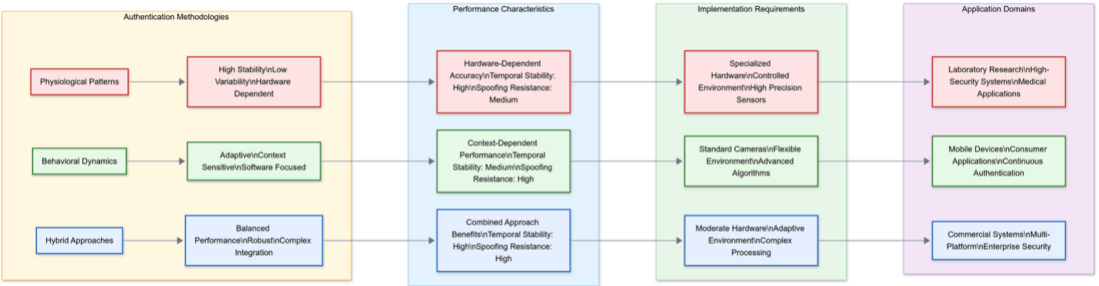
Authentication Methodologies
Physiological Patterns
High Stability\nLow Variability\nHardware Dependent
Behavioral Dynamics
Adaptive\nContext Sensitive\nSoftware Focused
Hybrid Approaches
Balanced Performance\nRobust\nComplex Integration
Performance Characteristics
Hardware-Dependent Accuracy\nTemporal Stability: High\nSpoofing Resistance: Medium
Context-Dependent Performance\nTemporal Stability: Medium\nSpoofing Resistance: High
Combined Approach Benefits\nTemporal Stability: High\nSpoofing Resistance: High
Implementation Requirements
Specialized Hardware\nControlled Environment\nHigh Precision Sensors
Standard Cameras\nFlexible Environment\nAdvanced Algorithms
Moderate Hardware\nAdaptive Environment\nComplex Processing
Application Domains
Laboratory Research\nHigh-Security Systems\nMedical Applications
Mobile Devices\nConsumer Applications\nContinuous Authentication
Commercial Systems\nMulti-Platform\nEnterprise Security

Figure 1. Comparison of Gaze-Based Authentication Methodologies

This comparative study (Table 2) explains the distinct characteristics and trade-offs associated with different gaze-based authentication approaches. Physiological approaches offer considerable temporal stability; yet, they require the utilization of special-purpose hardware. Comparably, behavioral approaches provide versatility and malleability using standard equipment, while the hybrids reach excellent performance by skillfully combining heterogeneous feature types. The choice of the individual methodology relies on the particular needs of the application at hand, available hardware resources, and security constraints.

Human eye movement exhibits substantial variability and complexity, resulting from physiological constraints in the oculomotor system, cognitive processes controlling attentional dynamics, and external variables affecting visual behavior across tasks. Biometric features in eye movement patterns result from intrinsic characteristics distinguishing users with adequate consistency for authentication across temporal contexts and environmental conditions. These features combine anatomical characteristics (extraocular muscle properties, neuronal circuit configurations, retinal structural variations) with acquired behavioral patterns (reading behaviors, visual search strategies, attention allocation processes, cognitive styles) developed over time [77]. Gaze-pattern variability yields discriminative cues for authentication across multiple dimensions: temporal (fixation durations, saccadic intervals), spatial (scanpath geometries, fixation distributions), kinetic (velocity profiles, acceleration trends), and physiological (pupil-size changes, blink rates). Understanding and characterizing these properties underpins the design of viable authentication algorithms that leverage biometric information in human gaze despite variability from fatigue, affective state, task demands, and environmental conditions [78]. Fixations are epochs of relative ocular stability during which visual information is acquired and processed. Duration depends on task needs, stimulus complexity, and processing speed differences. The spatial organization of fixations expresses tendencies in visual attention distribution, information processing tactics, and perceptual focuses. Experimental results reveal that fixation patterns have both stimulus-driven features and individual characteristics that serve as biometric signatures [32, 79].

Saccades are rapid ocular movements that shift visual attention between fixation points, characterized by short durations and high speeds. Saccadic movement parameters such as amplitude, velocity profiles, and directional tendencies are dictated by oculomotor system characteristics, which vary between individuals due to differences in muscle fiber makeup, neural control mechanisms, and biomechanical properties. Principal sequence parameters demonstrating the relationship between saccadic velocity and amplitude show variability that is reliably constant across time, making them effective biometric parameters for authentication. Additionally, saccadic latency and overshoot characteristics lend distinctiveness to gaze signatures, while accumulated microsaccades during fixation periods add discriminative information [80].

Smooth eye pursuits allow tracking of moving visual stimuli and show differences in gain and latency characteristics, reflecting brain control processes and oculomotor coordination capacities. Smooth pursuit gain, as the eye velocity to target velocity ratio, differs in individuals and reflects neural processing efficiency and motor control precision, with patterns showing under-compensation or over-compensation. Pursuit latency, the time between target movement start and smooth eye movement beginning, demonstrates persistent differences over sessions, acting as biometric markers. These parameters increase biometric data in dynamic stimulus systems, particularly when used with other gaze characteristics to enable multi-dimensional authentication processes [78].

Pupil dynamics are biometric features that mirror physiological and cognitive states through measurable changes in pupil size and response behaviors. Pupillary response parameters, including latency, amplitude, and recovery patterns, show differences that enhance authentication effectiveness when combined with other gaze-related features [67, 81]. Stability and uniqueness in gaze patterns over time are important considerations in biometric recognition system deployment, as these traits directly impact effectiveness and reliability in real-world applications. Longitudinal research suggests that despite variability in gaze patterns due to fatigue, mood state, environmental conditions, age variations, and visual acuity changes, inherent traits remain stable enough to enable reliable recognition. Stability dynamics vary at the feature level, with physiological quantities such as saccadic main sequence parameters and oculomotor plant parameters showing higher stability compared to behavioral features such as scanpath biases and attention allocation strategies. This variability necessitates careful feature selection and adaptive algorithms in long-term study designs [82].

2.4 Basic Biometric Authentication Concepts

Biometric systems rely on universality, distinctiveness, permanence, and collectability [83]. For gaze, universality generally holds for users with functional vision; distinctiveness has been shown via fixation, saccadic, scanpath, and pupillary features [24]; permanence is higher for physiological cues (e.g., main sequence, smooth pursuit) than for behavioral patterns, motivating adaptive modeling across time scales [69]; and collectability has improved with modern eye tracking but remains sensitive to environment and hardware [81].

Two stages, enrollment and verification, constitute the authentication process adopted in gaze-based systems. Enrollment involves feature extraction of characteristic patterns of enrolled users in controlled environments, where specific features are extracted for biometric templates during subsequent verification. Success depends on the quality and completeness of enrollment data, which requires careful stimulus design to elicit informative gaze responses; standardized acquisition protocols; feature-extraction pipelines that produce discriminative, efficient representations; and template-construction procedures that yield robust models [67]. Verification compares newly acquired gaze patterns against pre-enrolled templates to establish identity, using computational methods that balance accuracy, latency, and longevity. Algorithms must compensate for inherent variability in gaze due to inter-user behavioral differences, environmental perturbations, and measurement noise, so as to separate legitimate users from impostors. Similarity measures such as Euclidean distance, correlation, and dynamic time warping are commonly used for template matching, often coupled with classifiers—e.g., support vector machines, neural networks, or ensemble methods—that produce confidence scores indicative of match likelihood. Advanced systems integrate feature evaluation, template matching, and final classification with adaptive decision thresholds governed by security policy and observed user behavior [84].

2.5 Security and Threat Framework Considerations

The security domain encompasses traditional biometric vulnerabilities alongside new attack forms especially applicable to eye-tracking technologies. Understanding these vulnerabilities is essential for developing robust systems operating in risky environments [84]. Presentation attacks represent a major challenge through complex efforts to mimic natural user gaze behaviors via diverse technological means. Unlike other biometric approaches based on physical artifacts, gaze-based attacks involve sophisticated methods including video replay interventions, synthetic pattern generation through machine learning, mechanical simulation devices, or hybrid methods. Gaze pattern persistence makes detection difficult, requiring mimicry of both spatial features and temporal dynamics [9, 10]. Deep learning techniques for synthetic data generation introduce new possibilities for creating artificial gaze patterns that may deceive systems. GANs, VAEs, and other advanced approaches can produce realistic gaze sequences mimicking legitimate patterns by learning from large datasets. These AI-generated attacks pose challenges through adaptation to different users, temporal dependencies, and evolution to counter detection mechanisms. This sophistication necessitates detection mechanisms identifying subtle artifacts, statistical anomalies, and physiological implausibilities [85, 86].

Protecting gaze-based biometric templates is critical because they encode detailed behavioral information and may implicitly reveal sensitive cognitive traits or health indicators. To secure storage and transmission, systems should incorporate strong encryption, rigorous key management, and privacy-preserving mechanisms to prevent unauthorized disclosure or inference of individual data [87]. The continuous nature of gaze-based authentication introduces security concerns distinct from discrete, event-based systems, particularly around session management and temporally orchestrated attacks. In continuous monitoring, challenges include session hijacking (taking over an already authenticated session); progressive reconstruction of the authentication template via incremental changes in eye-movement patterns over time; adaptive attacks that continually modify their strategy to evade detection by blending with system responses; and the need to validate temporal consistency to ensure reliability over extended interactions. Addressing these issues requires advanced security frameworks that sustain long-duration authentication while adapting to legitimate user variability and changing environmental conditions [88]. Eye-tracking hardware also presents environmental vulnerabilities, including sensitivity to infrared interference, ambient illumination changes, and occlusions of sensors—factors that adversaries could exploit to mount denial-of-service attacks [89].

The privacy implications of gaze-based authentication extend beyond conventional biometric concerns to encompass behavioral and cognitive inferences drawn from eye-movement data, which can, in principle, reveal sensitive personal traits. Such data can reflect reading proficiency, information-processing speed, attentional deficits, neurological disorders, affective state, and even personal interests or preferences. These characteristics have significant implications for data minimization and purpose limitation, informed consent, and the risk of function creep, whereby authentication data may be repurposed for unauthorized secondary uses. Given the breadth and sensitivity of gaze data, a comprehensive evaluation of privacy-preserving strategies and compliance with regulatory requirements is essential [12, 13].

2.6 Performance Evaluation Metrics

Gaze-based authentication requires comprehensive evaluation across both security and usability dimensions. Classical biometric metrics (False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER)) provide the foundation, but the temporal dependence of gaze behavior, its behavioral variability, and sensitivity to environmental conditions necessitate additional, tailored procedures [14]. FAR quantifies incorrect impostor acceptance and thus indicates vulnerability to unauthorized access. FAR evaluation encompasses random impostor attempts, presentation attacks using artificial patterns, and zero-effort trials without privileged knowledge [90]. FRR measures incorrect denial of legitimate users, critically affecting usability. Gaze-based FRR evaluation must account for behavioral variability from fatigue, environmental changes, aging, medications, and emotional states. Temporal pattern changes require adaptive algorithms balancing legitimate user evolution with security [91].

EER identifies the operating point where FAR equals FRR, enabling system comparison. While EER provides valuable comparative metrics, it may not reflect performance in asymmetric security scenarios where false acceptance and rejection costs differ. EER interpretation requires careful consideration of testing conditions, population diversity, and environmental factors [92]. Detection Error Tradeoff (DET) curves analyze FAR-FRR trade-offs across decision thresholds, providing insights into performance across threat models, populations, and environments. DET curve shape and position indicate system robustness and discriminability, enabling algorithm and configuration comparison [93].

Usability metrics assess practical deployment aspects determining user acceptance and system viability. Authentication time represents a critical factor, requiring balance between data collection needs and user expectations. Additional considerations include calibration frequency and system complexity [94]. Calibration requirements represent critical usability considerations that can determine deployment success. Calibration frequency directly affects user acceptance and system practicality. Complex processes create adoption barriers, particularly for users with limited technical expertise. Modern systems focus on reducing calibration burden through implicit calibration and adaptive algorithms [12].

System robustness evaluation requires testing across diverse user populations and environmental conditions. Performance must be demonstrated across different visual characteristics, cultures, technical expertise levels, and external conditions including illumination changes and mobility impairments [72].

3 Frameworks and Methods for Implementation

This section explores architectural strategies across hardware, software, cloud, and embedded systems, each providing viable implementations for different domains [86, 95]. Architecture evolution reflects computing trends including sensor democratization, ML advancement, and cloud/edge emergence. Modern systems balance accuracy, efficiency, cost, convenience, privacy, and security trade-offs. Understanding architectures enables informed technology selection and deployment strategies [86, 95]. Table 3 compares architectural approaches, characteristics, and applications.

3.1 Hardware-Based Systems

Hardware-based systems utilize sophisticated eye-tracking technology with specialized infrared cameras, illumination, and signal processing for high-accuracy authentication. These systems achieve superior measurement precision and temporal resolution but require specialized sensors and calibrated optics, limiting deployment flexibility while meeting stringent security requirements [96, 97]. Performance gains involve trade-offs including greater investment requirements, implementation complexity, environmental sensitivity, and limited deployment versatility, making them suitable for environments prioritizing security and accuracy over deployment convenience [98].

Table 3. System Architecture Comparison for Gaze-Based Authentication

Architecture Type	Hardware Requirements	Performance Characteristics	Deployment Complexity	Typical Applications
Hardware-Based	Dedicated eye trackers, IR cameras, Specialized sensors	High precision, Controlled conditions	High	Research labs, High-security facilities
Software-Based	Standard cameras, Computational resources	Variable precision, Algorithm-dependent	Medium	Desktop applications, Kiosks
Cloud-Based	Basic sensors, Network connectivity	Scalable processing, Network-dependent	Low	Web services, Mobile apps
Embedded	Integrated sensors, Limited processing	Resource-constrained, Optimized algorithms	Medium	Smartphones, Wearables, IoT devices

3.1.1 Desktop Eye-Tracking Systems

Desktop eye-trackers provide high precision and consistency in controlled environments through advanced optics, calibration, and signal processing. Systems range from remote tracking allowing head movement to head-stabilized configurations maximizing accuracy [96, 97]. Infrared eye trackers use near-infrared cameras to capture high-definition ocular images while suppressing ambient light effects. Strategic infrared illumination creates corneal reflection patterns enabling accurate gaze estimation through sub-pixel pupil and reflection localization, providing ambient light tolerance, user comfort, and robust feature detection [96]. Modern desktop eye-tracking achieves high spatial accuracy and temporal resolution, enabling sophisticated authentication algorithms with automatic calibration and cross-user tracking accuracy. Desktop configurations require controlled environmental conditions including stable lighting and minimal infrared interference. While less mobile than portable alternatives, they provide superior authentication accuracy, making them suitable for high-security applications and research environments prioritizing precision over convenience [99].

3.1.2 Mobile and Wearable Eye-Tracking Devices

Portable eye-trackers combine wearable technologies for mobile gaze authentication across diverse settings, requiring energy efficiency, miniaturization, and environmental ruggedness while balancing authentication effectiveness with usability factors like battery life and ease of use. Advances in miniaturization and energy-efficient components enable natural operational environment deployment [100]. Head-mounted trackers maintain rigid eye-sensor geometry, achieving desktop-like accuracy with mobility through compact infrared cameras and efficient lighting with stringent calibration to maintain precision despite mechanical constraints [101]. Integration into smart glasses and XR headsets enables Virtual Reality (VR) environment authentication and supports foveated rendering [18, 102]. Portable eye-tracking units face technical challenges including power optimization, thermal control, and mechanical robustness requiring innovative engineering solutions. Power control techniques with variable sampling rates and sleep modes enable operation for extended periods while maintaining authentication effectiveness. Mechanical robustness requires designs maintaining calibration despite motion, vibrations, and mechanical strains in portable contexts [103].

3.1.3 Webcam-Based Gaze Estimation

Webcam-based systems utilize commercial cameras with specialized software algorithms for gaze direction determination, providing reduced hardware investment and broader deployment opportunities with accuracy trade-offs compared to specialized eye-tracking devices. These systems represent an effective compromise between high-accuracy specialized systems and deployable authentication techniques, leveraging ubiquitous consumer cameras to provide authentication capabilities with minimal hardware investment while using complex algorithms to extract biometric information from lower-precision sensors [104]. Consumer webcam adaptation extracts gaze signals from standard Red-Green-Blue (RGB) cameras using Computer Vision/Machine Learning (CV/ML) techniques that compensate for limited resolution, optics, and illumination. Reported accuracy (often a few degrees) is sufficient for many authentication scenarios without specialized hardware, with performance shaped by camera quality, lighting, and algorithm choice. Approaches include appearance-based mappings, geometric landmark/head-pose estimation, and hybrids that improve robustness [105]. Advanced deployments showcase effective performance using off-the-shelf cameras and browser-based environments, with machine learning approaches improving system robustness across different hardware setups. Smartphone front cameras enable mobile gaze estimation, although precision is bounded by optical and processing constraints. Head-pose estimation and gaze calculation can be enhanced with RGB-D sensors by utilizing geometric depth information [106, 107, 108].

3.2 Software-Based Systems

Software-centric gaze authentication relies on algorithmic methods rather than special-purpose hardware, using machine learning, computer vision, and signal processing techniques to glean gaze information from commercial cameras. Software-centric methods enable greater deployment variety and keep authentication accuracy in acceptable ranges through higher-level algorithmic processing of sensor output [18, 102, 109]. Software-centric methods offset hardware limitations by leveraging higher-level feature extraction, pattern recognition, and adaptive learning. This approach reduces hardware cost, increases deployment flexibility, improves environmental robustness, and enables continual performance improvements via software updates. These methods leverage advances in machine learning to deliver user-adaptive algorithms that maintain robust authentication across diverse deployments [102].

3.2.1 Algorithmic and Real-Time Approaches

Algorithm-based systems develop detailed mechanisms for feature extraction and classification to deliver reliable authentication despite hardware constraints. The shift from hardware-centric to software-driven methods enables broader deployment scenarios through machine-learning techniques that adapt to specific users and environments. Advanced computational approaches mitigate hardware limitations while preserving security across heterogeneous platforms [110]. Deep learning uses convolutional neural networks to learn mappings from ocular imagery to gaze vectors in end-to-end models. These techniques automatically discover optimal feature representations, eliminating manual feature engineering while achieving comparable accuracy with reduced calibration needs. Advantages include automatic adaptation across cameras and resolutions, robustness to illumination changes, and gains from larger training datasets. Neural network architectures yield strong, generalizable mappings across users, hardware, and environments [102, 109, 111].

State-of-the-art algorithmic approaches underpin high-performance authentication by leveraging next-generation computing paradigms. GazeNet combines multi-scale convolutional features with attention mechanisms for robust performance across users and conditions without explicit calibration. Ensemble learning methods combine complementary gaze estimation algorithms for improved performance. Transfer learning deploys pre-trained models from large datasets, reducing training requirements while enabling rapid adaptation across users and environments. These approaches benefit scenarios with limited training data or computational resources [112, 113, 114]. Real-time and edge processing architectures emphasize computational efficiency for interactive authentication through optimization techniques balancing performance and resource limitations. System efficiency requires careful algorithmic tuning and resource allocation using parallel processing and efficient data structures to ensure timely responses while maintaining accuracy and security. Real-time computation is critical for applications requiring instantaneous feedback, continuous verification, or interactive system integration, as authentication delays negatively impact user experience [95, 115, 116, 117]. For architectural details of edge computing—including processing split, local feature extraction, and distributed protocols—see Section 3.4.3 (Edge Computing Architectures); here we focus on algorithmic and real-time software considerations.

3.3 Cloud-Based Systems

Cloud-based gaze authentication systems utilize distributed computation and network connectivity for scalable authentication supporting numerous users and sophisticated processing. This service-oriented architecture provides on-demand authentication across platforms and geographies while decoupling data acquisition from processing and storage. Cloud advantages include computational scalability, centralized algorithm management, uniform authentication policies, and access to computationally intensive machine learning algorithms requiring large training datasets [95, 118].

The key advantage of cloud systems is their ability to provide robust authentication features for resource-constrained devices, while at the same time maintaining centralized control over security mechanisms, algorithm updates, and end users. This arrangement allows for efficient deployment of advanced authentication techniques within a range of end-use applications, such as mobile devices, embedded systems, and web applications, that generally do not have the capability to adopt complete local authentication processes because of their limited computational capabilities. Additionally, cloud structures are best suited to realize economies of scale offered by large computational resources, enabling the realization of economically viable authentication mechanisms. At the same time, they drive ongoing innovation through centralized algorithm releasing, large-scale data analytics, and deployment of advanced machine learning methodologies taking advantage of heterogeneous end-user populations and usage patterns. Nevertheless, cloud systems face significant challenges with respect to network latency, protecting privacy, maintaining data security, and the need to maintain authentication processes during network outages or connectivity issues [118, 119].

3.3.1 Remote Authentication Services

Remote authentication services provide centralized methods for gaze recognition-based authentication that can be accessed through various client systems that are networked together. This capability makes it possible to build scalable authentication designs that can support very large user populations while maintaining consistent security policies and authentication techniques across various platforms and deployment environments. These designs facilitate the application of combined authentication policies across multiple platforms based on the use of strong server-side processing capabilities and the creation of sophisticated distributed computing environments that can efficiently manage authentication requests from large numbers of concurrent users with minimal latency and maximum availability using sophisticated methods for load balancing, caching, and resource allocation. Paradigms for remote services provide significant advantages, such as centralized control of algorithms, a unified user experience across platforms, reduced processing loads on client-side systems, and the ability to implement large machine learning systems that require significant processing capability and large training datasets [120].

Scalable cloud architectures utilize distributed computing resources to process authentication requests from large populations of concurrent users, utilizing infrastructure management techniques like load balancing, auto-scaling, and distributed storage to maintain performance and availability despite variable demand conditions, while at the same time improving cost effectiveness and utilization of computation resources. Scalable cloud architectures are typically based on microservices architectures, which allow different components of the authentication system to scale independently based on patterns of demand, thus improving resource utilization and system robustness through fault isolation and redundancy mechanisms. Modern cloud platforms provide us with tools for measuring system performance, managing resource allocation, and maintaining high availability through geographic diversity and fault-tolerant automatic failover mechanisms that maintain authentication service continuity even in the face of underlying infrastructure faults or maintenance interruptions [121]. Cloud-based vision and ML services can support scalable deployment; however, vendor-specific details are omitted to ensure neutrality and longevity. Focus should remain on architectural considerations (latency, privacy, model update cadence, and availability) that are provider-agnostic.

3.3.2 Privacy-Preserving Cloud Authentication

Privacy-preserving cloud authentication is a sophisticated architecture that utilizes advanced cryptography to strengthen cloud computing's authentication mechanisms, safeguarding individuals' privacy and their biometric information. Privacy-preserving cloud authentication is a suggested architecture aimed at addressing expanding fears over cloud-based environments' security and confidentiality of biometric information through new technical mechanisms exploiting cloud computing benefits as well as ensuring effective privacy guards. These frameworks address security and confidentiality risks for biometric data in cloud environments by employing advanced cryptographic mechanisms, secure computing frameworks, and privacy-preserving machine-learning methods, enabling sophisticated authentication while protecting sensitive data from unauthorized use, inference, or misuse. The architecture recognizes biometric data as highly sensitive and therefore mandates rigorous protections, especially in cloud infrastructures where third-party providers process or store such information [122].

Homomorphic encryption enables computation on encrypted gaze data without decryption, allowing cloud-based authentication while preserving data confidentiality. Recent advances have made such schemes increasingly practical for biometric workloads, and implementations now support detailed authentication pipelines over ciphertext with acceptable efficiency and strong security guarantees. Secure multi-party computation allows multiple parties to jointly perform authentication computations without revealing their private inputs, enabling federated authentication frameworks to access decentralized data while preserving privacy; advanced cryptographic protocols ensure no participant gains the full dataset [123, 124].

Sophisticated privacy-preserving methods maintain user confidentiality while enabling advanced authentication capabilities in cloud environments. Differential privacy injects carefully calibrated noise into observed quantities and authentication outputs to impede identification of individuals, offering formal, tunable privacy guarantees that preserve utility. Federated learning enables heterogeneous devices or organizations to collaboratively train authentication models without transferring raw biometric data. This improves accuracy while preserving data locality by using distributed machine-learning techniques that aggregate knowledge across heterogeneous sources without centralizing datasets. Collectively, these advances significantly strengthen cloud authentication by leveraging large-scale computation and machine learning while addressing the sensitive privacy challenges inherent to storing biometric data in cloud infrastructure [118, 119].

3.4 Embedded Systems

Embedded gaze authentication integrates biometric capabilities directly into consumer electronics and Internet of Things (IoT) devices, emphasizing resource efficiency and responsive user interfaces while operating within the constraints of embedded computing environments. These authentication approaches are challenged by the need to find a subtle balance among authentication effectiveness and the limitations placed by energy consumption, computing capability, and spatial constraints. This requires innovative approaches to engineering that are capable of delivering an acceptable degree of authentication while meeting the demanding requirements commonly found with embedded applications such as instantaneous responsiveness, energy efficiency, thermal control, and cost effectiveness. The embedded computing paradigm provides critical applicability with respect to gaze-based authentication, given that it allows biometric security capabilities to be included with the broad range of networked and increasingly complex devices that typify modern society [95].

The main issue related to embedded gaze authentication is the development of systems that provide significant security benefits without compromising resource constraints. This requires implementing advanced optimization techniques aimed at eliminating computational loads, decreasing energy utilization, and increasing memory efficiency, with satisfactory security and authentication process accuracy levels achieved simultaneously. Generally, embedded systems are required to function independently with extended lifespans without access to exterior services or support; hence, they need authentication schemes that are not merely robust and reliable but are also capable of maintaining steady functionality across diverse environmental settings, different end-users, and different application arenas. Additionally, such schemes should have the resilience required to support changing situations and growing security needs. The effectiveness of embedded gaze authentication depends upon developing efficient algorithms, optimizing hardware settings, and developing smart systems for authentication capabilities that are technically competent and commercially viable under the limitations of the embedded application framework [78].

3.4.1 Mobile Device Integration

The authentication of portable devices is an emergent research area that integrates gaze authentication across mobile phones, tablet computers, and wearable technology to enable ubiquitous authentication systems that provide secure interactions over a vast range of personal computing devices in use by individuals in their daily lives. Such applications are critical in managing challenges related to diverse hardware compatibility, diverse application contexts, and user mobility, necessitating the creation of flexible algorithmic approaches and system architectures that can maintain authentication effectiveness across varying device classes, screen sizes, sensor configurations, and application contexts, as well as ease the changing conditions inherent to portable computing environments. The mobile integration framework recognizes that users interact with a variety of devices during their day-to-day activities, thus requiring authentication approaches that can offer consistent security experiences while respecting the inherent capabilities and limitations of each individual device [22, 125].

The inclusion of eye tracking in smartphones utilizes front cameras in conjunction with computational algorithms to enable gaze-based authentication without the necessity of special hardware. This technology leverages the advanced camera technology and powerful processors built into modern smartphones, thus providing authentication capabilities previously unique to specialized eye-tracking hardware. The TrueDepth camera system built into the Apple iPhone, and similar technologies, allows for basic attention detection and gaze direction evaluation in consumer devices by applying depth sensing, infrared illumination, and machine learning algorithms that can deliver a sufficient level of accuracy for the purpose of authentication, while maintaining the visual quality and user experience expectations of consumer products. This is in contrast to gaze authentication on Android devices, which utilizes the rich hardware ecosystem typical of Android devices to enable flexible authentication solutions. These systems utilize the Android Camera2 Application Programming Interface (API) and machine learning libraries to enable developers to create gaze authentication applications that can support diverse hardware configurations, display screen resolutions, and processing power in the wide range of Android devices offered in the market [126].

Sophisticated mobile deployments demonstrate the viability of augmenting authentication functionality within the limits of consumer-grade devices. Here, authentication technologies based on tablet platforms take advantage of the increased screen size and improved processing capacity to enable advanced gaze authentication functionality, accommodating dynamic, adaptive visual patterns and extended session lengths while maintaining user comfort using better user interface and interaction design. Additionally, the presence of wearable technologies extends the application base of gaze authentication to smartwatches, fitness bands, and other wearables, requiring systems to withstand limitations associated with power availability and processing resources, while all along maintaining strong security through highly optimized computational approaches, judicious hardware utilization, and intelligent power management mechanisms that provide for extended periods of authentication activity. These developments in mobile and wearable technologies represent the cutting edge of embedded gaze authentication, defining the viability of integrating sophisticated biometric security features into portable devices that have become ubiquitous in modern society [66, 78].

3.4.2 IoT and Smart Environment Applications

Internet of Things applications extend gaze-based authentication to environmental control systems, smart home devices, and ambient computing platforms, creating pervasive authentication capabilities that can provide seamless security across the interconnected ecosystem of smart devices that increasingly populate modern living and working environments. These systems often operate in challenging environmental conditions and must demonstrate robust performance across diverse user populations, requiring authentication algorithms that can maintain reliable operation despite variations in lighting conditions, environmental noise, user positioning, and the diverse range of users who may interact with IoT devices including individuals with varying levels of technology familiarity, different physical capabilities, and diverse cultural backgrounds. The IoT paradigm imposes distinct requirements on gaze-based authentication: autonomous operation, low-maintenance lifecycles, and seamless integration with existing smart-environment infrastructure, all while delivering meaningful security benefits [127]. In smart homes, gaze-based authentication can govern lighting, climate, entertainment, and security subsystems, enabling user identification and personalized experiences while restricting unauthorized access. These deployments favor hands-free interaction that accommodates diverse levels of technical expertise through natural modalities. In automotive settings, gaze biometrics support vehicle access control, driver identification, and personalization of settings, and must function under harsh conditions—varying illumination, vibration, and temperature extremes—while providing rapid authentication without compromising safety [128, 129].

Specific IoT deployments showcase the versatility of gaze-based authentication across domains. In industrial IoT, gaze authentication supports equipment access control and safety interlocks, meeting stringent reliability requirements while operating amid extreme temperatures, vibration, dust, and electromagnetic interference. In healthcare settings, gaze biometrics enable secure device control and patient identification, requiring high reliability and adherence to regulatory frameworks to ensure protected access to critical systems. These examples illustrate the modality's applicability across sectors [130, 131].

3.4.3 Edge Computing Architectures

Edge computing paradigms distribute computational operations over local devices and network infrastructure, boosting equilibrium of computational requirements, latency, and privacy of data. This paradigm supports hybrid approaches that utilize local processing and cloud abilities simultaneously without experiencing separate handicaps, yet maintains local ownership of data. Edge computing architecture supports gaze-based authentication by embedding complex authentication protocols in resource-limited environments, providing for efficacy, privacy, and commercial viability [132]. Local feature extraction performs initial gaze analysis locally, which reduces bandwidth usage and enforces privacy protections by means of higher-level algorithms that extricate compact, privacy-respecting feature sets at the expense of retaining discriminative information pertinent to effective authentication. Hierarchical processing models utilize different levels of computing resources, from local microcontroller units to cloud infrastructure, and as such, enable flexible computing architecture that dynamically relocates processing resources in concert with available capacities and security requirements, providing a balancing act between efficacy, privacy, and cost considerations [133].

Advanced edge computing implementations perform distributed authentication that adapts in real time to heterogeneous resource conditions and application-specific requirements using sophisticated monitoring and optimization mechanisms. These approaches sustain authentication efficiency while optimizing resource utilization across distributed systems. Distributed authentication patterns enable collaboration among edge devices during critical phases, ensuring end-to-end data integrity. Consensus mechanisms further improve authentication outcomes through collaborative computation while preserving privacy and reducing per-device computational load. Collectively, these capabilities demonstrate edge computing's ability to deliver robust authentication across diverse deployment environments and resource constraints [134, 135].

4 Security Evaluation and Performance Analysis

This section discusses the evaluation methods classified under the third dimension in our framework, comprising measures of accuracy, techniques for countering spoofing attempts, and usability measures that are essential in the evaluation of systems. Evaluating gaze-based authentication requires methodological frameworks assessing effectiveness across deployment environments, threat models, and user specifications.

Current biometric testing standards need adaptation for gaze-specific aspects including temporal behavior, cognitive and environmental influences, and specific vulnerabilities. Evaluation frameworks must address performance domain interactions, recognizing that improvements in one aspect may negatively impact others, necessitating careful trade-off analysis. Developing standardized testing protocols and metrics remains a key research direction for meaningful method comparisons [136].

Standards alignment: We follow the principles in ISO/IEC 19795-1 for biometric performance testing and reporting and adopt ISO/IEC 30107:2023 presentation attack terminology (bona fide presentation vs presentation attack; attack instruments such as replay, synthetic/generative, and mechanical) as well as recent minimal reporting guidance for eye-tracking research [14, 137, 138]. Where relevant, we specify protocol attributes (dataset, subjects/sessions, impostor type, PAD on/off) to ensure comparability and traceability across studies. Table 4 systematically organizes the key evaluation metrics across three critical dimensions: accuracy performance, spoofing resistance capabilities, and usability assessment factors, providing a structured framework for comprehensive system evaluation.

Table 4. Performance Metrics and Evaluation Framework for Gaze-Based Authentication

Metric Category	Specific Metrics	Literature Range	Evaluation Method	Security Implications
Accuracy Metrics	Equal Error Rate (EER), False Acceptance Rate (FAR), False Rejection Rate (FRR)	Varies by study, System-dependent, Context-dependent	Cross-validation, Hold-out testing, Impostor testing	Primary performance indicator, Security risk assessment, Usability impact
Spoofing Resistance	Presentation Attack Detection (PAD), Liveness Detection Rate, Robustness Score	Performance varies significantly by attack type, Depends on detection method and sophistication	Synthetic attack testing, Video replay attacks, Environmental variations	Anti-spoofing capability depends on stimulus design, Sensitive to prompt unpredictability
Usability Assessment	Enrollment Time, Authentication Speed, User Acceptance Rate	Varies by stimulus complexity, Limited empirical data	User studies, Response time measurement, Subjective evaluation	Adoption barrier, User experience, Practical deployment

4.1 Accuracy and Performance Measurement Metrics

Accuracy metrics underpin discrimination performance assessment but should be interpreted with gaze-specific caveats (temporal dynamics, environmental sensitivity, and calibration effects). When reporting EER/FAR/FRR or DET/ROC curves, specify dataset (subjects/sessions), hardware class, session protocol, and whether results reflect zero-effort impostors, informed impostors, or presentation attacks. Attribute numeric ranges to specific studies; avoid global ranges without protocol context. Comprehensive evaluation requires systematic documentation of key parameters to ensure reproducibility and meaningful comparison across studies. Essential documentation includes methodology and dataset characteristics such as dataset designation, number of participants, session frequency, and enrollment versus testing division protocols. Impostor model specification must clearly indicate whether results reflect zero-effort, informed/targeted, or presentation attack scenarios, including the type of attack instrument employed. Presentation attack detection and liveness detection status should be documented, specifying whether systems are active or inactive and providing details of challenge-response mechanisms where applicable. Performance reporting should include comprehensive metrics and curves such as EER, FAR/FRR at stated thresholds, DET/ROC curves with operating points, and identification metrics including rank-1 accuracy and CMC curves where relevant. Hardware class specifications must detail whether systems employ research-grade infrared equipment, commodity RGB cameras, head-mounted displays, or mobile/embedded devices, along with sampling rates and illumination characteristics. Calibration procedures require documentation of periodicity and methodology, including automated calibration and drift management approaches. Environmental and user conditions significantly impact performance and should include illumination spectrum, geographical environment, user exhaustion levels, and task environment characteristics.

4.1.1 False Acceptance and Rejection Rates

The False Acceptance Rate (FAR) refers to the probability that an authentication system will falsely accept an impostor as an authorized user, thus representing a key security metric to evaluate the effectiveness of gaze-based authentication systems against unauthorized access attempts. In order to determine the FAR of gaze-based systems, it is necessary to investigate different attack approaches and types of impostors with the goal of providing a thorough security evaluation while recognizing that individual impostor classifications represent different threats that require different countermeasures. The estimation of the FAR in gaze-based systems is highly challenging due to the complexity of the analysis of gaze patterns, the possibility of similarities within different users, and the impact of environmental circumstances and physical conditions on the detection of unique gaze-related features [139]. Zero-effort impostor attacks represent the baseline threat model where impostors attempt authentication without specific knowledge of legitimate user gaze patterns, essentially relying on chance or natural similarities in gaze behavior to achieve unauthorized access. Studies have reported low FAR under zero-effort conditions in controlled settings [140, 141], indicating the inherent discriminative power of gaze patterns for user identification. Random impostor evaluation examines performance when impostors are randomly selected from the user population, providing insights into the natural discrimination capability of gaze features across diverse user populations and revealing how systems perform across the spectrum of human gaze variation.

Informed impostor attacks are categorized by attackers' possessing a degree of awareness concerning legitimate users' gaze patterns, thus being higher-end threat models employing known gaze behaviors, statistical behavioral patterns, or social engineering methods to raise the likelihood of attack successes. Informed impostor attacks present a heightened challenge for gaze-based authentication because adversaries can mimic observed gaze behaviors or exploit system-specific weaknesses to increase their success rate. Analyzing systems under informed-adversary models reveals vulnerability surfaces and underscores the need for additional defenses—liveness detection, challenge-response protocols, or multimodal authentication—to harden resistance against skilled attackers familiar with legitimate users' behavioral patterns [142]. The False Rejection Rate (FRR) is the probability that a system denies access to a legitimate user and is a key usability metric that directly impacts user satisfaction and real-world adoption. Evaluating FRR in terms of gaze-based mechanisms requires accounting for inherent users' gaze behavior variability, which may result from fatigue, environmental factors, and temporal variations in behavior. Additionally, it is fundamental to consider that gaze behavior is subject to a variety of systematic and stochastic variations affecting authentication effectiveness, even in legitimate users. Precise FRR estimation of gaze-based authentication mechanisms requires a thorough insight into variability sources of intra-user behavior, as well as developing effective mechanisms able to compensate for intrinsic variations in gaze behavior while ensuring safety against unauthorized attack attempts [78].

Intra-session variability analysis examines FRR within a single authentication session, quantifying short-term effects such as attention shifts, eye fatigue, and environmental distractions that can cause deviations from the enrolled gaze profile. Well-calibrated systems can achieve low FRR within a session, though performance may degrade over longer sessions due to fatigue, attention drift, or changing environmental conditions. Inter-session stability evaluation measures FRR across sessions separated by hours, days, or weeks, assessing temporal stability of gaze patterns and the system's ability to adapt to natural behavioral changes over time (e.g., learning effects, variations in visual acuity, or cognitive state) [143, 144]. Cross-environment robustness testing evaluates FRR when authentication occurs under different environmental conditions (lighting, noise, location), providing insight into consistency under real-world deployment scenarios. Effective gaze authentication should maintain acceptable FRR across such conditions by compensating for factors like ambient-light variation that may degrade eye-tracking quality, changes in user position that affect gaze-estimation accuracy, and environmental distractions that alter gaze behavior [145].

4.1.2 Equal Error Rate and Operating Point Analysis

The Equal Error Rate (EER) summarizes the trade-off between false rejection and false acceptance by identifying the operating point where FRR equals FAR. It provides a convenient basis for comparing methods and systems; however, comprehensive evaluation requires analyzing performance across the full operating range because applications differ in their preferred usability–security balance. EER is popular for its clarity and ease of interpretation, but it may not capture nuanced behavior under specific deployment conditions [146]. State-of-the-art gaze-authentication systems exhibit varied performance depending on implementation details, feature-extraction pipelines, and experimental protocols. Reported results vary widely across studies due to differences in approaches, hardware configurations, and evaluation setups. Desktop platforms—often operating under controlled conditions with higher-quality sensors—tend to outperform mobile and webcam-based deployments, where hardware and environmental constraints introduce additional error. These observations illustrate the trade-offs between accuracy and deployment convenience; outcomes also depend strongly on testing protocols, dataset quality, selected gaze features, and classifier design [147].

Higher-order performance analyses provide a richer, dynamic characterization of system behavior beyond a single summary metric. Detection Error Tradeoff (DET) curves visualize performance across operating points, revealing how FRR and FAR interact and exposing curve topology, regions of inflection or plateau, and behavior under extreme conditions. Receiver Operating Characteristic (ROC) curves offer a complementary view focused on the trade-off between true positives and false positives, particularly useful when security requirements are asymmetric. Cost-sensitive analysis incorporates application-specific costs of false acceptance and false rejection to select operating points tailored to deployment needs; however, the optimal balance between usability and security depends on factors such as required security level, user tolerance for failure, and the consequences of unauthorized access [148, 149, 150].

4.1.3 Identification Accuracy and Scalability

Accuracy measures quantify the effectiveness of gaze-based recognition in large-population settings. Beyond binary verification, identification is a multi-class task that demands separation among hundreds of enrolled identities rather than a single claimed identity. These metrics are especially relevant when identification—not just verification—is required, such as in adaptive user interfaces, large-scale access control, or free-viewing surveillance scenarios. Rank-1 identification accuracy measures the probability that the true identity appears at the top rank, reflecting how discriminable gaze cues are across users. Observed Rank-1 varies with population size, task design, and sensor quality; performance typically declines as the gallery grows due to increased similarity in gaze behavior. Cumulative Match Characteristic (CMC) curves visualize identification effectiveness as a function of rank, enabling leverage of additional candidates and providing insights into error distribution [151, 152].

Scalability analysis examines how identification accuracy degrades as the enrolled population grows. This perspective clarifies operational limits of gaze-based identification and helps determine population sizes appropriate for different application scenarios. A detailed understanding of scalabilityincluding its constraintsis essential for large deployments and informs architectural choices across feature extraction, classifier design, and system configuration to maintain efficiency as user counts increase. The distinction between closed-set and open-set evaluations is critical: in closed-set tests all subjects are enrolled, whereas open-set tests include unknown individuals who are neither enrolled nor recognized; the latter more closely reflects real deployments with attempted access by unenrolled users. Open-set protocols necessitate auxiliary mechanisms for detecting and rejecting unknowns, increasing system burden but enabling more realistic assessment of performance [153, 154]. Given these multifaceted evaluation challenges, a comprehensive framework is needed to capture interdependencies among accuracy metrics, security considerations, and usability factors (see Figure 2). The framework highlights inherent trade-offs and how these dimensions jointly determine overall system performance, guiding the selection of operating points for specific application requirements.

4.2 Spoofing Resistance and Anti-Spoofing Techniques

The ability to counter spoofing is a critical security requirement of gaze-based authentication approaches, with attackers trying to escape authentication mechanisms through the utilization of presentation attack tactics and the creation of artificial data that exploit the inherent flaws related to measuring and inspecting gaze activity. The assessment of spoof resistance requires consideration of different attack modalities alongside the effectiveness of countermeasures, while understanding that the attack profile of gaze-based authentication remains constantly fluid, with attackers developing next-generation tactics designed to create extremely realistic artificial gaze patterns or control the authentication processes. Spoof resistance should be based on current attack approaches, along with potential future attack vectors, so that even next-generation machine learning approaches are capable of creating highly realistic artificial gaze data that is difficult to distinguish from real patterns [155]. The challenge of developing resistance to spoofing by gaze-based authentication is exacerbated by the embryonic status of the technology, compounded by limited understanding of the diverse attack vectors that would be available to attackers. Older, more mature biometric modalities, like face and fingerprint recognition, have long been the subject of practical deployment, which may shed light on previously overlooked vulnerabilities or attack approaches. Additionally, the complexities of human gaze, along with advanced algorithms necessary to support gaze analysis, offer numerous possible vulnerabilities that malicious agents may exploit, ranging from sensor-level vulnerabilities that construct basic gaze data to algorithm-level attacks that seize on weaknesses of pattern recognition and classification approaches [155].

4.2.1 Presentation Attack Detection

Presentation attacks are referred to as submitting fabricated or manipulated gaze data to authentication systems in a bid to gain unauthorized entry. This kind of action is a serious and viable danger to gaze authentication systems, at least by virtue of how simple it is for attackers to submit spoofed gaze data. According to definitions issued in ISO/IEC 30107:2023, there is a necessity to demarcate true presentation from presentation attack, and different modalities of attack (such as replay of a video, synthesis or generative attack, and mechanical devices). Presentation attack detection entails constructing analytical procedures capable of clearly distinguishing attack presentations from legitimate presentations, and concurrently ensuring sufficient authentication functionality for legitimate users [156]. Replay attacks are a primary challenge for gaze-based authentication: an adversary presents pre-recorded gaze patterns from an authorized user (e.g., on a display placed in front of the eye tracker) to spoof the point of regard. Effective countermeasures must discriminate in-vivo gaze from replays by exploiting cues that are difficult to synthesize, including microsaccades and other fine oculomotor dynamics, environment-dependent corneal reflections, and temporal artifacts indicative of artificial sources. Liveness detection assesses whether the captured signal originates

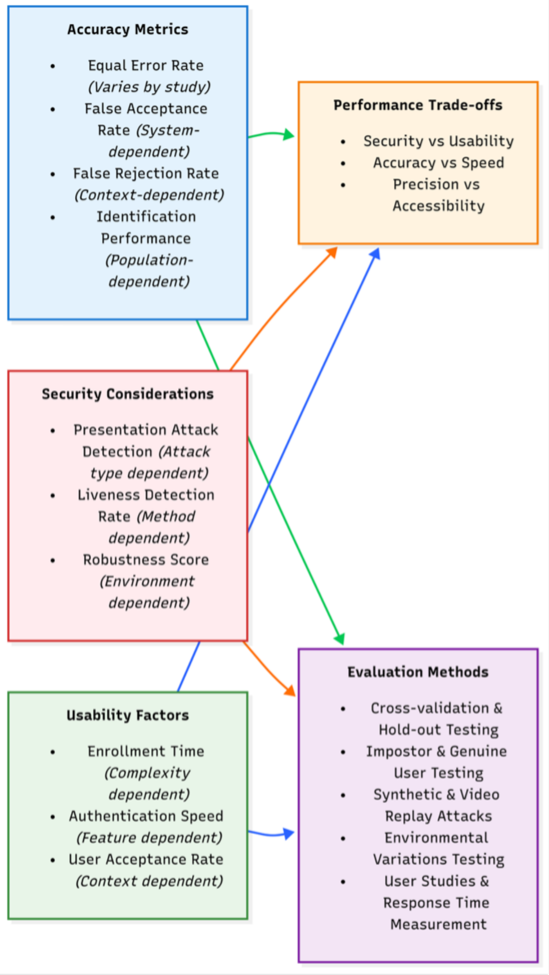
Accuracy Metrics
Equal Error Rate (Varies by study)
False Acceptance Rate (System-dependent)
False Rejection Rate (Context-dependent)
Identification Performance (Population-dependent)
Performance Trade-offs
Security vs Usability
Accuracy vs Speed
Precision vs Accessibility
Security Considerations
Presentation Attack Detection (Attack type dependent)
Liveness Detection Rate (Method dependent)
Robustness Score (Environment dependent)
Usability Factors
Enrollment Time (Complexity dependent)
Authentication Speed (Feature dependent)
User Acceptance Rate (Context dependent)
Evaluation Methods
Cross-validation & Hold-out Testing
Impostor & Genuine User Testing
Synthetic & Video Replay Attacks
Environmental Variations Testing
User Studies & Response Time Measurement

Figure 2. Performance Metrics and Security Trade-offs in Gaze-Based Authentication

from a live human by analyzing features such as the pupillary light reflex, natural micro-movements, and other physiological or behavioral signatures that are hard to fake. These approaches emphasize physiological indicators that separate genuine eyes from synthetic presentations [157, 158].

Sophisticated presentation attack detection methodologies employ advanced analysis techniques to detect subtle cues indicating the presence of fake gaze data. Challenge-response protocols require users to follow precise gaze paths or respond to dynamic stimuli, thus making replay attack approaches impossible since these are based on the need for real-time interaction instead of presenting static images. These methods could include arbitrary visual stimuli, interactive calibration techniques, or tasks that call for instant gaze responses, which cannot be pre-recorded or anticipated by possible attackers. Temporal consistency analysis examines the temporal attributes of gaze patterns with the aim of revealing spoofing attack evidence, noting that natural gaze behavior possesses unique temporal characteristics, such as inherent variability, correlation structures, and dynamic aspects that are difficult for replay attack tactics or synthetic generation algorithms to mimic [10, 137, 159].

4.2.2 Synthetic Data Detection

The developments in machine learning techniques dedicated to creating artificial data have posed new challenges before gaze authentication mechanisms. Modern algorithms have the potential of creating artificial gaze patterns that are significantly similar to genuine ones and consequently, have the potential of confusing authentication mechanisms by generating data that are reflective of the statistical and temporal profile of natural human gaze activity. This emerging threat shifts the attack landscape for gaze authentication: conventional presentation-attack detection may fail to flag carefully engineered synthetic gaze signals produced by advanced machine-learning models [155]. Generative Adversarial Networks (GANs) utilize state-of-the-art deep learning methods to synthesize artificial gaze patterns closely mimicking those displayed by real users. This generation is made possible through the use of adversarial training processes that successfully capture the complex statistical and temporal properties underlying human gaze behavior. The detection of GAN-generated gaze data requires the use of innovative analysis techniques able to identify faint artifacts present within these artificial patterns. These artifacts can include statistical anomalies, temporal discrepancies, or features discernible within the frequency space, which can indicate the synthetic origin of the generated data. The aim of statistical anomaly detection includes inspecting the statistical properties of gaze patterns to identify departures from normal human behavior. It recognizes that synthetic gaze data might have statistical properties different from those displayed by authentic human patterns, identifiable through methods such as modified correlation structures, anomalous distribution properties, or the lack of higher-order statistical dependences characteristic of legitimate human gaze movements [159, 160, 161].

Sophisticated detection approaches of synthetic data employ several complementary analysis techniques to promote the reliability of the detection process. Among them, frequency domain analysis exploits the spectral properties of gaze signals to detect synthetic data, since artificial construction mechanisms tend to embed specific artifacts in the frequency domain that are not present in natural gaze patterns. Such artifacts can appear as anomalous spectral peaks, missing frequency components, or different power distribution profiles. Additionally, multimodal verification fuses gaze analysis with other biometric modalities to strengthen spoofing resistance. Cross-modal consistency checks leverage correlations between gaze and complementary physiological or behavioral traits, forcing attackers to generate coherent synthetic signals across modalities simultaneously. This requirement raises the attack complexity substantially and reduces the likelihood of successful spoofing [162].

4.2.3 Robustness Against Advanced Attacks

Sophisticated attackers with deep knowledge of authentication mechanisms and access to bespoke tools pose the most significant threats to gaze-based deployments in challenging environments. Careful analysis of these threats is essential to pinpoint vulnerabilities and to design countermeasures that withstand well-planned, well-resourced attacks. Assessing resilience requires studying subtle and emerging attack profiles driven by rapid technological advances. Adversarial machine-learning attacks manipulate gaze signals to induce misclassification while remaining imperceptible to humans, exploiting algorithmic blind spots with carefully crafted perturbations. These understated threats leverage insight into the specific models used, enabling gaze patterns tailored to algorithmic weaknesses. Physical device spoofing includes mechanically replicating eye motion or presenting artificial eye imagery via robotic eye simulators, high-definition displays, or actuators that reproduce eye dynamics. Effective defenses against physical spoofing demand holistic security measures that evaluate hard-to-simulate properties—subtle movement signatures, biological processes, and environment-dependent interactions [11, 85, 163].

Social engineering attacks exploit observation or interaction to extract a user's gaze behavior, which is then replicated via behavioral mimicry or technological aids. Effective countermeasures must account for the visibility and replicability of gaze cues—some aspects can be gleaned through casual surveillance—since such leakage can seed later spoofing attempts. Insider threats occur when adversaries hold legitimate access to systems or data; with knowledge of internals, templates, or operating procedures, insiders can circumvent controls and thus pose a particularly challenging risk. Mitigations require robust template protection and tightly scoped access controls that curb privileged misuse while preserving necessary administrative functionality [10, 87]. To synthesize these concerns, Table 5 maps major attack classes to representative vectors, primary defenses, and key limitations.

4.3 Usability Assessment and User Experience Evaluation

Usability assessment addresses practical aspects of deployment and user acceptance, recognizing that security must be balanced with user experience for successful real-world operation across diverse populations and contexts. Evaluation spans subjective satisfaction, objective performance metrics, accessibility, and long-term adoption. Gaze-based authentication introduces specific challenges due to the interaction paradigm, potential learning effects, and the need to accommodate users with varying technology familiarity and distinct visual/motor characteristics [97].

4.3.1 User Experience and Acceptance Factors

User experience studies examine phenomenological aspects of gaze authentication, including user satisfaction, perceived security, usability, and intent to adopt such systems in diverse settings. This evaluation provides valuable understanding regarding the variables determining the end-users' acceptance of and efficient usage of gaze authentication systems during practical application contexts. Understanding end-users' perspective is critical to the effective integration of such systems and long-term usage, with even

Table 5. Attack Classification and Defense Strategies for Gaze-Based Authentication

Attack Class	Description	Representative Vectors	Primary Defenses	Notes/Limitations
Video replay (presentation)	Replayed eye videos or on-screen animations	Screen/display spoofing near sensor	Challenge–response tasks, liveness via pupillary light reflex, blink/microsaccade cues	Needs unpredictable prompts, may raise usability costs
Synthetic/generative (GAN/VAE)	AI-generated gaze sequences resembling user	Data-driven synthesis matched to template	Temporal/frequency anomaly detection, multi-modal cross-check, PAD ensembles	Arms race with generative models, require up-to-date detectors
Mechanical simulation	Robotic/optical rigs emulate eye kinematics	Robotic eye, motorized rigs, high-res displays	Oculomotor-plant liveness (OPC), 3D consistency, corneal-reflection physics checks	Specialized but high-threat for high-value targets
Adversarial ML	Crafted inputs to fool classifiers	Digital perturbations, surrogate-model attacks	Adversarial training, input sanitization, model ensembling	May degrade accuracy, difficult to comprehensively defend
Template compromise	Theft/modification of stored templates	Insider breach, insecure storage	Cancelable templates, encryption at rest/in transit, Homomorphic Encryption (HE)/Secure Multi-Party Computation (SMPC), Differential Privacy (DP)	Requires careful key management, revocability constraints
Social engineering/observation	Observing and mimicking gaze behavior	Shoulder surfing, surveillance	Challenge–response, multi-factor fusion, behavioral variance checks	Low-tech but partially effective without CR

the most advanced authentication methodology suffering failure if it does not meet end-users' demands or comprehensively address privacy, usability, and social acceptability concerns [164]. The survey of perceived security examines user confidence in gaze-based authentication technologies compared with standard authentication processes. This survey contends that users are inclined to perceive gaze-based authentication as safer than password authentication, foremost based upon the great difficulty involved with duplicating or impersonating gaze movements. However, concerns about privacy and monitoring are often expressed by users, which could influence their receptiveness to adopting such technology. Real-world studies show that users' perceptions of security are shaped by multiple factors, including their understanding of the technology, prior experience with biometric authentication, and awareness of potential vulnerabilities and attack surfaces. Usability findings emphasize simplicity and consistency in gaze-based authentication: users generally prefer mechanisms that require fewer explicit actions and integrate seamlessly into daily routines with minimal workflow disruption or behavior change. In this respect, gaze-based methods offer inherent advantages by enabling passive, continuous authentication during routine computer use, without explicit user effort [165].

Privacy concerns strongly influence willingness to adopt gaze-based recognition. Users worry that rich gaze data could reveal sensitive attributes beyond identity—cognitive states, health indicators, interests, or behavioral patterns—information they may wish to keep private. Addressing these concerns requires fair privacy policies and technical safeguards that harden recognition pipelines. Recommended measures include data minimization, secure storage and transmission, and user-centric controls over biometric information. Social acceptability also shapes adoption: the visibility of eye-tracking hardware, calibration demands, and potential stigma around biometrics can deter use, particularly in public or professional settings [166, 167]. Trust is built when systems demonstrate consistent performance, transparency, and robust security; cultivating trust depends on clear communication and dependable operation [168].

4.3.2 Authentication Time and Efficiency

Authentication time is a key usability factor: users expect prompt results that do not disrupt ongoing tasks. Requirements vary by application context and user expectations. Gaze-based systems must balance sufficient data collection for security with responsiveness, creating an inherent accuracy–usability trade-off that requires careful tuning across deployments. Although the fleeting nature of gaze enables continuous authentication, observation windows must still be long enough to reliably discriminate among users [169]. Data-collection duration analysis estimates the time needed to acquire enough gaze evidence for dependable decisions; required durations depend on system complexity, environmental conditions, and individual variability. Processing-latency evaluation measures the time for feature extraction, matching, and decision making. Real-time applications must keep latency low enough for interactive interfaces while allocating computation to preserve accuracy. Achieving this balance calls for efficient algorithms, parallel or pipelined processing, and, where appropriate, specialized hardware [9, 170].

Overall authentication time spans both data acquisition and processing, providing an end-to-end measure of responsiveness from initiation to decision. Timing requirements vary by application, and user satisfaction hinges on balancing security confidence against response time. In continuous authentication, effectiveness depends on computational overhead and attentional cost: systems must preserve identity assurance while minimizing user distraction and resource consumption, which calls for algorithms that maintain authentication state with low load [91, 171].

4.3.3 Calibration Requirements and System Setup

Calibration procedures form an underlying factor of the effectiveness of gaze-based authentication systems. Strict or demanding calibration requirements could significantly impact user acceptance and system usability, potentially creating barriers that outweigh the security benefits of gaze-based authentication. There is a need for effective systems that reduce calibration requirements without compromising authentication accuracy. Such a need highlights the imperative of creating new methodologies that can provide reliable gaze measurement without subjecting end-users to the need for adequate technical knowledge or the willingness to undergo complex procedures [172, 173, 174]. This initial calibration difficulty assessment considers the time, effort, and skill invested in the initial installation of a system. It recognizes that simple calibration procedures, requiring minimal end-user guidance and little technical expertise, are necessary to promote widespread adoption across various end-users with differing technological capabilities. This consideration of calibration requirement standards examines the frequency with which end-users must perform repeated calibration processes to maintain authentication integrity. Systems that require frequent recalibration are met with resistance from end-users and practical impediments in field deployment that can undermine their potential in real-world applications, since users expect systems to be reliable without needing to be constantly maintained or adapted [175, 176].

Automatic calibration methods strive to minimize explicit calibration dependency by utilizing adaptive approaches that derive knowledge of user attributes during typical system usage. This innovation marks a significant advancement, with the potential of boosting usability while maintaining authentication effectiveness through smart manipulation of characteristic variables and variable environmental parameters. These approaches harness machine learning mechanisms that allow the dynamic tuning of calibration parameters based on user experiences and feedbacks of system responses, thus allowing systems themselves to automatically compensate for changes of user attributes or conditions of context without requiring explicit processes of recalibration. Cross-session calibration stability determines the effectiveness of calibration parameters transferability across different usage sessions and environmental settings, with effective calibration reducing the requirement of frequent setup processes and boosting consistent authentication performance across different usage patterns and time intervals [99, 177].

4.3.4 Environmental Adaptability and Robustness

Environmental robustness evaluates the performance of systems under a wide range of conditions users are likely to face in real-world uses. It recognizes that authentication processes need to function well in the varied conditions typically present in normal use environments as opposed to the controlled conditions of lab tests. For authentication systems to be effective, it is critical that they provide consistent performance despite the many variables inherent in real-world environments, such as varying light, ambient noise, user locations, and environmental factors that could affect the accuracy of visual judgments and user behavior [178]. Lighting robustness tests a system's performance under different lighting conditions, including natural, artificial, and low-light environments. This testing is critical because it ensures that gaze authentication systems maintain their effectiveness under lighting conditions commonly found in real-world applications, eliminating the need for adjustments according to the environment or user behavioral patterns. Background noise and distractions testing examines the system's resilience to visual or auditory disruption that might affect users' gaze responses. Ideal systems should maintain authentication accuracy even in conditions where users find themselves distracted or subjected to concurrent demands for their attention that draw their attention away from the authentication task. System functionality testing in a multi-user environment tests its performance with multiple users, considering potential interference from others and the system's capacity to correctly identify the intended user while avoiding the authentication of nearby users who might be in contact with the system [89, 179, 180].

Device mobility and positioning flexibility evaluate system tolerance for variations in user positioning, device orientation, and movement during authentication, recognizing that mobile authentication systems must accommodate natural variations in device usage patterns including handheld operation, desktop usage, and mobile scenarios where users may not maintain consistent positioning relative to eye-tracking sensors. These adaptability requirements present significant challenges for gaze-based authentication systems, as environmental variations can affect both the quality of gaze measurements and the consistency of user gaze patterns, requiring sophisticated algorithms that can maintain authentication performance while adapting to changing conditions and usage contexts [181].

4.3.5 Accessibility and Inclusive Design

Issues of accessibility extend to the ability of gaze authentication schemes to support end-users with different visual capabilities, motor capabilities, and levels of technological expertise. This highlights the underlying maxim that authentication schemes should allow equitable access to security technology by all end-users across the broad range of human diversity. Inclusive design principles require authentication schemes to allow equitable access by large end-user bases, since the deprivation of even one particular end-user base constitutes not just an ethical challenge but also a practical constraint, negatively impacting market penetration and societal impact of gaze authentication schemes.

The analysis of visual impairment accommodations addresses the effectiveness of systems designed for users suffering from varied forms and severities of visual impairment. It is recognized that while gaze-based authentication essentially requires functional vision, these systems should be adapted to enable individuals with corrected vision, partial visual impairment, or specific visual conditions like astigmatism, color blindness, or age-related modifications in vision that could affect the accuracy or reliability of gaze measurements. Motor disability requirements address the needs of individuals suffering from motor impairments that could hinder head movement, eye motion regulation, or device interactions. This scenario calls for the creation of adaptive systems that can adapt to the inherent variations in motor control capabilities while maintaining the accuracy and security of authentication. Age-related variations in performance explain how accuracy and usability in authentication differ among age groups and note that aging could affect various aspects of visual and motor capability that could render gaze authentication less effective. These include modifications in visual acuity, eye movement dynamics, attentional control, and technology familiarity [32, 68]. Cultural and linguistic factors can influence gaze behavior—for example, reading direction, script characteristics, or culturally shaped viewing habits—so systems must deliver consistent performance across groups to avoid bias or degraded effectiveness. Differences in technological sophistication also matter: users with limited experience may find setup and interaction challenging. Authentication workflows should therefore provide clear guidance and assistance while avoiding digital barriers that exclude less-experienced users. Given the relative newness of gaze-based authentication, accessibility deserves particular emphasis; unconventional usage patterns and diverse needs may require inclusive design accommodations [182, 183]. Table 8 summarizes the principal usability and configuration considerations, outlining typical performance indicators, key influencing factors, and the associated design implications.

Table 6. Usability and Setup Summary for Gaze-Based Authentication

Factor	Typical Range/Observation	Primary Drivers	Design Implications
Enrollment time	Variable (study-dependent)	Stimuli length, session protocol, calibration	Minimize via efficient stimuli and implicit calibration
Authentication speed	Variable depending on complexity	Feature richness, processing latency	Balance accuracy vs. latency, precompute where possible
Calibration frequency	Low–medium (desired)	Drift, device changes, lighting	Use drift detection and auto-calibration to reduce burden
Continuous auth overhead	Low–moderate	Sampling rate, model complexity	Duty-cycling, adaptive sampling, on-device inference
User acceptance	Variable, limited field studies	Perceived privacy, friction, reliability	Transparent privacy, clear feedback, low failure costs
Accessibility	Varies	Visual conditions, motor control, age	Inclusive design, alternative modes/fallbacks

4.4 Datasets and Benchmarks for Gaze-Based Authentication

The development and evaluation of gaze-authentication schemes largely rely on the availability of high-quality datasets that contain diverse patterns of gaze from diverse users, conditions, and settings. Standard datasets allow shared research, fair comparisons across diverse approaches of methodology, and consequently encourage the development of robust machine learning models that can be widely generalized across diverse application settings. The quality of available datasets largely dictates the research questions that are enabled and the validity of experimental results, making the choice of datasets a critical factor behind the design of authentication schemes.

Available datasets for gaze-based authentication vary widely in scope, scale, and purpose, aligning with diverse research goals and deployment scenarios. Some are collected in controlled laboratories with high-precision eye trackers to support fine-grained physiological analyses; others capture more naturalistic behavior closer to in-the-wild conditions. Temporal coverage also differs markedly: certain datasets include a single session suitable for early prototyping, whereas others provide longitudinal recordings that enable studies of temporal stability and extended authentication protocols. Validating algorithms therefore demands datasets with accurate ground-truth labels, sufficient sample sizes for statistical power, and representative populations spanning usage conditions. Cross-dataset comparisons are complicated by differences in hardware, collection protocols, stimulus paradigms, and subject demographics, underscoring the need for domain adaptation and careful generalization when designing systems for varied contexts. Table 7 summarizes key datasets frequently cited in gaze-authentication research, highlighting distinctive characteristics, scale, hardware configurations, and application relevance.

Table 7. Key Datasets for Gaze-Based Authentication Research

Dataset	Modality/Context	Subjects/Sessions	Sampling/Hardware	Stimuli	Identity Labels	Notes
GazeBase [15]	Desktop, multi-stimulus	Large-scale, longitudinal	Research-grade eye trackers	Mixed (reading, pursuit, saccades)	Yes	Longitudinal; suitable for temporal stability and ID
GazeBaseVR [16]	VR/HMD binocular	Large-scale, longitudinal	Head-Mounted Display (HMD)-integrated trackers	VR tasks	Yes	VR context; binocular sign cross-domain studies
NVGaze [51]	Near-eye dataset	—	Near-eye sensors	Gaze calibration tasks	Yes/Meta	Anatomy-informed; low-latency benchmarks
Gaze360 [18]	In-the-wild appearance-based	~238 subjects	RGB cameras, unconstrained	Free viewing	Indirect	Robust appearance-based estimation
LPW [17]	Pupil detection	22	Unconstrained videos	Free viewing	N/A	Pupil/feature detection benchmarking

5 Applications and Use Cases

This section investigates application domains for gaze-based biometric authentication deployment, examining unique requirements, challenges, and opportunities across domains from high-security commercial to consumer applications requiring seamless user experiences. Each domain has different accuracy, latency, environmental, and usage specifications requiring tailored implementation strategies. Figure 3 visualizes these diverse domains and system adaptations.

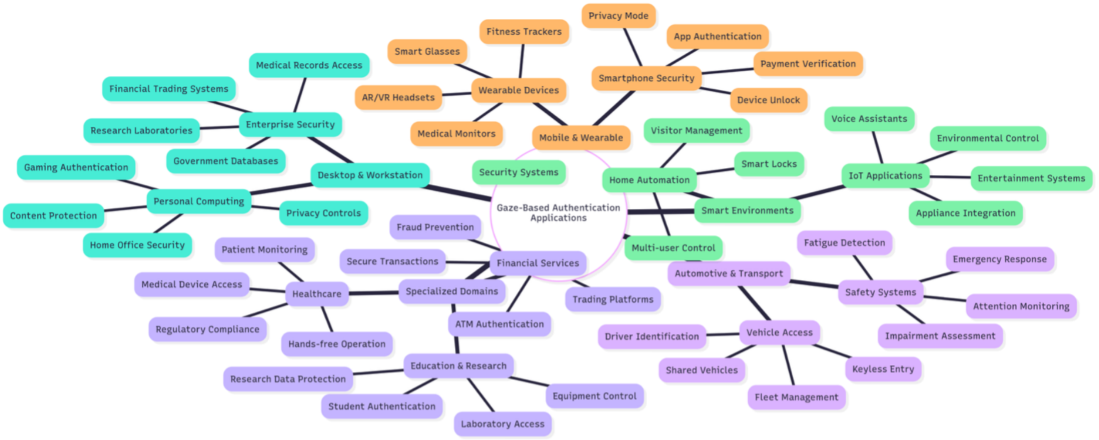

Figure 3. Gaze-Based Authentication Deployment Scenarios and Application Domains

This application landscape illustrates the diverse deployment scenarios where gaze-based authentication provides unique advantages. Each application domain presents distinct requirements regarding accuracy, speed, environmental conditions, and user experience, necessitating tailored approaches to system design and implementation (see Table 8).

Table 8. Deployment Domains and Requirements for Gaze-Based Authentication

Domain	Primary Requirements	Typical Hardware	Auth Mode	Reported Metrics (examples)	Notes
Desktop/Workstation	High accuracy, continuous auth, low friction	Desktop IR trackers	Continuous + periodic	Low EER in controlled lab settings	Enterprise, research labs
Mobile/Tablet	Robust to motion/lighting, low power	Front RGB cam	Quick unlock + in-app	Moderate FRR in the wild	Short sessions, ambient use
Wearables/VR/AR	Hands-free, low latency, comfort	HMD-integrated trackers	Continuous	Varies by HMD, task	XR privacy/safety constraints
Automotive	Safety-critical, reliability	Integrated cameras	Continuous + attention	Robustness > raw EER	Must not hinder safety
Smart Home/IoT	Convenience, shared devices	Embedded cams/sensors	Event-based	PAD emphasis	Multi-user, ambient contexts

5.1 Desktop and Workstation Security

Desktop and workstation security utilizes controlled environments and computational resources for high-accuracy gaze-based authentication. Desktop settings provide consistent user positioning, controlled lighting, and ample compute, enabling sophisticated authentication methods. These conditions support high accuracy and integrate smoothly with established workflows [184].

5.1.1 Enterprise Security Applications

Enterprise environments are well-suited to gaze-based authentication because operations are centrally managed with strong security and productivity requirements. These settings handle sensitive data and regulatory obligations, so authentication must be low-friction while defending against both external and insider threats [29, 185]. Trading platforms use gaze-based authentication for continuous trader verification when accessing confidential market data and executing high-risk transactions. Gaze pattern stability provides uninterrupted verification without disrupting operations while increasing financial transaction security. Health information systems use gaze authentication for electronic patient record and medical equipment access, enforcing Health Insurance Portability and Accountability Act (HIPAA) compliance. Hands-free operation benefits examination rooms where contact may be impractical due to infection control or sterile condition requirements [186, 187]. Government and defense systems benefit from gaze-based authentication for sensitive data protection and secure facility access. High-security environments leverage inherent anti-spoofing properties and continuous authentication for constant security monitoring. Research and development facilities use gaze authentication to secure intellectual property while permitting uninterrupted legitimate user access. This increases productivity while maintaining security, especially in team environments requiring shared resource access with personal accountability [185, 188].

5.1.2 Personal Computer Security

Personal computer security applications focus on protecting individual user privacy and data while providing convenient authentication for home environments. These applications balance security needs, user acceptance, and economic considerations, recognizing individual users have different priorities, budgets, technical skills, and usage patterns compared to enterprise environments [12]. Password substitution schemes use gaze-based authentication instead of conventional passwords, providing security from password-related vulnerabilities while enhancing convenience and reducing cognitive burden. Literature reports significant user preference for gaze-based authentication, especially among users with password handling challenges. Multi-factor authentication complemented by gaze biometrics creates secure schemes robust across attack vectors while remaining understandable to users with minimal security knowledge. This integration yields authentication systems combining gaze patterns with standard factors [189]. Parental control software uses gaze-based authentication to restrict content or application access by user identity, leveraging the inherent difficulty of overcoming gaze authentication for effective access control against children or unauthorized parties. Privacy-preserving applications implement gaze authentication for private document, communication, and sensitive operation access. Continuous authentication systems enable automatic shutdown upon unauthorized party detection, ensuring constant privacy protection without requiring active user security actions [190, 191].

5.2 Mobile and Wearable Device Authentication

Mobile and wearable device authentication leverages ubiquitous mobile technology with integrated eye-tracking capabilities, supporting gaze-based authentication across diverse user populations and usage environments. Implementations must address device mobility, environmental changes, and resource constraints including battery limitations, computational capability, lighting variations, and location changes affecting performance. Mobile platforms offer advantages and challenges, promising widespread applicability while requiring novel approaches to overcome technical and usability issues [50].

5.2.1 *Smartphone and Tablet Security*

Smartphone and tablet apps leverage front-facing cameras and on-device compute to deliver gaze-based authentication without dedicated hardware, broadening accessibility for mainstream users. Designs must account for mobile usage patterns—handheld motion, user movement, lighting variability—and remain effective across device orientations and operating modes. Gaze-based device unlocking can replace PINs, passwords, or fingerprints, improving convenience while mitigating shoulder-surfing risks and passcode complexity. Integration with existing platform security services and protocols simplifies deployment and preserves compatibility with familiar applications. Mobile payment authentication uses gaze-based biometrics for financial payments, combining device ownership and biometric authentication for effective two-factor authentication in high-value transactions, addressing mobile financial service security issues [192, 193]. Application-specific authentication uses gaze-based biometrics to control access to specific applications or datasets, enabling rigorous access management based on user identity and context. This strategy benefits shared device environments and sensitive applications like banking, healthcare, or enterprise systems requiring stringent protection. Continuous authentication monitors user identity during sessions and automatically secures devices upon detecting untrusted users. This prevents unauthorized access when devices are unattended while ensuring seamless experiences for trusted users without intrusive authentication requests [194, 195].

5.2.2 *Wearable Technology Integration*

Wearable computing integration enables gaze-based authentication in smartwatches, fitness trackers, smart glasses, and other devices, providing convenient hands-free authentication across everyday activities. Applications must work under strict power and computational constraints while maintaining reliability through innovative algorithmic optimization, energy efficiency, and interface design [74, 41]. Smart glasses authentication leverages native eye-tracking functionality for hands-free interface communication and customized user experiences. Combining gaze authentication with augmented reality enables context-aware computing while addressing privacy and security concerns in public spaces. Personalized fitness trackers use gaze authentication for accurate health data attribution while protecting privacy. Automatic user recognition enables device sharing without compromising data integrity, essential for family fitness tracking and shared device usage [196, 197]. Smartwatch security programs utilize gaze-based authentication for device unlocking and payment verification, complementing security for devices vulnerable to theft or loss. Programs integrate with existing platforms developing robust architectures protecting devices and services. Medical technology implements gaze biometrics for wearable medical equipment access and accurate patient data capture. Authentication system reliability and security are critical in medical environments where data integrity affects patient care and unauthorized access compromises safety and privacy [198, 199].

5.3 Automotive and Transportation Security

Gaze-based authentication in automotive and transport security enables vehicle access control, driver identification, and system personalization. Authentication solutions must meet high dependability, safety, and security standards, performing reliably under harsh environmental conditions including temperature variations, vibration, changing lighting, and requiring fail-safe operation ensuring vehicle safety integrity. The automotive setting offers unique benefits with predetermined driver locations relative to systems, while presenting challenges related to safety-critical functions and seamless integration with existing vehicle systems [200, 201].

5.3.1 *Vehicle Access and Personalization*

Motor vehicle personalized access systems incorporate gaze authentication replacing traditional key-based control, enabling automatic vehicle settings adjustment based on driver identity. This technology provides improved user experience with enhanced security and convenience while requiring high security and dependability under diverse environmental conditions with fail-safe measures preventing lockout or misuse. Keyless entry systems use gaze-based authentication for vehicle access without physical keys or fobs, increasing security while reducing risks from misplaced or stolen keys. Driver recognition systems automatically identify registered drivers and adjust vehicle settings including seat positions, mirrors, temperature, and infotainment options while providing ongoing identity authentication during operation [202, 203]. Fleet management systems utilize gaze-based authentication to monitor driver identity and ensure operational procedure compliance. Real-time driver identity monitoring enhances fleet security and accountability, preventing unauthorized use while monitoring behavior and ensuring safety regulation compliance. Shared vehicle authentication uses gaze-based biometrics for car-sharing and ride-sharing access control, ensuring access limitation to authorized individuals. This technology enables smooth access experiences for shared mobility services by eliminating physical key exchange requirements [204, 205].

5.3.2 Driver Monitoring and Safety Systems

Driver safety and monitoring systems combine gaze authentication with attention monitoring and fatigue detection to enhance vehicular safety while facilitating identity confirmation. This provides end-to-end solutions addressing security and safety issues through integrated gaze analysis systems requiring reliability under all driving conditions with robust algorithms differentiating normal gaze fluctuations from potential safety threats while maintaining accurate identity verification. Attention monitoring systems utilize gaze tracking technology to determine the attentiveness and alertness of drivers, with the added benefit of providing continuous identity verification. The integration of safety monitoring with authentication creates comprehensive driver surveillance solutions capable of detecting both unauthorized drivers and attention lapses that could undermine safety. The addition of fatigue detection combines gaze authentication with algorithms for determining fatigue levels and thus ensures that only alert, authorized drivers are operating the vehicle. Such a feature is highly applicable in situations like commercial transport and long-distance driving, where driver fatigue poses significant safety issues and regulatory necessities can demand constant monitoring of drivers [206, 207]. Impairment detection systems are essential for monitoring eye movement patterns to identify signs of driver impairment, while also ensuring ongoing identity authentication. This feature allows such systems to limit vehicle use by unauthorized or impaired drivers through instantaneous evaluation of gaze traits that can indicate intoxication caused by alcohol, drug use, or health conditions that compromise driving safety. The integration of emergency response functions uses driver identity data collected from verification based on gaze to enable individualized emergency actions and relevant medical information during accidents. This feature improves emergency response efficiency and patient outcomes by allowing first responders to obtain critical information related to driver identity, medical conditions, emergency contact numbers, and other relevant information that can affect emergency treatment decisions [200, 201].

5.4 Smart Home and IoT Applications

The use of smart home technology in combination with the Internet of Things (IoT) supports gaze-based authentication paradigms by adding them to environmental control systems, home security systems, and ambient computing platforms. This combination supports robust authentication features that can easily integrate into the growing ecosystem of networked devices found in modern homes. Such applications often run under challenging environmental conditions and need to support a broad range of user populations and usage patterns that include different levels of technology expertise, varying physical skills, and diverse household configurations that include children, older adults, and visitors that require different degrees of access and engagement with the system [208, 209].

5.4.1 Smart Home Security and Ambient Computing

Residential security systems integrate gaze-based verification with traditional lock functionality, improving security and convenience. These systems must provide consistent performance under varying environmental conditions, lighting, weather, and diverse user demographics [210, 211]. Intelligent lock systems employ gaze authentication for keyless access, eliminating conventional keys while providing security against lock picks and duplicates. Integration with smart home networks enables comprehensive security solutions combining surveillance with identity-based interventions. Visitor management systems incorporate gaze authentication for access control while ensuring privacy. In shared households, gaze authentication provides customized access control and settings for different members, supporting age-restricted filtering and personalized device configurations [210, 211, 208, 209]. The applications of ambient computing and personalization use gaze-based authentication to create adaptive surroundings tailored to user identity and preference without explicit interaction. This provides an example of smart environments where the technology permeates daily life by means of non-intrusive authentication and personalization technologies [53, 212]. Environmental control systems use gaze-based authentication mechanisms to switch lights, temperature, and other parameters automatically according to the identity of the person. Entertainment system customization assists with individualized content suggestions and access controls, but the inclusion of appliances adds personalized use and security for smart devices. Voice assistant customization utilizes gaze and voice biometrics for improved multi-modal authentication for ambient computing settings [213].

6 Challenges and Future Directions

This section analyzes current limitations, research needs, and potential developments in gaze-based biometric authentication. We outline adoption hurdles while highlighting promising research avenues. Improvement requires addressing technical limitations and system issues including standardization, user acceptance, and real-world implementation. The challenges and opportunities illustrate complex interactions between technological advances, user expectations, and practical limitations. Understanding these challenges enables balancing current limitations with innovations for widespread implementation across applications [13, 14, 137].

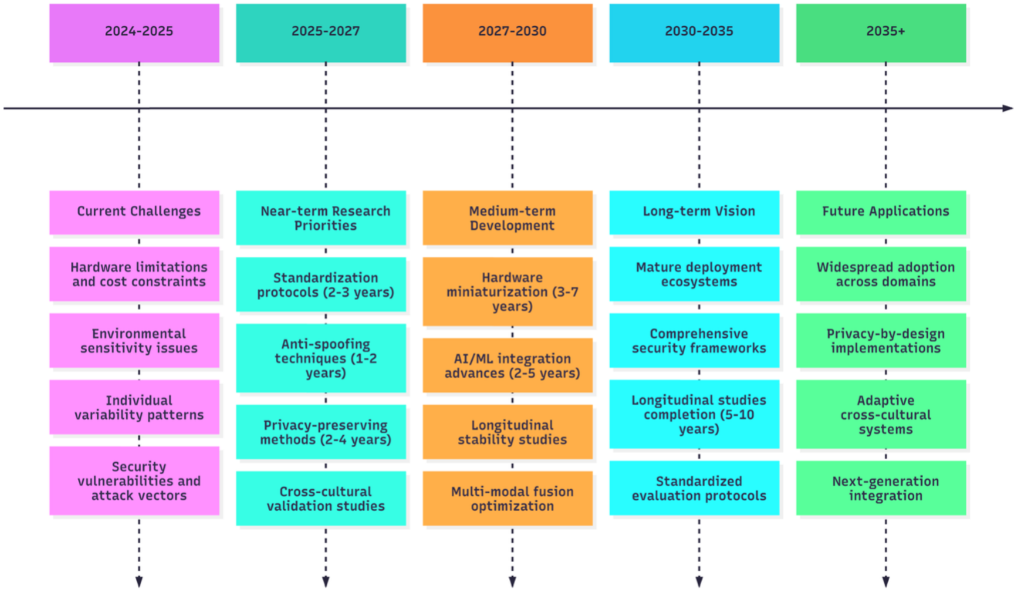
2024-2025
2025-2027
2027-2030
2030-2035
2035+
Current Challenges
Hardware limitations and cost constraints
Environmental sensitivity issues
Individual variability patterns
Security vulnerabilities and attack vectors
Near-term Research Priorities
Standardization protocols (2-3 years)
Anti-spoofing techniques (1-2 years)
Privacy-preserving methods (2-4 years)
Cross-cultural validation studies
Medium-term Development
Hardware miniaturization (3-7 years)
AI/ML integration advances (2-5 years)
Longitudinal stability studies
Multi-modal fusion optimization
Long-term Vision
Mature deployment ecosystems
Comprehensive security frameworks
Longitudinal studies completion (5-10 years)
Standardized evaluation protocols
Future Applications
Widespread adoption across domains
Privacy-by-design implementations
Adaptive cross-cultural systems
Next-generation integration

Figure 4. Research Roadmap for Gaze-Based Authentication (2024-2035)

This research roadmap illustrates the evolutionary path from current challenges to future opportunities in gaze-based authentication, showing the progression from addressing immediate technical limitations through near-term research priorities and medium-term development goals to achieving the long-term vision of mature, standardized deployment across diverse application domains.

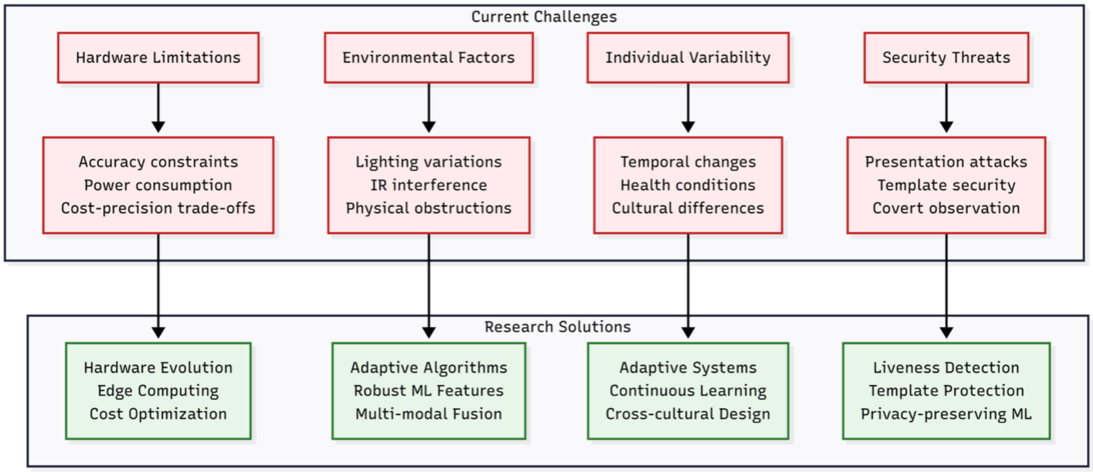

Figure 5. Risk Assessment Matrix for Gaze-Based Authentication Systems

This challenge–solution matrix illustrates how current research systematically addresses core limitations while creating opportunities for advanced applications and broader societal impact in gaze-based authentication systems.

Table 9. Risk Assessment and Mitigation Strategies for Gaze-Based Authentication

Risk Category	Risk Level	Impact	Likelihood	Mitigation Strategies	Research Priority
Spoofing Attacks	High	Critical	Medium	CR tasks (randomized stimuli), Pupil Light Response (PLR) cues, blink/microsaccade dynamics, OPC checks; anti-synthetic temporal/spectral analysis; fusion with periocular/face [10, 38, 137, 159]	Very High
Privacy Breaches	High	High	Medium	On-device inference; encryption at rest/in-transit; HE/SMPC/DP; data minimization [119]	High
Environmental Variations	Medium	Medium	High	Adaptive illumination; robust features; auto-recalibration/drift detection; quality gating [99, 179]	High
Hardware Limitations	Medium	High	Low	Redundancy; watchdogs; safe fallback modes; health monitoring	Medium
User Acceptance	Medium	Medium	Medium	Implicit calibration; low-friction User Experience (UX); transparent privacy controls; clear feedback	Medium
Calibration Drift	Low	Medium	Medium	Online adaptation; drift detection; periodic light-touch recalibration [175, 174]	Medium
Health Conditions	Low	High	Low	—	Low

6.1 Current Limitations and Technical Challenges

Despite substantial progress in gaze-based authentication, inherent limitations still constrain practicality and usability across contexts and user populations. These span hardware accuracy and environmental robustness; algorithmic constraints driven by inter- and intra-person variability and temporal drift; emerging attack vectors; privacy risks; and usability factors such as acceptance and system complexity. Systematically characterizing these limitations is essential to steer future research, set realistic performance targets, and design mitigations without compromising core quality attributes. Addressing them will require interdisciplinary collaboration that integrates advances in hardware, algorithms, security evaluation, and human–computer interaction.

6.1.1 Hardware and Environmental Constraints

Hardware limitations remain a primary obstacle to wide-scale deployment of gaze-based authentication, constraining effectiveness and viability across application domains. Current eye-tracking technology faces practical challenges that force trade-offs among accuracy, cost, power consumption, and environmental robustness. Consumer-grade trackers typically lag research-grade devices in accuracy, leaving difficult authentication tasks out of reach on commodity hardware. This accessibility–precision tension complicates consumer deployment: broad availability often comes at the expense of the fidelity needed for reliable decisions. Sensitivity to illumination, infrared interference, and occlusions further degrades tracking quality and authentication performance, and many schemes still assume controlled conditions rarely met in practice [103]. Persistent calibration requirements also hinder usability; despite progress in automatic methods, most systems still need user-specific calibration that is time-consuming and may need to be repeated, creating friction that suppresses adoption and everyday use. Moreover, technical limitations around power consumption limit the use of gaze authentication systems in mobile and wearable technology since eye-tracking hardware and computational processes come with significant power requirements, thereby reducing battery life and making continuous authentication applications less practical. Therefore, development of energy-conserving gaze authentication systems is another key area of research that has to balance the demands of authentication performance against the need to conserve energy [53, 105].

6.1.2 Individual Variability and Temporal Stability

The uniqueness of gaze patterns provides biometric verification with both great promise and challenging situations, creating a paradox that inherently contains distinctive features that make it challenging to develop algorithms. This uniqueness requires using sophisticated methods that are capable of distinguishing relevant individual features from momentary fluctuations. Inter-individual variability in gaze patterns can be substantial, requiring systems to model diverse human behavior while maintaining discrimination capability. Factors such as age, visual acuity, and cultural background influence patterns, creating challenges for consistent performance across populations. Intra-individual variability from fatigue, emotional state, and environmental conditions requires systems to distinguish natural variations from impostor attempts [36, 214]. Temporal stability varies across gaze characteristics, with some features stable over time while others change due to aging, health conditions, or learning effects. Understanding long-term stability is crucial for robust systems. Learning effects may improve consistency but create vulnerabilities if attackers can replicate patterns [215].

6.1.3 *Security Vulnerabilities and Attack Vectors*

Inherent vulnerabilities in gaze-based authentication remain a persistent challenge, demanding careful analysis and design to maintain effective security across diverse attack scenarios. As technology advances, dynamic risk patterns emerge with attackers designing increasingly subtle tactics. As system deployment increases, attackers are expected to develop more elaborate assault techniques exploiting technological vulnerabilities and human conduct, emphasizing constant security protocol enhancement and threat profiling for effective countermeasures against developing attack vectors. Presentation attack evolution continues with attackers developing new approaches for avoiding gaze-based authentication schemes. Although current frameworks are capable of detecting simple replay attack attempts, advanced approaches to spoofing, such as the development of artificial data or mechanical stimulations, pose serious challenges that justify developing countermeasures. Template security is of utmost concern for gaze-based authentication schemes, largely because of the large behavioral data incorporated into gaze templates that potentially could be used by malicious parties for purposes other than authentication. This scenario raises serious privacy issues and offers opportunities for malicious parties intending to breach user data, consider identity theft, unauthorized behavioral inspection, or conduct other malicious operations. The security vulnerability related to covert perception results from the capabilities of attackers to monitor and capture user gaze streams covertly, potentially with the application of social engineering mechanisms. The potential gaze streams at issue are obtainable through video observation and custom-built hardware, making them different from other biometric modalities, which are more difficult to monitor covertly [10, 87, 163].

The vulnerabilities inherent in machine learning, especially for gaze verification systems, are open to exploitation through adversarial attacks, which manipulate input data to result in misclassification. Given the growing use of machine-learning–based verification, it is essential to characterize and mitigate these vulnerabilities to preserve system integrity. The threat is significant: adversaries can mount remote, input-space attacks using carefully crafted samples that appear benign to human reviewers yet induce misclassification [85]. AI-generated synthetic gaze can produce realistic sequences (e.g., via GANs/VAEs) that evade conventional systems. Effective countermeasures should advance liveness/PAD and develop robust classifiers that detect subtle temporal- and frequency-domain artifacts in synthetic data, while privacy-preserving methods must prevent inference of cognitive or health attributes inadvertently encoded in gaze [216, 161].

6.2 Research Gaps and Future Directions

Our review identifies several key research gaps in gaze-based biometric authentication. Many of these gaps are interrelated and will require coordinated efforts spanning data collection, modeling, evaluation, and deployment. A persistent issue is the over-reliance on Western samples with limited cross-cultural validation. Differences in reading direction, attentional conventions, and norms of eye contact can affect stability and discriminability, risking biased performance. Future work should establish standardized cross-cultural protocols and develop adaptive algorithms that accommodate diversity without explicit profiling to ensure fairness across populations. Closely linked is the relatively underexplored question of temporal stability and plasticity of gaze patterns. Long-term stability remains poorly characterized, particularly with respect to aging, medical conditions, and environmental variation over extended periods. The visual system changes with age—presbyopia, reduced contrast sensitivity, slower saccades, and shifts in attentional allocation—which can degrade authentication accuracy over time. Medical impairments, corrective interventions, and progressive ocular disorders introduce additional temporal variation that systems must accommodate without increasing spoofing risk. More research is needed on flexible systems that track gradual change, define principled re-enrollment strategies for different user groups, and disentangle legitimate temporal variation from adversarial manipulation.

The proliferation of AI-generated synthetic gaze data poses severe security risks, making reliable detection and mitigation imperative. Modern generative models—GANs and VAEs—can synthesize highly plausible gaze behaviors that threaten deployed mechanisms. As realism increases, defenses must co-evolve: liveness/PAD should advance, and robust authentication models must discriminate minute artifacts in fabricated sequences. In parallel, privacy-preserving protocols are needed to prevent leakage of sensitive attributes from gaze patterns, including cognitive processes, health status, and emotional state inferred from eye-movement dynamics. Progress is further hindered by the absence of standardized evaluation methods, reference datasets, and agreed-upon metrics, which prevents fair comparison across populations, systems, and deployment scenarios. Closing this gap requires benchmark platforms that reflect real-world variability in users and environments, standardized datasets spanning deployment contexts, and clear reporting guidelines to support reproducibility and rigorous comparison. These research needs create opportunities for methods that directly address current limitations while enabling new applications; priorities include adaptive algorithms for diverse populations, resilient security frameworks against evolving attacks, standardized test procedures, and privacy-preserving modalities to enable safe deployment of gaze-based authentication.

6.3 Emerging Trends and Future Opportunities

The trend of technological convergence opens potential possibilities for gaze-based authentication while, at the same time, introducing challenges in need of innovative research approaches. Emerging trends need to be comprehensively understood in order to develop research frameworks and ensure that systems have sufficient malleability for networked technological environments. Machine learning and artificial intelligence advancements are a main driving factor for gaze-based authentication advancements. Core to this advancement are deep learning approaches, allowing increasingly advanced gaze analysis algorithms to become progressively efficient in smaller numbers of training datasets and increasingly robust in variability in environmental conditions. Convolutional and recurrent neural networks are particularly effective for improving gaze estimation and authentication accuracy: they capture subtle pattern nuances and adapt as conditions change without hand-engineered features. Edge computing is reshaping deployment by moving substantial computation onto mobile and embedded devices, reducing latency, strengthening on-device privacy, and enabling strategies previously limited by compute or connectivity constraints [95].

Hardware engineering developments enable new applications through enhanced sensor functionality, creating small, accurate, energy-efficient eye-tracking devices integrated into consumer products. Advances in camera technologies, infrared illumination, and signal processing enable consumer-grade devices achieving research-grade performance while maintaining practical resource requirements and power consumption. These innovations are crucial for mobile and wearable technologies where size, weight, and battery limitations traditionally prevented sophisticated eye-tracking deployment.

Immersive computing platforms employing augmented and virtual reality create new environments for gaze-dependent authentication techniques. These platforms offer unique integration opportunities with natural user interactions through inherent gaze tracking for foveated rendering. However, they present challenges for authentication mechanisms in interactive three-dimensional environments with variable visual stimulation and dynamic orientations [19, 217].

Application domains are rapidly evolving: IoT growth creates opportunities for gaze-based authentication across new device classes but introduces resource and deployment constraints. IoT deployments require methods that operate under strict compute, power, and network budgets while still delivering security. A central challenge is to design lightweight algorithms that sustain acceptable performance and interoperate across heterogeneous IoT platforms [208]. Autonomous and robotic systems present promising HRI use cases, enabling continuous operator verification to enhance safety and security. These systems must operate effectively in dynamic environments with mobile platforms, changing illumination, and varied user orientations, requiring robust algorithms maintaining authentication effectiveness through difficult conditions [218, 219]. Healthcare and medical practice offer prominent gaze-based authentication scenarios, driven by hands-free operation needs and increased security for medical equipment and patient data. Healthcare markets require stringent robustness, safety, and regulatory compliance, necessitating specially designed methodologies and careful validation. As a non-contact solution, gaze-based authentication suits hospital settings where other input methods may be impractical due to sterile conditions or patient care requirements [187]. Financial technology applications increasingly explore gaze-based authentication to enhance digital payment and banking platform security through continuous authentication and improved user experience. These applications require high security and reliability while maintaining user convenience and regulatory compliance, offering opportunities for advanced authentication processes providing security integration without compromising usability [186].

6.4 Recommendations for Future Research

Based on our analysis, we recommend targeted research areas addressing current gaps. Priority areas include standardization efforts, as the lack of widely adopted evaluation procedures hinders approach comparisons and interoperable system development. Standard methodologies would enable fair result comparison and commercial viability. Longitudinal studies are essential for understanding long-term stability and performance. Current work uses small samples and short timeframes, limiting practical understanding. Research should address aging, health changes, environmental factors, and learning effects while developing adaptive algorithms maintaining security [137]. Cross-cultural validation ensures consistent operation across

Table 10. Future Research Directions and Priorities

Research Area	Priority Level	Expected Impact	Timeline	Key Challenges	Required Resources
Standardization Protocols	Very High	High	2-3 years	Industry consensus, Regulatory approval	Standards bodies, Industry collaboration
Anti-Spoofing Techniques	Very High	Critical	1-2 years	Advanced attack methods, Real-time detection	Security expertise, Attack datasets
Privacy-Preserving Methods	High	High	2-4 years	Performance trade-offs, Regulatory compliance	Cryptography expertise, Legal frameworks
Cross-Cultural Validation	High	Medium	3-5 years	Global data collection, Cultural sensitivity	International collaboration, Diverse datasets
Longitudinal Studies	High	Medium	5-10 years	Long-term commitment, Participant retention	Sustained funding, Research infrastructure
Hardware Miniaturization	Medium	High	3-7 years	Technical limitations, Cost constraints	Hardware R&D, Manufacturing partnerships
AI/ML Integration	Medium	High	2-5 years	Algorithm complexity, Training data	Computing resources, ML expertise

diverse populations, examining reading habits, attention strategies, and cultural protocols while developing adaptive algorithms without explicit profiling. Security evaluation frameworks must address conventional and emerging attacks including AI-generated patterns and advanced spoofing methods [220]. Methodological developments include synthetic data generation for training while mitigating privacy concerns, requiring validation to ensure realistic behavior without artifacts. Explainable AI techniques enable understanding of authentication decisions and bias identification, crucial for trust and fairness [86, 221].

Federated learning enables collaborative development while preserving user privacy and data locality, avoiding centralized aggregation vulnerabilities. Real-world evaluation frameworks should replace laboratory-only testing to provide reliable vulnerability and capability measures [222].

7 Conclusion

This survey integrates 222 publications within a three-dimensional taxonomic framework combining authentication approaches, system architectures, and security evaluations, addressing gaps in previous literature. Unlike HCI-focused surveys, this work integrates threat-oriented security analysis with practitioner-focused comparisons across datasets, hardware, and deployments. Our systematic review methodology encompassed multiple academic sources including major databases (IEEE Xplore, Springer Link, ScienceDirect, ACM Digital Library, MDPI), conference proceedings, and preprint repositories with rigorous inclusion criteria prioritizing peer-reviewed studies with clear experimental protocols and quantitative metrics. The resulting taxonomy provides researchers and practitioners with structured guidance for methodology selection, architectural decisions, and security considerations across diverse application domains. This comprehensive framework enables systematic comparison of approaches while identifying critical research gaps and future opportunities in gaze-based biometric authentication systems.

Physiological characteristics exhibit temporal stability and resistance to voluntary control, whereas behavioral characteristics facilitate drift-resilient calibration. Hybrid approaches consistently outperform single-modality systems—often by orders of magnitude in Equal Error Rate (EER)—delivering higher accuracy and stronger spoof resistance at the cost of greater complexity. Architectural trade-offs persist between precision and cost: desktop IR trackers offer the highest accuracy but are several times more expensive than consumer alternatives. Mobile/edge deployments are increasingly viable by leveraging on-device inference and adaptive calibration, addressing latency and privacy constraints. Cloud deployments provide scalability when appropriate privacy controls are in place, while state-of-the-art software pipelines can achieve usable accuracy using only commercial-off-the-shelf cameras, broadening deployability without specialized sensors. Security remains a central concern, necessitating effective liveness detection, presentation-attack detection, multimodal fusion, and strong template protection across diverse deployment scenarios.

Enterprise desktop deployments benefit from continuous verification, whereas XR and automotive applications are constrained by latency and safety requirements that mandate real-time processing and fail-safe mechanisms. Mobile and IoT scenarios require a careful balance of power efficiency and privacy, often favoring edge processing to reduce data transmission while maintaining authentication effectiveness. Healthcare settings are strong candidates given hands-free interaction needs and stringent privacy regulation, while financial trading platforms leverage continuous monitoring for high-value, high-security transactions. Smart-home and ambient-intelligence use cases are promising through sensor-network integration, though heterogeneous devices and limited standardization remain hurdles. These varied demands call for adaptive authentication protocols that adjust to context-dependent security requirements and environmental constraints.

Three core weaknesses hinder widespread adoption: (i) an accuracy–cost imbalance in commodity hardware; (ii) limited real-world robustness across diverse environmental conditions; and (iii) the absence of standardized evaluation protocols that enable meaningful performance comparisons. Privacy preservation and fairness across cultural groups remain critical challenges requiring immediate attention. Our analysis identifies priority research areas addressing these limitations through standardized evaluation protocols aligned with ISO/IEC 19795-1 and 30107-3 standards, enabling consistent and threat-aware testing of research contributions. Enhanced presentation attack detection must implement temporal and spectral signature analysis to counteract replay attacks, mechanical simulation, and AI-generated artificial gaze patterns while hardening template security and session robustness mechanisms. Privacy-preserving learning methodologies, including federated learning, differential privacy, and homomorphic encryption, should be integrated with architectures optimized for end-device inference to minimize exposure and transmission of sensitive biometric data. Cross-cultural validation and longitudinal stability research must develop adaptive authentication mechanisms capable of distinguishing between legitimate temporal changes and fraudulent access attempts. Application-specific benchmarks and datasets for XR, automotive, and mobile/IoT domains should be published with reproducible evaluation pipelines to accelerate practical deployment. Limitations include English-language bias potentially underrepresenting regional research contributions, rapidly evolving AI-based attack methods that outpace defensive measures, and varied evaluation protocols that limit meta-analysis capabilities across studies. Integrating sound engineering practices, comprehensive evaluation frameworks, and privacy-by-design principles can establish gaze-based authentication as a trusted security component across diverse applications. Realizing this potential requires coordinated efforts spanning hardware design innovation, algorithm development, security evaluation standardization, and international collaboration on regulatory frameworks.

Acknowledgements

The authors thank the creators of the GazeBase, GazeBaseVR, Gaze360, and LPW datasets, and anonymous reviewers for their valuable feedback.

Authors contributions

Author 1: Conceptualization, Writing – Original Draft, Supervision. Author 2: Literature Review, Data Curation, Visualization. Author 3: Formal Analysis, Writing – Review and Editing.

Conflict of interest

The authors have no conflict of interest to declare.

References

[1] Bonneau J, Herley C, Van Oorschot PC, Stajano F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE symposium on security and privacy. IEEE; 2012. p. 553-67.

[2] Florencio D, Herley C. A large-scale study of web password habits. In: Proceedings of the 16th international conference on World Wide Web; 2007. p. 657-66.

[3] Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology. 2004;14(1):4-20.

[4] Khamis M, Hassib M, Zezschwitz Ev, Bulling A, Alt F. GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication. In: Proceedings of the 19th acm international conference on multimodal interaction; 2017. p. 446-50.

[5] Rigas I, Komogortsev OV. Current research in eye movement biometrics: An analysis based on BioEye 2015 competition. Image and Vision Computing. 2017;58:129-41.

[6] Holland C, Komogortsev OV. Biometric identification via eye movement scanpaths in reading. In: 2011 International joint conference on biometrics (IJCB). IEEE; 2011. p. 1-8.

[7] Komogortsev OV, Jayarathna S, Aragon CR, Mahmoud M. Biometric identification via an oculomotor plant mathematical model. In: Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications; 2010. p. 57-60.

[8] Kasprowski P, Ober J. Eye movements in biometrics. In: International Workshop on Biometric Authentication. Springer; 2004. p. 248-58.

[9] Komogortsev OV, Karpov A. Liveness detection via oculomotor plant characteristics: Attack of mechanical replicas. In: 2013 international conference on biometrics (ICB). IEEE; 2013. p. 1-8.

[10] Hadid A, Evans N, Marcel S, Fierrez J. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine. 2015;32(5):20-30.

[11] Ebrahimpour N, Ayden MA, Altay B. Liveness control in face recognition with deep learning methods. The European Journal of Research and Development. 2022;2(2):92-101.

[12] Katsini C, Abdrabou Y, Raptis GE, Khamis M, Alt F. The role of eye gaze in security and privacy applications: Survey and future HCI research directions. In: Proceedings of the 2020 CHI conference on human factors in computing systems; 2020. p. 1-21.

[13] Cavoukian A, et al. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada. 2009;5(2009):12.

[14] Mansfield A. Information technology–biometric performance testing and reporting–part 1: Principles and framework. ISO/IEC. 2006:19795-1.

[15] Griffith H, Lohr D, Abdulin E, Komogortsev O. GazeBase, a large-scale, multi-stimulus, longitudinal eye movement dataset. Scientific Data. 2021;8(1):184.

[16] Lohr D, Aziz S, Friedman L, Komogortsev OV. GazeBaseVR, a large-scale, longitudinal, binocular eye-tracking dataset collected in virtual reality. Scientific Data. 2023;10(1):177.

[17] Tonsen M, Zhang X, Sugano Y, Bulling A. Labelled pupils in the wild: a dataset for studying pupil detection in unconstrained environments. In: Proceedings of the ninth biennial ACM symposium on eye tracking research & applications; 2016. p. 139-42.

[18] Kellnhofer P, Recasens A, Stent S, Matusik W, Torralba A. Gaze360: Physically unconstrained gaze estimation in the wild. In: Proceedings of the IEEE/CVF international conference on computer vision; 2019. p. 6912-21.

[19] Agarwal A, Ramachandra R, Venkatesh S, Prasanna SM. Biometrics in extended reality: a review. Discover Artificial Intelligence. 2024;4(1):81.

[20] Leigh RJ, Zee DS. The neurology of eye movements. Oxford university press; 2015.

[21] Daugman J. How iris recognition works. In: The essential guide to image processing. Elsevier; 2009. p. 715-39.

[22] Bowyer KW, Hollingsworth K, Flynn PJ. Image understanding for iris biometrics: A survey. Computer vision and image understanding. 2008;110(2):281-307.

[23] Ebrahimpour N. Iris recognition using mobilenet for biometric authentication. In: 9th International zeugma conference on scientific research, Gaziantep, Turkey; 2023. .

[24] Bednarik R, Kinnunen T, Mihaila A, Fränti P. Eye-movements as a biometric. In: Scandinavian conference on image analysis. Springer; 2005. p. 780-9.

[25] Lisberger SG, Morris EJ, Tychsen L. Visual motion processing and sensory-motor integration for smooth pursuit eye movements. Annual review of neuroscience. 1987;10:97-129.

[26] Laeng B, Sirois S, Gredebäck G. Pupillometry: A window to the preconscious? Perspectives on psychological science. 2012;7(1):18-27.

[27] Hallal L, Rhinelander J, Venkat R. Recent trends of authentication methods in extended reality: A survey. Applied System Innovation. 2024;7(3):45.

[28] Rigas I, Economou G, Fotopoulos S. Biometric identification based on the eye movements and graph matching techniques. Pattern Recognition Letters. 2012;33(6):786-92.

[29] Eberz S, Rasmussen KB, Lenders V, Martinovic I. Looks like eve: Exposing insider threats using eye movement biometrics. ACM Transactions on Privacy and Security (TOPS). 2016;19(1):1-31.

[30] Rayner K, Li X, Williams CC, Cave KR, Well AD. Eye movements during information processing tasks: Individual differences and cultural effects. Vision research. 2007;47(21):2714-26.

[31] Schuetz I, Fiehler K. Eye tracking in virtual reality: Vive pro eye spatial accuracy, precision, and calibration reliability. Journal of Eye Movement Research. 2022;15(3):10-16910.

[32] Rayner K. Eye movements in reading and information processing: 20 years of research. Psychological bulletin. 1998;124(3):372.

[33] Zhang Y, Hu W, Xu W, Chou CT, Hu J. Continuous authentication using eye movement response of implicit visual stimuli. proceedings of the acm on interactive, mobile, wearable and ubiquitous technologies. 2018;1(4):1-22.

[34] Yoon HJ, Carmichael TR, Tourassi G. Gaze as a biometric. In: Medical Imaging 2014: Image Perception, Observer Performance, and Technology Assessment. vol. 9037. SPIE; 2014. p. 39-45.

[35] Ebaid D, Crewther SG. Visual information processing in young and older adults. Frontiers in aging neuroscience. 2019;11:116.

[36] Rayner K. The 35th sir frederick bartlett lecture: Eye movements and attention in reading, scene perception, and visual search, 62,(8). 62,(8); 2009.

[37] Seha S, Papangelakis G, Hatzinakos D, Zandi AS, Comeau FJ. Improving eye movement biometrics using remote registration of eye blinking patterns. In: ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE; 2019. p. 2562-6.

[38] Boutros F, Damer N, Raja K, Ramachandra R, Kirchbuchner F, Kuijper A. Fusing iris and periocular region for user verification in head mounted displays. In: 2020 IEEE 23rd International Conference on Information Fusion (FUSION). IEEE; 2020. p. 1-8.

[39] Ma W, Li M, Wu J, Zhang Z, Jia F, Zhang M, et al. Multiple step saccades in simply reactive saccades could serve as a complementary biomarker for the early diagnosis of Parkinson's disease. Frontiers in Aging Neuroscience. 2022;14:912967.

[40] Li S, Savaliya S, Marino L, Leider AM, Tappert CC. Brain signal authentication for human-computer interaction in virtual reality. In: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). IEEE; 2019. p. 115-20.

[41] Krishna V, Ding Y, Xu A, Höllerer T. Multimodal biometric authentication for VR/AR using EEG and eye tracking. In: Adjunct of the 2019 International Conference on Multimodal Interaction; 2019. p. 1-5.

[42] Mathis F, Fawaz HI, Khamis M. Knowledge-driven biometric authentication in virtual reality. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems; 2020. p. 1-10.

[43] Mathis F, Williamson J, Vaniea K, Khamis M. Rubikauth: Fast and secure authentication in virtual reality. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems; 2020. p. 1-9.

[44] George C, Khamis M, von Zezschwitz E, Burger M, Schmidt H, Alt F, et al. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS; 2017. .

[45] Pandiani DSM, Presutti V. Seeing the intangible: Surveying automatic high-level visual understanding from still images. CoRR. 2023.

[46] Olade I, Liang HN, Fleming C, Champion C. Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr). In: Proceedings of the 2020 4th international conference on virtual and augmented reality simulations; 2020. p. 45-52.

[47] Holland A, Morelli T. Dynamic keypad–digit shuffling for secure pin entry in a virtual world. In: International Conference on Virtual, Augmented and Mixed Reality. Springer; 2018. p. 102-11.

[48] Rajarajan S, Maheswari K, Hemapriya R, Sriharilakshmi S. Shoulder surfing resistant virtual keyboard for internet banking. World Applied Sciences Journal. 2014;31(7):1297-304.

[49] Liebers J, Schneegass S. Gaze-based authentication in virtual reality. In: ACM Symposium on Eye Tracking Research and Applications; 2020. p. 1-2.

[50] D'Amelio A, Patania S, Bursic S, Cuculo V, Boccignone G. Using gaze for behavioural biometrics. Sensors. 2023;23(3):1262.

[51] Kim J, Stengel M, Majercik A, De Mello S, Dunn D, Laine S, et al. Nvgaze: An anatomically-informed dataset for low-latency, near-eye gaze estimation. In: Proceedings of the 2019 CHI conference on human factors in computing systems; 2019. p. 1-12.

[52] Kotwal K, Ulucan I, Ozbulak G, Selliah J, Marcel S. Vrbiom: a new periocular dataset for biometric applications of hmd. arXiv preprint arXiv:240702150. 2024.

[53] Bulling A, Ward JA, Gellersen H, Tröster G. Eye movement analysis for activity recognition using electrooculography. IEEE transactions on pattern analysis and machine intelligence. 2010;33(4):741-53.

[54] Zhang Y, Chong MK, Müller J, Bulling A, Gellersen H. Eye tracking for public displays in the wild. Personal and Ubiquitous Computing. 2015;19(5):967-81.

[55] Summaira J, Li X, Shoib AM, Li S, Abdul J. Recent advances and trends in multimodal deep learning: A review. arXiv preprint arXiv:210511087. 2021.

[56] Trifan M, Ionescu B, Ionescu D. A Real Time Self-Generating Control for AI Platforms. In: 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI). IEEE; 2024. p. 000599-604.

[57] Mungoli N. Adaptive feature fusion: enhancing generalization in deep learning models. arXiv preprint arXiv:230403290. 2023.

[58] Progonov D, Cherniakova V, Kolesnichenko P, Oliynyk A. Behavior-based user authentication on mobile devices in various usage contexts. EURASIP Journal on Information Security. 2022;2022(1):6.

[59] Barua A, Ahmed MU, Begum S. A systematic literature review on multimodal machine learning: Applications, challenges, gaps and future directions. Ieee access. 2023;11:14804-31.

[60] Hammad M, Liu Y, Wang K. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. Ieee Access. 2018;7:26527-42.

[61] Hassan B, Izquierdo E, Piatrik T. Soft biometrics: A survey: Benchmark analysis, open challenges and recommendations. Multimedia Tools and Applications. 2024;83(5):15151-94.

[62] Ross A, Jain A. Information fusion in biometrics. Pattern recognition letters. 2003;24(13):2115-25.

[63] Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion. Information Fusion. 2019;52:187-205.

[64] Kaur G, Bhushan S, Singh D. Fusion in multimodal biometric system: A review. Indian Journal of Science and Technology. 2017;10(28):1-10.

[65] Malhotra M, Chhabra I. MANIT: a multilayer ANN integrated framework using biometrics and historical features for online examination proctoring. Scientific Reports. 2025;15(1):29302.

[66] Reynolds DA, Quatieri TF, Dunn RB. Speaker verification using adapted Gaussian mixture models. Digital signal processing. 2000;10(1-3):19-41.

[67] Epp C, Lippold M, Mandryk RL. Identifying emotional states using keystroke dynamics. In: Proceedings of the sigchi conference on human factors in computing systems; 2011. p. 715-24.

[68] Stellmach S, Dachselt R. Look & touch: gaze-supported target acquisition. In: Proceedings of the SIGCHI conference on human factors in computing systems; 2012. p. 2981-90.

[69] Jain A, Nandakumar K, Ross A. Score normalization in multimodal biometric systems. Pattern recognition. 2005;38(12):2270-85.

[70] Diaz RAC, Ghita M, Copot D, Birs IR, Muresan C, Ionescu C. Context aware control systems: An engineering applications perspective. IEEE Access. 2020;8:215550-69.

[71] Komogortsev OV, Karpov A, Price LR, Aragon C. Biometric authentication via oculomotor plant characteristics. In: 2012 5th IAPR International Conference on Biometrics (ICB). IEEE; 2012. p. 413-20.

[72] Sluganovic I, Roeschlin M, Rasmussen KB, Martinovic I. Using reflexive eye movements for fast challenge-response authentication. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016. p. 1056-67.

[73] Song C, Wang A, Ren K, Xu W. Eyeveri: A secure and usable approach for smartphone user authentication. In: IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. IEEE; 2016. p. 1-9.

[74] Zhu H, Jin W, Xiao M, Murali S, Li M. Blinkey: A two-factor user authentication method for virtual reality devices. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2020;4(4):1-29.

[75] Jeon J, Noh YG, Kim J, Hong JH. Pre-AttentiveGaze: gaze-based authentication dataset with momentary visual interactions. Scientific Data. 2025;12(1):263.

[76] Lohr D, Proulx MJ, Raju MH, Komogortsev OV. Ocular Authentication: Fusion of Gaze and Periocular Modalities. arXiv preprint arXiv:250517343. 2025.

[77] Čeněk J, Halámková D, Caha J, Lacko D, Kalenská P, Stachoň Z, et al. Cross-cultural analysis of eye-movement patterns in visual scene perception: a comparison of seven cultural samples. Scientific Reports. 2025;15(1):28574.

[78] Lohr D, Griffith H, Komogortsev OV. Eye know you: Metric learning for end-to-end biometric authentication using eye movements from a longitudinal dataset. IEEE Transactions on Biometrics, Behavior, and Identity Science. 2022;4(2):276-88.

[79] Le Bras T, Allibe B, Doré-Mazars K. The way we look at an image or a webpage can reveal personality traits. Scientific Reports. 2024;14(1):15488.

[80] Linka M, Broda MD, Alsheimer T, de Haas B, Ramon M. Characteristic fixation biases in Super-Recognizers. Journal of Vision. 2022;22(8):17-7.

[81] Pusara M, Brodley CE. User re-authentication via mouse movements. In: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security; 2004. p. 1-8.

[82] Egner T. Principles of cognitive control over task focus and task switching. Nature Reviews Psychology. 2023;2(11):702-14.

[83] Rigas I, Economou G, Fotopoulos S. Human eye movements as a trait for biometrical identification. In: 2012 IEEE fifth international conference on biometrics: theory, applications and systems (BTAS). IEEE; 2012. p. 217-22.

[84] Bulling A, Weichel C, Gellersen H. EyeContext: Recognition of high-level contextual cues from human visual behaviour. In: Proceedings of the sigchi conference on human factors in computing systems; 2013. p. 305-8.

[85] Biggio B, Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018. p. 2154-6.

[86] Goodfellow IJ, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative adversarial nets. Advances in neural information processing systems. 2014;27.

[87] Nagar A, et al. Biometric template security. Michigan State University. Computer Science; 2012.

[88] Boutros F, Damer N, Raja K, Ramachandra R, Kirchbuchner F, Kuijper A. Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation. Image and Vision Computing. 2020;104:104007.

[89] Morimoto CH, Koons D, Amir A, Flickner M. Pupil detection and tracking using multiple light sources. Image and vision computing. 2000;18(4):331-5.

[90] Ohno T, Mukawa N, Yoshikawa A. FreeGaze: a gaze tracking system for everyday gaze interaction. In: Proceedings of the 2002 symposium on Eye tracking research & applications; 2002. p. 125-32.

[91] Kumar M, Garfinkel T, Boneh D, Winograd T. Reducing shoulder-surfing by using gaze-based password entry. In: Proceedings of the 3rd symposium on Usable privacy and security; 2007. p. 13-9.

[92] Phillips PJ, Scruggs WT, O'toole AJ, Flynn PJ, Bowyer KW, Schott CL, et al. FRVT 2006 and ICE 2006 large-scale experimental results. IEEE transactions on pattern analysis and machine intelligence. 2009;32(5):831-46.

[93] Poh N, Bengio S. Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication. Pattern Recognition. 2006;39(2):223-33.

[94] Martin A, Doddington G, Kamm T, Ordowski M, Przybocki M. The DET curve in assessment of detection task performance. 1997.

[95] Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE internet of things journal. 2016;3(5):637-46.

[96] Narcizo FB, Dos Santos FED, Hansen DW. High-accuracy gaze estimation for interpolation-based eye-tracking methods. Vision. 2021;5(3):41.

[97] Kar A, Corcoran P. A review and analysis of eye-gaze estimation systems, algorithms and performance evaluation methods in consumer platforms. IEEE Access. 2017;5:16495-519.

[98] Elnozahy SSFA, Pari SC, Liang LC. Raspberry Pi-Based Face Recognition Door Lock System. IoT. 2025;6(2):31.

[99] Hansen DW, Pece AE. Eye tracking in the wild. Computer Vision and Image Understanding. 2005;98(1):155-81.

[100] Tonsen M, Steil J, Sugano Y, Bulling A. Invisibleeye: Mobile eye tracking using multiple low-resolution cameras and learning-based gaze estimation. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2017;1(3):1-21.

[101] Abbeloos W, Goedemé T. Exploring the potential of combining time of flight and thermal infrared cameras for person detection. arXiv preprint arXiv:161202223. 2016.

[102] Cheng Y, Wang H, Bao Y, Lu F. Appearance-based gaze estimation with deep learning: A review and benchmark. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2024;46(12):7509-28.

[103] Hansen DW, Ji Q. In the eye of the beholder: A survey of models for eyes and gaze. IEEE transactions on pattern analysis and machine intelligence. 2009;32(3):478-500.

[104] Kudinov AA, Elsakov SM. Improved continuous authentication system with counterfeit protection. Journal of Computational and Engineering Mathematics. 2019;6(1):35-47.

[105] Morimoto CH, Mimica MR. Eye gaze tracking techniques for interactive applications. Computer vision and image understanding. 2005;98(1):4-24.

[106] Zhu Z, Ji Q. Novel eye gaze tracking techniques under natural head movement. IEEE Transactions on biomedical engineering. 2007;54(12):2246-60.

[107] Sigut J, Sidha SA. Iris center corneal reflection method for gaze tracking using visible light. IEEE Transactions on Biomedical Engineering. 2010;58(2):411-9.

[108] Li F, Munn S, Pelz J. A model-based approach to video-based eye tracking. Journal of Modern Optics. 2008;55(4-5):503-31.

[109] Krafka K, Khosla A, Kellnhofer P, Kannan H, Bhandarkar S, Matusik W, et al. Eye tracking for everyone. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2016. p. 2176-84.

[110] Jeyaraman N, Jeyaraman M, Yadav S, Ramasubramanian S, Balaji S. Revolutionizing healthcare: the emerging role of quantum computing in enhancing medical technology and treatment. Cureus. 2024;16(8).

[111] Cerrolaza JJ, Villanueva A, Cabeza R. Study of polynomial mapping functions in video-oculography eye trackers. ACM Transactions on Computer-Human Interaction (TOCHI). 2012;19(2):1-25.

[112] Blignaut P. A new mapping function to improve the accuracy of a video-based eye tracker. In: Proceedings of the south african institute for computer scientists and information technologists conference; 2013. p. 56-9.

[113] Yoo DH, Chung MJ. A novel non-intrusive eye gaze estimation using cross-ratio under large head motion. Computer Vision and Image Understanding. 2005;98(1):25-51.

[114] Zhang C, Chi J, Zhang Z, Gao X, Hu T, Wang Z. Gaze estimation in a gaze tracking system. Science China Information Sciences. 2011;54(11):2295-306.

[115] Baobaid A, Meribout M, Tiwari VK, Pena JP. Hardware accelerators for real-time face recognition: A survey. Ieee Access. 2022;10:83723-39.

[116] İBRAHİMOĞU N, Aytekin MC, Yıldız F. Knowledge Distillation from ResNet to MobileNet for Accurate On-Device Face Recognition. AIPA's International Journal on Artificial Intelligence: Bridging Technology, Society and Policy. 2025;1(2):1-15.

[117] İbrahimoğlu N, Osmani A, Ghaffari A, Günay FB, Çavdar T, Yıldız F. FootprintNet: a Siamese network method for biometric identification using footprints. The Journal of Supercomputing. 2025;81(5):714.

[118] McMahan B, Moore E, Ramage D, Hampson S, y Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics. PMLR; 2017. p. 1273-82.

[119] Dwork C, Roth A, et al. The algorithmic foundations of differential privacy. Foundations and trends® in theoretical computer science. 2014;9(3–4):211-407.

[120] Thomas SG, Myakala PK. Beyond the cloud: Federated learning and edge ai for the next decade. Journal of Computer and Communications. 2025;13(2):37-50.

[121] Jain AK, Flynn P, Ross AA. Handbook of biometrics. Springer Science & Business Media; 2007.

[122] Yadav BP, Prasad CSS, Padmaja C, Korra SN, Sudarshan E. A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing. In: IOP Conference Series: Materials Science and Engineering. vol. 981. IOP Publishing; 2020. p. 022043.

[123] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on Theory of computing; 2009. p. 169-78.

[124] Yao AC. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982). IEEE; 1982. p. 160-4.

[125] Abate AF, Nappi M, Riccio D, Sabatino G. 2D and 3D face recognition: A survey. Pattern recognition letters. 2007;28(14):1885-906.

[126] Yang S, Jin M, He Y. Continuous gaze tracking with implicit saliency-aware calibration on mobile devices. IEEE Transactions on Mobile Computing. 2022;22(10):5816-28.

[127] Ometov A, Petrov V, Bezzateev S, Andreev S, Koucheryavy Y, Gerla M. Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Network. 2019;33(2):82-8.

[128] Ross A, Jain AK. Multimodal biometrics: An overview. In: 2004 12th European signal processing conference. IEEE; 2004. p. 1221-4.

[129] Pankanti S, Prabhakar S, Jain AK. On the individuality of fingerprints. IEEE Transactions on pattern analysis and machine intelligence. 2002;24(8):1010-25.

[130] Wildes RP. Iris recognition: an emerging biometric technology. Proceedings of the IEEE. 2002;85(9):1348-63.

[131] Bhatti OS, Barz M, Sonntag D. EyeLogin-calibration-free authentication method for public displays using eye gaze. In: ACM Symposium on Eye Tracking Research and Applications; 2021. p. 1-7.

[132] Onyemauche U, Osundu U, Etumnu R, Nwosu Q. The use of Eye Gaze Gesture Interaction Artificial Intelligence Techniques for PIN Entry. 2020.

[133] Wang Y, Chen X, Wang Q. Privacy-preserving security inference towards cloud-edge collaborative using differential privacy. arXiv preprint arXiv:221206428. 2022.

[134] Patel C. Secure lightweight authentication for multi user IoT environment. arXiv preprint arXiv:220710353. 2022.

[135] Chen J, Dojen R, Jurcut A. Detection and prevention of new attacks for ID-based authentication protocols. In: Proceedings of the 2020 9th International Conference on Networks, Communication and Computing; 2020. p. 78-86.

[136] Ku M, Li T, Zhang K, Lu Y, Fu X, Zhuang W, et al. Imagenhub: Standardizing the evaluation of conditional image generation models. arXiv preprint arXiv:231001596. 2023.

[137] ISO/IEC 30107-1:2023 — iso.org;. [Accessed 02-09-2025]. https://www.iso.org/standard/83828.html.

[138] Dunn MJ, Alexander RG, Amiebenomo OM, Arblaster G, Atan D, Erichsen JT, et al. Minimal reporting guideline for research involving eye tracking (2023 edition). Behavior research methods. 2024;56(5):4351-7.

[139] Ghosh S, Dhall A, Hayat M, Knibbe J, Ji Q. Automatic gaze analysis: A survey of deep learning based approaches. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023;46(1):61-84.

[140] Lowe DG. Distinctive image features from scale-invariant keypoints. International journal of computer vision. 2004;60(2):91-110.

[141] Bay H, Tuytelaars T, Van Gool L. Surf: Speeded up robust features. In: European conference on computer vision. Springer; 2006. p. 404-17.

[142] Dalal N, Triggs B. Histograms of oriented gradients for human detection. In: 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05). vol. 1. Ieee; 2005. p. 886-93.

[143] Krizhevsky A, Sutskever I, Hinton GE. Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems. 2012;25.

[144] Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:14091556. 2014.

[145] He K, Zhang X, Ren S, Sun J. Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2016. p. 770-8.

[146] Kinnunen TH, Lee KA, Tak H, Evans N, Nautsch A. t-EER: Parameter-free tandem evaluation of countermeasures and biometric comparators. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023;46(5):2622-37.

[147] Huang G, Liu Z, Van Der Maaten L, Weinberger KQ. Densely connected convolutional networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2017. p. 4700-8.

[148] Szegedy C, Liu W, Jia Y, Sermanet P, Reed S, Anguelov D, et al. Going deeper with convolutions. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2015. p. 1-9.

[149] Schroff F, Kalenichenko D, Philbin J. Facenet: A unified embedding for face recognition and clustering. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2015. p. 815-23.

[150] Taigman Y, Yang M, Ranzato M, Wolf L. Deepface: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2014. p. 1701-8.

[151] Parkhi O, Vedaldi A, Zisserman A. Deep face recognition. In: BMVC 2015-Proceedings of the British Machine Vision Conference 2015. British Machine Vision Association; 2015. .

[152] Sun Y, Wang X, Tang X. Deep learning face representation from predicting 10,000 classes. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2014. p. 1891-8.

[153] Hu J, Shen L, Sun G. Squeeze-and-excitation networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2018. p. 7132-41.

[154] Woo S, Park J, Lee JY, Kweon IS. Cbam: Convolutional block attention module. In: Proceedings of the European conference on computer vision (ECCV); 2018. p. 3-19.

[155] Ali A, Hoque S, Deravi F. Directed Gaze Trajectories for biometric presentation attack detection. Sensors. 2021;21(4):1394.

[156] Hu G, Sun M, Zhang C. A High-Accuracy Advanced Persistent Threat Detection Model: Integrating Convolutional Neural Networks with Kepler-Optimized Bidirectional Gated Recurrent Units. Electronics. 2025;14(9):1772.

[157] Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, et al. Attention is all you need. Advances in neural information processing systems. 2017;30.

[158] Devlin J, Chang MW, Lee K, Toutanova K. Bert: Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers); 2019. p. 4171-86.

[159] Evans N. Handbook of biometric anti-spoofing: Presentation attack detection. Springer; 2019.

[160] Tan X, Triggs B. Enhanced local texture feature sets for face recognition under difficult lighting conditions. IEEE transactions on image processing. 2010;19(6):1635-50.

[161] Howard A, Sandler M, Chu G, Chen LC, Chen B, Tan M, et al. Searching for mobilenetv3. In: Proceedings of the IEEE/CVF international conference on computer vision; 2019. p. 1314-24.

[162] Zhang X, Zhou X, Lin M, Sun J. Shufflenet: An extremely efficient convolutional neural network for mobile devices. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2018. p. 6848-56.

[163] Uludag U, Jain AK. Attacks on biometric systems: a case study in fingerprints. In: Security, steganography, and watermarking of multimedia contents VI. vol. 5306. SPIE; 2004. p. 622-33.

[164] Kepkowski M, Machulak M, Wood I, Kaafar D. Challenges with passwordless FIDO2 in an enterprise setting: A usability study. In: 2023 IEEE secure development conference (SecDev). IEEE; 2023. p. 37-48.

[165] De Luca A, Harbach M, von Zezschwitz E, Maurer ME, Slawik BE, Hussmann H, et al. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In: Proceedings of the sigchi conference on human factors in computing systems; 2014. p. 2937-46.

[166] Harbach M, Von Zezschwitz E, Fichtner A, De Luca A, Smith M. {It's} a hard lock life: A field study of smartphone ({Un) Locking} behavior and risk perception. In: 10th symposium on usable privacy and security (SOUPS 2014); 2014. p. 213-30.

[167] Schaub F, Balebako R, Durity AL, Cranor LF. A design space for effective privacy notices. In: Eleventh symposium on usable privacy and security (SOUPS 2015); 2015. p. 1-17.

[168] Egelman S, Jain S, Portnoff RS, Liao K, Consolvo S, Wagner D. Are you ready to lock? In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security; 2014. p. 750-61.

[169] Sluganovic I, Roeschlin M, Rasmussen KB, Martinovic I. Analysis of reflexive eye movements for fast replay-resistant biometric authentication. ACM Transactions on Privacy and Security (TOPS). 2018;22(1):1-30.

[170] Rigas I, Komogortsev O, Shadmehr R. Biometric recognition via eye movements: Saccadic vigor and acceleration cues. ACM Transactions on Applied Perception (TAP). 2016;13(2):1-21.

[171] Bulling A, Roggen D. Recognition of visual memory recall processes using eye movement analysis. In: Proceedings of the 13th international conference on Ubiquitous computing; 2011. p. 455-64.

[172] Nyström M, Hooge IT, Hessels RS, Andersson R, Hansen DW, Johansson R, et al. The fundamentals of eye tracking part 3: How to choose an eye tracker. Behavior Research Methods. 2025;57(2):67.

[173] Niehorster DC, Nyström M, Hessels RS, Andersson R, Benjamins JS, Hansen DW, et al. The fundamentals of eye tracking part 4: Tools for conducting an eye tracking study. Behavior Research Methods. 2025;57(1):46.

[174] Santini T, Fuhl W, Kasneci E. Calibme: Fast and unsupervised eye tracker calibration for gaze-based pervasive human-computer interaction. In: Proceedings of the 2017 chi conference on human factors in computing systems; 2017. p. 2594-605.

[175] Drewes H, Schmidt A. Interacting with the computer using gaze gestures. In: Ifip conference on human-computer interaction. Springer; 2007. p. 475-88.

[176] Porta M, Turina M. Eye-S: a full-screen input modality for pure eye-based communication. In: Proceedings of the 2008 symposium on Eye tracking research & applications; 2008. p. 27-34.

[177] Sibert LE, Jacob RJ. Evaluation of eye gaze interaction. In: Proceedings of the SIGCHI conference on Human Factors in Computing Systems; 2000. p. 281-8.

[178] Motlicek P, Duffner S, Korchagin D, Bourlard H, Scheffler C, Odobez JM, et al. Real-Time Audio-Visual Analysis for Multiperson Videoconferencing. Advances in Multimedia. 2013;2013(1):175745.

[179] Duchowski AT. A breadth-first survey of eye-tracking applications. Behavior Research Methods, Instruments, & Computers. 2002;34(4):455-70.

[180] Radach R, Hyona J, Deubel H. The mind's eye: Cognitive and applied aspects of eye movement research. Elsevier; 2003.

[181] Majaranta P, Räihä KJ. Twenty years of eye typing: systems and design issues. In: Proceedings of the 2002 symposium on Eye tracking research & applications; 2002. p. 15-22.

[182] Poole A, Ball LJ. Eye tracking in HCI and usability research. In: Encyclopedia of human computer interaction. IGI Global Scientific Publishing; 2006. p. 211-9.

[183] Jacob RJ, Karn KS. Eye tracking in human-computer interaction and usability research: Ready to deliver the promises. In: The mind's eye. Elsevier; 2003. p. 573-605.

[184] Chamberlain L. Eye tracking methodology; theory and practice. Qualitative Market Research: An International Journal. 2007;10(2):217-20.

[185] Kaur P, Kumar N, Singh M. Biometric cryptosystems: a comprehensive survey. Multimedia Tools and Applications. 2023;82(11):16635-90.

[186] Kang J. Mobile payment in Fintech environment: trends, security challenges, and services. Human-centric Computing and Information sciences. 2018;8(1):32.

[187] Das AK, Sharma P, Chatterjee S, Sing JK. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Journal of Network and Computer Applications. 2012;35(5):1646-56.

[188] Amin R, Islam SH, Biswas G, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems. 2018;80:483-95.

[189] Khamis M, Trotter L, Mäkelä V, Zezschwitz Ev, Le J, Bulling A, et al. Cueauth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2018;2(4):1-22.

[190] De Luca A, Weiss R, Hussmann H, An X. Eyepass-eye-stroke authentication for public terminals. In: CHI'08 Extended Abstracts on Human Factors in Computing Systems; 2008. p. 3003-8.

[191] Schneegass S, Steimle F, Bulling A, Alt F, Schmidt A. Smudgesafe: Geometric image transformations for smudge-resistant user authentication. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing; 2014. p. 775-86.

[192] Frank M, Biedert R, Ma E, Martinovic I, Song D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE transactions on information forensics and security. 2012;8(1):136-48.

[193] Sae-Bae N, Ahmed K, Isbister K, Memon N. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In: proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2012. p. 977-86.

[194] Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In: 4th USENIX workshop on offensive technologies (WOOT 10); 2010. .

[195] Conti M, Zachia-Zlatea I, Crispo B. Mind how you answer me! Transparently authenticating the user of a smartphone when answering or placing a call. In: Proceedings of the 6th ACM symposium on information, computer and communications security; 2011. p. 249-59.

[196] Azuma RT. A survey of augmented reality. Presence: teleoperators & virtual environments. 1997;6(4):355-85.

[197] LiKamWa R, Liu Y, Lane ND, Zhong L. Moodscope: Building a mood sensor from smartphone usage patterns. In: Proceeding of the 11th annual international conference on Mobile systems, applications, and services; 2013. p. 389-402.

[198] Pering T, Agarwal Y, Gupta R, Want R. Coolspots: reducing the power consumption of wireless mobile devices with multiple radio interfaces. In: Proceedings of the 4th international conference on Mobile systems, applications and services; 2006. p. 220-32.

[199] Pantelopoulos A, Bourbakis NG. A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2009;40(1):1-12.

[200] Mbouna RO, Kong SG, Chun MG. Visual analysis of eye state and head pose for driver alertness monitoring. IEEE transactions on intelligent transportation systems. 2013;14(3):1462-9.

[201] Jo J, Lee SJ, Park KR, Kim IJ, Kim J. Detecting driver drowsiness using feature-level fusion and user-specific classification. Expert Systems with Applications. 2014;41(4):1139-52.

[202] Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, et al. Comprehensive experimental analyses of automotive attack surfaces. In: 20th USENIX security symposium (USENIX Security 11); 2011. .

[203] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, et al. Experimental security analysis of a modern automobile. In: 2010 IEEE symposium on security and privacy. IEEE; 2010. p. 447-62.

[204] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle. Black Hat USA. 2015;2015(S 91):1-91.

[205] Jha S, Busso C. Probabilistic estimation of the gaze region of the driver using dense classification. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC). IEEE; 2018. p. 697-702.

[206] Sahayadhas A, Sundaraj K, Murugappan M. Detecting driver drowsiness based on sensors: a review. Sensors. 2012;12(12):16937-53.

[207] Vural E, Cetin M, Ercil A, Littlewort G, Bartlett M, Movellan J. Drowsy driver detection through facial movement analysis. In: international workshop on human-computer interaction. Springer; 2007. p. 6-18.

[208] Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks. 2017;2017(1):6562953.

[209] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer networks. 2015;76:146-64.

[210] Weber RH. Internet of Things–New security and privacy challenges. Computer law & security review. 2010;26(1):23-30.

[211] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE; 2017. p. 618-23.

[212] Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010;54(15):2787-805.

[213] Cook DJ, Das SK. How smart are our environments? An updated look at the state of the art. Pervasive and mobile computing. 2007;3(2):53-73.

[214] Yarbus AL. Eye movements and vision. Springer; 2013.

[215] Just MA, Carpenter PA. A theory of reading: from eye fixations to comprehension. Psychological review. 1980;87(4):329.

[216] Tan M, Le Q. Efficientnet: Rethinking model scaling for convolutional neural networks. In: International conference on machine learning. PMLR; 2019. p. 6105-14.

[217] Blignaut P. Fixation identification: The optimum threshold for a dispersion algorithm. Attention, Perception, & Psychophysics. 2009;71(4):881-95.

[218] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials. 2015;17(4):2347-76.

[219] Fong T, Nourbakhsh I, Dautenhahn K. A survey of socially interactive robots. Robotics and autonomous systems. 2003;42(3-4):143-66.

[220] Evans NW, Kinnunen T, Yamagishi J. Spoofing and countermeasures for automatic speaker verification. In: INTERSPEECH 2013, 14th Annual Conference of the International Speech Communication Association; 2013. .

[221] Adadi A, Berrada M. Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). IEEE access. 2018;6:52138-60.

[222] Gao J, Li P, Chen Z, Zhang J. A survey on deep learning for multimodal data fusion. Neural computation. 2020;32(5):829-64.