Multi-dimensional Identity Construction and Continuous Authentication Methods: A Survey

Talha Hussain Hashmi[1,2], Guiyuan Tang[1,2], Xiaowei Liu[1,2], and Zhiwei Zhang[1,2,*]
[1]School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, 710071, China
[2]Shaanxi key Laboratory of Network and System Security, Xidian University, Xi'an, Shaanxi, 710071, China
[*]Corresponding author

In the rapidly evolving digital era, where interconnected devices like smartphones proliferate, sensitive data exchange has surged, amplifying cybersecurity risks. Therefore, a need for robust authentication to safeguard privacy and prevent unauthorized access, driving innovative solutions that enhance digital security. This survey paper focuses on the critical need for advanced authentication methods to address escalating cyber threats and the shortcomings of traditional single-factor authentication. Conventional methods, reliant on passwords or tokens, are highly susceptible to breaches and user negligence, leaving significant security vulnerabilities. This study bridges these gaps through an in-depth exploration of Continuous Authentication (CA) techniques, which utilize real-time monitoring of user behavior and biometric data to enhance security and usability. A comprehensive analysis of multi-dimensional identity factors (physiological, behavioral, and context-aware) highlights how their integration can improve reliability while respecting privacy. The study provides insights into balancing security, usability, and privacy, guiding the development of modern, user-centric authentication frameworks.

Index Terms—**Continuous authentication, Biometric data, Single-factor authentication, Traditional methods, Privacy.**

I. Introduction

DIGITAL technologies are advancing rapidly, leading to widespread adoption of interconnected systems such as smartphones [1], smart homes [2], and the Internet of Things (IoT) [3]; this proliferation of connected devices has heightened the volume and sensitivity of personal data exchanged, creating critical security vulnerabilities. Strong and efficient identity verification mechanisms are essential to protect users and ensure a smooth experience. Authentication serves as the cornerstone of digital security, ensuring only legitimate users can access protected resources while safeguarding personal information [4]. It plays a key role in safeguarding personal information and resources. As cyber threats increase in frequency and complexity, the need for multifactor authentication has grown [5]. Traditional authentication systems often use single-factor authentication (SFA). SFA usually involves something the user knows, like a password or PIN. But, SFA is inadequate against cyber-attacks. Weak passwords are easily cracked. Users often reuse credentials across platforms, increasing breach risks [6], [7]. Therefore, the focus has moved to multi-factor authentication (MFA). MFA enhances security by combining knowledge-based (passwords), possession-based (mobile devices, smartcards), and biometric factors (fingerprints, face recognition, iris scans) [8], [9]. MFA improves login-time assurance through the combination of more than one distinct factor type, commonly categorized as something the user knows, something the user has, and something the user is. MFA therefore strengthens entry-point decisions, yet it does not, on its own, ensure that the authenticated user remains the same entity throughout the session [10]. Multi-dimensional identity construction is conceptually separate from MFA. MFA typically establishes initial trust at login, while multi-dimensional identity construction supplies the evidence used to strengthen MFA implementations (e.g., multi-biometric "something you are" combined with possession), and it also supplies the continuous signals used for CA to maintain trust after login [11].

Continuous authentication (CA) addresses the limitations of traditional authentication. Unlike session-based authentication, where users authenticate once for a session, CA continuously monitors user behaviors and biometrics in real-time, verifies identity throughout the session [12], [13]. It passively analyzes factors like keystroke dynamics, facial expressions, voice, and how users interact with their devices. CA systems enhance both security and usability without requiring user input after the initial authentication [14]. Integrating CA with multi-dimensional identity construction enables more accurate user assessment by leveraging personal data, including physiological, behavioral, and contextual information. This comprehensive approach strengthens authentication and reduces unauthorized access risks, but also creates challenges balancing security and privacy concerns.

The development of authentication methods mirrors the increasing complexity of cyber threats. Initially reliant on inherently vulnerable passwords, over 80% of data breaches involve compromised credentials [15], highlighting the urgent need for more secure approaches. MFA significantly lowers unauthorized access risk by combining verification factors [20]. However, introduces challenges like user inconvenience and system complexity [21], [22]. To address these issues, biometric authentication has gained traction due to its convenience and difficulty in forging. Fingerprint and facial recognition are now standard in many devices, offering higher security compared to traditional password systems [23], [24]. However, biometric data is highly sensitive and, if compromised, cannot be changed like a password, raising significant privacy concerns and necessitating robust protection

Manuscript received October 3, 2025; revised December 29, 2025. Corresponding author: Zhang Zhiwei (email: zwzang@xidian.edu.cn)

[25], [27]. Additionally, biometric systems can experience false acceptance and rejection rates, which may impact user trust and system reliability [28].

CA enhances security and user convenience by continuously monitoring user behaviors and biometrics in real-time [30], [31]. This model employs biometric, behavioral, and contextual information for verification, making it difficult for unauthorized access to go undetected. Modern studies integrate advanced algorithms to process complex datasets, improving the accuracy and reliability of CA systems [30], [32]. However, challenges include safeguarding the security and privacy of the continuously collected personal information [35]. High accuracy in a range of real-life environments is also critical, with variations in behavior and environments having an impact on system performance [36], [38]. User acceptance is critical for successful CA system implementations, requiring trust in responsible information processing and minimal authentication intrusion [39], [40]. Overcoming obstacles requires robust encryption, regulatory compliance (e.g., GDPR [41]), and user-friendly, secure interfaces that maintain usability. Thus, CA offers a secure, effective, user-focused solution for digital environments.

Multi-Factor Authentication (MFA) should be introduced as the entry-point control that verifies identity at login using two or more factors, since it strengthens access decisions through multiple independent proofs of identity rather than a single credential. MFA can also be expressed as an authentication strategy that “considers more than one significant attribute” for identifying a user, which highlights the design intent of reducing single-point failure at login [42]. Continuous Authentication (CA) should be defined as in-session identity assurance that keeps checking whether the active user remains the legitimate account holder, instead of assuming the user stays legitimate after the first login [43]. The relationship between the two needs to be explicit and repeated throughout the paper: MFA establishes initial trust, while CA maintains trust after access is granted, reducing the post-login exposure window that MFA alone cannot cover [42,43]. Recent empirical results support the practical value of this framing, since sliding-window, multimodal CA has been reported to achieve 99.3% verification accuracy, detect impostors within 12 seconds, and keep false alarms under 1%, which makes CA suitable as a runtime companion to MFA rather than a purely theoretical add-on [43]. This relationship is also timely for deployments, because a 2025 systematic review of payment-system MFA found that 33% of industry tools still rely on OTP-based MFA, even as research pushes toward richer biometrics and behavioral signals, which strengthens the case for CA as the continuity layer that complements legacy MFA instead of replacing it [44].

CA enhances real-time security but is constrained by a trade-off between security, usability, and privacy. CA solutions’ constant monitoring of behavioral and biometric signals raises user concerns over surveillance and data misuse. Furthermore, CA systems require accurate data, as errors (false positives or negatives) undermine trustworthiness [45]. Integrating multi-factor authentication (biometrics, behavior monitoring, context-aware factors) introduces challenges in technical compatibility, complexity, and data breach risks. As digital connectivity expands, need for secure, user-friendly authentication grows, necessitating multi-layered solutions beyond traditional methods. CA is promising, yet research lacks clarity on balancing its core triad: security, usability, and privacy. Progress has been made, but studies focus on isolated factors like biometrics or behavior, with some exploring integrated frameworks. Privacy concerns and ethical issues in continuous monitoring remain underexplored. This survey addresses these gaps, examining how multi-dimensional identity construction integrates with CA. It identifies best practices for balancing security, usability, and privacy. The goal is to advance development of secure, user-centric systems that meet demands. Key research questions include:

• How can multi-dimensional identity factors be seamlessly integrated into CA frameworks to enhance security without compromising user experience?

• Which combination of biometric, behavioral, and contextual data provides the most reliable and secure authentication in diverse digital environments?

This survey paper emphasizes the demand for authentication methods to address cyber threats and the limitations of traditional single-factor authentication. Passwords and tokens are vulnerable to breaches and human error, creating security gaps. The paper investigates CA techniques that leverage real-time monitoring of user behavior and biometrics to enhance security and usability. It explores the integration of multi-dimensional identity factors (physiological, behavioral, and contextual) for improved reliability and privacy. The survey is structured to cover foundational concepts, authentication techniques, security and privacy implications, usability challenges, privacy-preserving methodologies, and future directions, concluding with recommendations for secure, user-centric systems.

A. Motivation of the Study

Existing literature lacks a comprehensive analysis comparing traditional and continuous authentication CA models and algorithms, which is the primary motivation for this study. Our research provides a vital resource for understanding these methods, assisting researchers in selecting superior CA techniques and developing models for smart devices.

1) Contributions

• It revisits the foundations of traditional authentication (e.g., passwords, PINs, static biometrics) and explains their diminishing efficacy compared to modern solutions. • It catalogues and evaluates the full spectrum of CA frameworks, grouping them by the behavioral or physiological dynamics they track to confirm a user’s identity over time. • We compare competing CA approaches to lay out the pros and cons. For every study reviewed we note the authentication strategy adopted, the sensors employed, the datasets analyzed, the neural-network or statistical models trained, and the reported performance figures. • Finally, we discuss the insights gained, the persistent challenges, and directions for future work.

TABLE I: A horizontal comparison clarifies the contribution of the present survey by situating it against closely related reviews that focus either on continuous authentication (CA) or on multi-factor authentication (MFA) in isolation

Primary scope	Evidence	What it emphasizes	Aspects	Present survey	Ref.
Continuous Authentication Systems (CAS) and user profiling	-	Reports that supervised learning dominates CAS, with frequent use of score-level fusion; evaluation attention centers on FRR/FAR/EER, while usability, security, and scalability are less consistently addressed	Limited treatment of CA as an operational companion to MFA	The present survey explicitly structures CA through physiological, behavioral, and context-aware identity dimensions and discusses trade-offs and integration constraints as first-order issues	[46]
Behavioral biometrics on mobile devices (authentication + demographic detection)	122 studies included from 14,179 screened	Concentration of evidence in touch gestures (n=76) and movement (n=63); keystroke (n=30); reports low mean reporting quality (5.5/14)	Narrower modality scope (behavioral, mobile-heavy); limited system-level framing beyond study quality	The present survey extends beyond mobile behavioral signals to include broader identity construction and context-aware factors, aligned with its multi-dimensional taxonomy	[47]
MFA in digital payment systems with NIST alignment	70 academic papers (2017–2024) + 13 industry tools	Quantifies implementation gaps: 33% of industry tools still rely on OTP-based MFA; 60% of reviewed papers integrate biometrics; payment systems show 77% alignment with NIST standards	CA and post-login identity assurance are largely outside scope	The present survey addresses the post-login gap by framing CA as continuous session assurance and discusses privacy/usability trade-offs that shape deployability	[44]
Continuous biometric authentication taxonomy with emphasis on sampling (2018–2024)	80 papers	Proposes a classification framework focused on data sampling strategies and supports metric-level comparison across continuous biometrics	Less emphasis on context-aware identity and broader CA–MFA system architecture	The present survey's distinct angle is the "multi-dimensional identity construction" framing that includes contextual and behavioral layers alongside biometrics	[48]

II. WIDELY DEPLOYED AUTHENTICATION METHODS

Traditional authentication methods rely on single-factor and multi-factor approaches to verify user identities. Password protection remains a common method, utilizing passphrases or PINs as a knowledge-based factor [49], [50]. Widely implemented and easy to use, passwords are vulnerable to weaknesses such as easily guessed, reused across platforms, or susceptible to phishing attacks, leading to a significant number of data breaches [51], [52]. Token-based authentication introduces a possession factor, where users present a physical device such as smartcards or smartphones [53], [54]. Although tokens add an extra layer of security, they come with challenges such as the potential for loss or theft and the complexity of managing additional hardware [55], [56]. Biometric authentication methods, including voice recognition and facial recognition, have gained popularity due to their convenience and difficulty to forge [22], [57]. Voice biometrics leverage built-in microphones in devices to authenticate users based on unique vocal characteristics, but advancements in technology raise concerns about voice mimicry and spoofing [52], [58]. Facial recognition systems have evolved from simple image analysis to more sophisticated techniques that assess three-dimensional features and user expressions, enhancing security but also introducing privacy issues and the risk of being bypassed with photos or masks [59], [60]. Ocular methodologies such as iris and retina scanning offer high accuracy and are challenging to replicate; they require specialized, high-quality hardware and robust image analysis techniques, making them costly and less accessible [61], [62]. Other methods include hand geometry and vein recognition, which analyze the physical shape and vein patterns of a user's hand for authentication [63], [64]. While these methods provide a non-intrusive means of verification, they face limitations related to environmental robustness and susceptibility to advanced spoofing attacks [65]. Fingerprint scanners are extensively used in personal devices for their intuitive nature, but they are prone to being replicated from surfaces and raise significant privacy concerns [66]. Thermal image recognition and geographical location-based authentication add contextual layers to security by analyzing unique thermal patterns and validating access based on the user's location. However, these methods are influenced by user conditions and environmental factors, which can affect their reliability and accuracy [19], [67], [68]. Traditional authentication methods offer varying levels of security and convenience; each comes with its own set of advantages and limitations. The continuous evolution of cyber threats necessitates the integration of more sophisticated and multi-dimensional authentication mechanisms to enhance security without compromising user experience [69], [70]. Today, identification and authentication for accessing sensitive data are among the primary use cases for MFA.

III. MODES OF CONTINUOUS AUTHENTICATION

Continuous authentication is not only a change in when identity is checked, it also changes what can go wrong during checking. Each modality discussed in this section is therefore analyzed through five deployment-critical dimensions: (i) signal stability over time (behavioral drift), (ii) sensor availability and context dependence, (iii) adversarial exposure (iv) privacy risk, and (v) resource cost (latency, energy, and on-device feasibility). This structure enables the survey to derive

TABLE II: WIDELY DEPLOYED AUTHENTICATION METHODS

Method	Advantages	Drawbacks	Level	Usability	Ref.
Password Protection	Simple, common	Low Entropy, Forgotten codes	Low	High	[49], [50], [51], [52]
Token Presence	Hard to copy	Token Loss, Added overhead	Medium	Moderate	[53], [54], [55], [56]
Voice Biometrics	Easy, non-intrusive	Privacy risks, Health dependency	Medium	High	[54], [58]
Facial Recognition	Secure, touchless	Privacy risks, Environmental Sensitivity	High	High	[59], [60]
Ocular-Based	Accurate, secure	Costly, User Intrusiveness	High	Moderate	[61], [62]
Hand Geometry	Simple, non-intrusive	Less secure, Placement Sensitivity	Medium	High	[63], [64], [65]
Vein Recognition	Hard to replicate	Costly scanners, Data vulnerability	High	Moderate	[63], [64]
Fingerprint Scanner	Common, easy	Spoofable, Acquisition Quality	Medium	High	[66]
Thermal Recognition	Unique, touchless	Environment Sensitive, Accuracy Variability	Medium	Low	[19], [67], [68]
Geo-Location	Context-based	Unreliable GPS, Spoofing prone	Low	High	[19], [67], [68]

challenges from method properties. Recent research offers various definitions for CA. Traore [72] defines CA as ”a new generation of security mechanisms that continuously monitor user behavior and use this as a basis to re-authenticate them periodically”. Similarly, Ibanez-Lissen et al. [73] describe CA as ”a security mechanism that monitors user actions at every point in time during a session and determines if that user is the legitimate one”. These definitions, however, have limitations. Traore definition primarily focuses on behavioral biometrics, overlooking other authentication factors, while Ibanez-Lissen definition does not specify whether the authentication process is active or passive. Additional studies emphasize the need for a more comprehensive definition that includes multiple authentication dimensions. Stylios and Aegean [74] argue that CA should integrate physiological and behavioral biometrics alongside context-aware authentication modes to establish a robust security framework. Furthermore, Hasan et al. [75] highlight the importance of passive monitoring in CA systems to enhance user experience and reduce disruptions. Building on these insights, we suggest defining CA as the continuous and passive monitoring of users through the recognition of physiological biometrics, behavioral biometrics, and context-aware authentication modes during a session. This comprehensive definition addresses the multifaceted nature of modern authentication systems, ensuring that CA integrates a broad range of user features and actions to enhance both security and user convenience. We suggest CA as continuously and passively monitoring users by means of recognizing user features and actions (i.e., physiological biometrics, behavioral biometrics, or context-aware authentication modes). Section 3 reviews authentication methods through the lens that MFA governs entry-point assurance, whereas multi-dimensional identity construction provides the signals that can strengthen MFA and enable CA for post-login assurance. Figure 1 shows a multimodal biometric framework integrating behavioral (voice, hand geometry) and physiological (facial, vein, fingerprint) features.

A. Physiological Biometrics

Physiological biometrics (fingerprint recognition, face recognition, and iris recognition) are among the well-known and most used traditional authentication modes. These modes are also utilized for continuous authentication. Figure 1 presents a continuous authentication (CA) architecture that constructs identity using two complementary signal families. Behavioral modalities (e.g., voice recognition, hand geometry) support ongoing user verification during interaction, capturing dynamic patterns that can be sampled repeatedly over time While physiological modalities (e.g., Face, vein, fingerprint, thermal) primarily support user enrollment and high-confidence verification, providing more stable biological signatures for template creation. Raw signals are transformed through feature extraction, then processed by an authentication algorithm that performs matching and decision-making against the enrolled profile. The system outputs user validation decisions, while selected/fused features enable multimodal fusion and are stored as an enrollment profile in cloud or local repositories for subsequent continuous checks

1) Face and Voice as Biometrics

Continuous authentication methods using face and voice biometrics have emerged as critical solutions for enhancing security in mobile and computing environments. Abolarinwa [76] proposed a face recognition-based authentication system for mobile devices. By employing a Support Vector Machine (SVM) classifier trained on facial images from 10 participants, they achieved a False Acceptance Rate (FAR) ranging from 0.1% to 1% with overall accuracy of 64%. Similarly, Lu et al. [77] developed a voice-based authentication method, evaluated with 18 users, achieving a recognition accuracy of 97% and

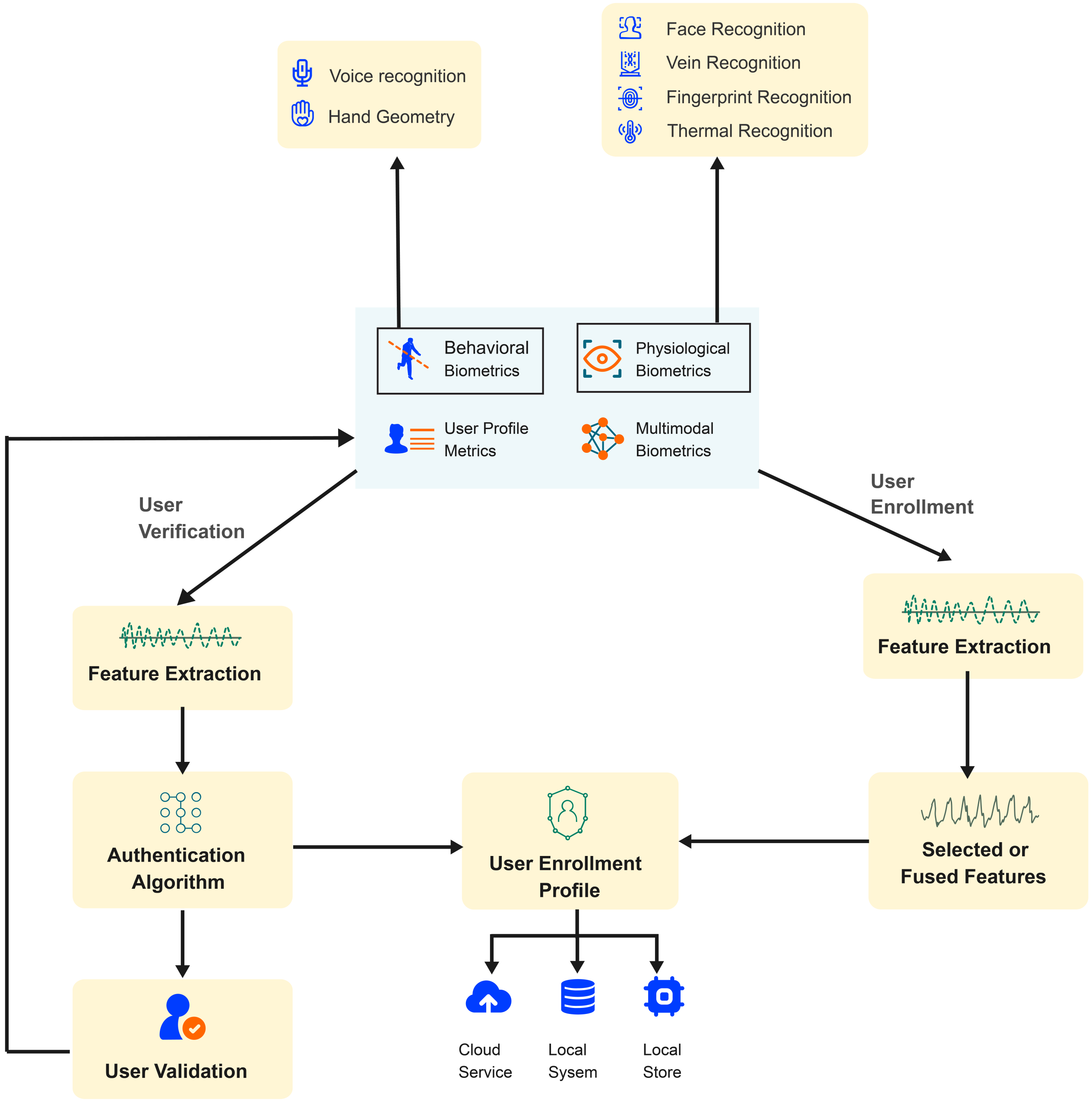

Fig. 1: Modes of continuous authentication.

a False Positive Rate (FPR) of 0.1%. Alharbi and Alshanbari [78] advanced this field by combining FaceNet for face recognition and Gaussian Mixture Model (GMM) for voice recognition in a multimodal biometric system, demonstrating a notable reduction in Equal Error Rate (EER) compared to unimodal methods. Abbaas and Serpen [79] employed an ensemble classifier integrating face and voice biometrics, reporting accuracy, precision, True Negative Rate (TNR), and True Positive Rate (TPR), all exceeding 99%, while maintaining FPR and False Negative Rate (FNR) below 1%. Stokkenes et al. [80] facilitated the development of multimodal biometric systems by creating a dataset that includes face, voice, and periocular data from 150 participants. This dataset has proven instrumental in testing and optimizing multimodal biometric methods. Abuhamad et al. [42] conducted an extensive survey of over 140 studies on behavioral biometrics, which included several voice-based and multimodal approaches integrating face and voice recognition, emphasizing the superior performance of such systems. Fereidooni et al. [81] introduced AuthentiSense using few-shot learning with face/voice integration, achieving 97% F1-score for mobile platforms. Other notable contributions include the work by Alshardan et al.

TABLE III: Continuous authentication methods using face and voice biometrics

Type	Method	Algorithm	Participants	Advantages	Drawbacks	Performance	Ref
Face	Face recognition (mobile)	SVM	10	Simple, common	Spoofable, quality-dependent	FAR: 0.1–1%, TAR: 73%, Acc: 64%	[76]
Voice	Voice authentication	-	18	Easy, non-intrusive	Mimicry risk, privacy	Acc: 97%, FPR: 0.1%	[77]
Multimodal	FaceNet + GMM (face & voice)	FaceNet + GMM	-	High security	Complex integration	Lower EER	[78]
Multimodal	Face & voice ensemble	Ensemble	-	High performance	Needs classifiers	Acc, Prec, TNR, TPR >99%; FPR, FNR <1%	[79]
Multimodal	Face, voice, periocular data	-	150	Supports research	-	Dataset for testing	[80]
Survey	Behavioral biometrics review	-	140+ studies	Comprehensive	-	Highlights multimodal edge	[42]
Multimodal	AuthentiSense (face & voice)	Few-Shot	-	Few-shot effective	Needs data	F1: 97% (mobile)	[81]
Multimodal	Deep learning multimodal	Deep Learning	-	Strong integration	High cost	Acc: 96.8%, Low EER	[82]

[82], who proposed a deep learning-based multimodal authentication framework combining face and voice biometrics, reporting an overall accuracy of 96.8% and a reduced EER compared to individual modalities. Additionally, Zhang et al. [83] investigated the role of facial expressions and voice variations in CA systems, achieving a True Accept Rate (TAR) of 92% with a FAR of 0.8%. Yadav et al. [84] explored a hybrid approach using Convolutional Neural Network (CNNs) for face recognition and Recurrent Neural Network (RNNs) for voice authentication achieving a combined accuracy of 98.2%. Thomas and Preetha Mathew [85] developed a face and voice authentication system under varying lighting and noise conditions, achieving performance with an EER below 2%. These studies collectively demonstrate the efficacy and potential of integrating face and voice biometrics for CA, highlighting advancements in recognition accuracy and multimodal integration by synthesizing findings from diverse methodologies, this research underscores the critical role of face and voice biometrics in securing digital environments. Face- and voice-based continuous authentication usually performs well in controlled capture, yet its main challenges come from capture variability and presentation risk. Illumination, pose, and ambient noise degrade the stability of similarity scores, which forces systems to either widen decision thresholds (raising false accepts) or increase sampling (down user experience). Continuous use also increases the exposure window for replay and presentation attacks, so liveness and presentation attack detection become a practical requirement rather than an optional add-on. Recent biometric PAD literature stresses that spoof resistance must be treated as a measurable performance axis, not a qualitative claim, because operational error rates can shift once attacks are considered.

2) Gait Recognition

The gait recognition has experienced significant advancements in recent years. Figure 2 Illustrates a unified view of gait recognition using multiple or single cameras. Highlights 3D (skeleton-based, cross-view) and 2D (model based, appearance-based) methods for capturing and analyzing human walking patterns. Han and Bhanu [86] employed model-based gait recognition techniques that used body segment dynamics to extract unique gait patterns, achieving an accuracy of 92% on the USF Gait Dataset. Similarly, Shiraga et al. [87] proposed a CNN-based approach for cross-view recognition using OU-ISIR dataset, achieving 95.4% TAR with 3.1% FAR. This approach outperformed earlier handcrafted feature methods by leveraging deep feature representation. Wu et al. [88] introduced a spatiotemporal gait representation method that encoded motion dynamics in a compact form, achieving an accuracy of 94.8% on the CASIA-B dataset under normal walking conditions. Zhang et al. [89] extended this work by incorporating generative adversarial networks (GANs) to enhance cross-view gait recognition, reporting TAR values exceeding 96% on multiple benchmark datasets. While earlier studies focused on silhouette-based methods [90], recent advancements have shifted towards skeleton-based approaches, as demonstrated by Qin et al. [91], who achieved a FAR of only 2.5% using 3D pose estimation techniques integrated with graph convolutional networks. Another notable contribution was made by Chao et al. [92], who developed a (GEI)-based deep learning model that achieved state-of-the-art performance with 97.3% accuracy on the OU-MVLP dataset. The model reduced computational complexity while maintaining high accuracy, showcasing GEI's potential in feature extraction. Furthermore, Huang et al. [93] explored domain adaptation techniques, achieving 93% TAR on cross-domain datasets by minimizing domain discrepancies through adversarial training. In contrast, Cheng et al. [94] investigated the role of temporal attention mechanisms, achieving a TAR of 94.5% on the CASIA-B dataset under occluded scenarios, which was previously a challenging condition for traditional models. The use of hybrid methods combining handcrafted and deep learning features has also shown promise. Gadaleta and Rossi [95] combined accelerometer- based data with CNNs, achieving an accuracy of 91% in real-world scenarios with varying walking surfaces. Similarly, Yousef et al. [96] proposed a hybrid deep learning model that integrates residual networks

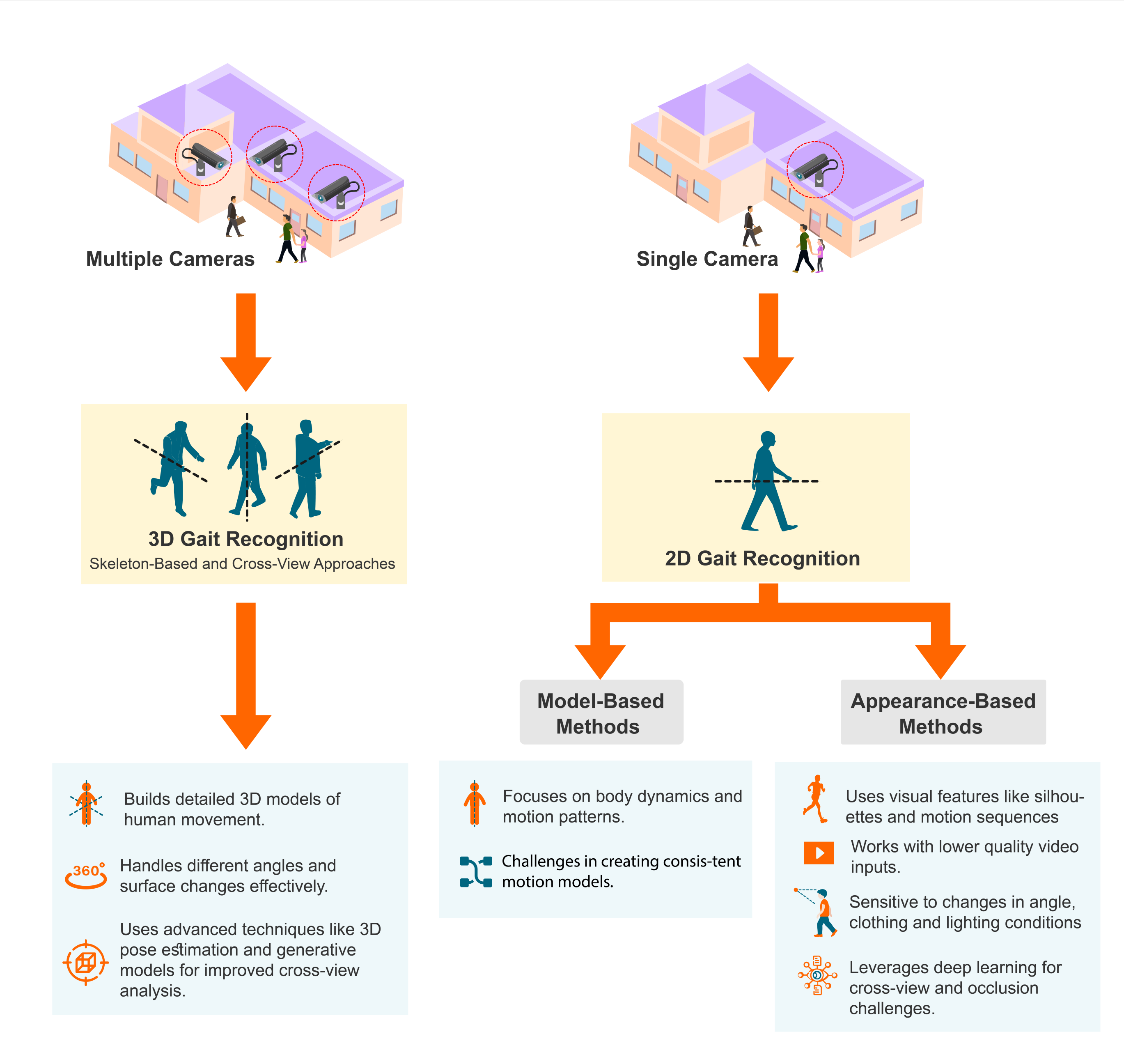
Multiple Cameras
Single Camera
3D Gait Recognition
Skeleton-Based and Cross-View Approaches
2D Gait Recognition
Model-Based Methods
Appearance-Based Methods
Builds detailed 3D models of human movement.
360°
Handles different angles and surface changes effectively.
Uses advanced techniques like 3D pose estimation and generative models for improved cross-view analysis.
Focuses on body dynamics and motion patterns.
Challenges in creating consis-tent motion models.
Uses visual features like silhou-ettes and motion sequences
Works with lower quality video inputs.
Sensitive to changes in angle, clothing and lighting conditions
Leverages deep learning for cross-view and occlusion challenges.

Fig. 2: Gait Recognition

and RNN, reporting a FAR of 1.8% and a TAR of 97% on the TUM Gait dataset. Such hybrid models effectively address the limitations of both traditional and deep learning approaches. Despite these advancements, challenges such as occlusion, varying walking speed, and cross-view recognition remain prevalent. To address these, Ghosh [97] employed transformer architectures, achieving state-of-the-art results with a TAR of 96.8% on the OU-ISIR dataset under varying speed conditions, while Wang et al. [98] used self-supervised learning against occlusions (94.2% accuracy on CASIA-B). Recent studies emphasize large-scale datasets, exemplified by Shen et al. [99] introducing a dataset with over 20,000 subjects, facilitating the development of more generalized gait recognition models. Gait is attractive for passive CA, but the derived challenges are tightly coupled to device placement and context switching. Pocket, hand-held, and bag placement produce different inertial signatures, which can resemble "intra-user variation" at the classifier level and inflate false rejections if the model is not placement-aware. Context changes create discontinuities that look like impostor segments, so robust systems need segment-quality gating and context-aware fusion rather than longer windows alone. Evidence from context-aware fusion research shows that adaptive weighting can materially reduce error, with multimodal schemes reporting accuracy gains when the system dynamically shifts weight based on signal reliability and configuration changes [49].

Motion dynamics, characterized by unique gait patterns have emerged as a reliable biometric modality for human

TABLE IV: Continuous authentication methods using gait recognition

Type	Method	Algorithm	Participants	Advantages	Drawbacks	Performance	Ref
Model-based	Body segment dynamics	Not specified	USF Gait Dataset	High accuracy	Needs precise modeling	Acc: 92%	[86]
CNN-based	Cross-view recognition	CNN	OU-ISIR Dataset	Effective, superior	High computation	TAR: 95.4%, FAR: 3.1%	[87]
Spatiotemporal	Motion encoding	Not specified	CASIA-B (Normal)	Compact, accurate	Struggles with abnormal gait	Acc: 94.8%	[88]
GANs-based	Cross-view with GANs	GANs	Multiple Datasets	Enhanced TAR	Complex training	TAR > 96%	[89]
Skeleton-based	3D poses with GCNs	GCNs	Not specified	Low FAR, 3D poses	Needs precise data	FAR: 2.5%	[91]
GEI-based	GEI deep learning	Deep Learning	OU-MVLP Dataset	High accuracy	Needs quality GEI	Acc: 97.3%	[92]
Domain Adapt.	Adversarial training	Adv. Training	Cross-Domain Datasets	Robust to shifts	Hyperparam. sensitive	TAR: 93%	[93]
Attention	Occlusion handling	Attention Mech.	CASIA-B (Occluded)	Works under occlusion	Needs complex model	TAR: 94.5%	[94]
Hybrid	CNN + accelerometer	CNN	Real-world Scenarios	High real-world accuracy	Needs sensors	Acc: 91%	[95]
Hybrid	ResNet + RNN	ResNet + RNN	TUM Gait Dataset	High TAR, low FAR	Complex, high computation	FAR: 1.8%, TAR: 97%	[96]

activity recognition. Gait-based techniques utilize data from body-worn motion sensors (e.g., gyroscopes, accelerometers) to extract and analyze movement patterns for authentication. Ray-Dowling [100] placed sensors on the waist of 36 participants, adopting Fast Fourier Transform (FFT) for feature extraction with 72–88% accuracy and 7% EER, noting performance depends on sensor placement. In a larger work, Gafurov [101] performed a study of gait-based recognition with sensors at a range of locations in the body. There were 100 subjects: 30 with sensors at ankles, 30 at arms, 100 at hips and 50 with mobiles in pockets. K-Nearest Neighbors (KNN) algorithm was adopted for classification, with EERs of 5%, 10%, 13%, and 7.3%, respectively, for sensors at ankles, at arms, at hips, and in pockets. These experiments reveal how the position of sensors can affect accuracy in recognition. Recent studies in gait-based recognition try to make such a system increasingly reliable and efficient under variable environments. Ellavarason et al. [102] developed a hybrid algorithm with Principal Component Analysis (PCA) and Support Vector Machines (SVMs) and achieved 90% accuracy with a custom made dataset of 60 subjects, Similarly Liu et al. [103] developed a deep learning algorithm with the use of convolutional neural networks (CNNs) for feature extraction in gait, with an EER of 4.2% with the OU-ISIR dataset. These experiments reveal how deep and machine learning can simplify and make gait recognition effective and efficient. To make performance even efficient, many studies have proposed fusing information between several sensors. Correspondingly, a pace variance compensating temporal attention mechanism with an EER of 3.8% using CASIA-B was proposed by Kumar and Verma [104].

3) *Iris Recognition*

Iris recognition has witnessed remarkable advancements via integration of machine learning, deep learning, and improved hardware for feature acquisition. Daugman [105] established the development of the iris recognition algorithm using a patented mathematical model that extracted iris patterns as phase information, achieving a FAR of 0.0001% and a TAR of 99.9% on the ICE dataset. Similarly, Wildes [106] proposed an automated system leveraging Laplacian pyramids for feature extraction, achieving 98% TAR with 0.01% FAR, establishing a foundation for subsequent iris biometric systems. More recently, Proença and Alexandre [107] and Hasan [108] addressed challenges of iris recognition under visible light. They developed a segmentation algorithm to accurately process degraded iris images, achieving 90.4% accuracy on the UBIRIS dataset. Yan et al. [109] extended this work, introducing a novel normalization technique to handle off-angle iris images, reporting 94.5% TAR on the CASIA-IrisV3 database. Omran and AlShemmary [110] adopted CNNs for iris feature extraction, achieving 98.8% accuracy and 0.003% FAR on IITD datasets. To improve cross-sensor performance, Kerrigan et al. [111] adopted one-to-one sensor mapping for domain adaptation via GANs, reducing cross-sensor performance degradation and achieving 96% TAR on ND IRIS-0405 datasets. Ahmad and Fuller [112] adopted lightweight deep neural networks for smartphone iris recognition, achieving 91.2% accuracy and 93% TAR on real time smartphone-captured datasets. To address occlusion, Yin et al. [113] developed a multi-task feature extraction and segmentation scheme, achieving 97.6% TAR on CASIA-Iris Thousand datasets. Nguyen et al. [114] developed a deep model with spatial attention, achieving 98.3% TAR and negligible 0.002% FAR on MICHE-I datasets. In contrast, Liang et al. [115] used near-infrared imaging for contactless iris recognition, achieving 99.1% accuracy on IIIT-contactless datasets and robustness in variable lighting. With access to larger datasets, work in this direction continued to become even more cultured, with iris recognition technology being developed and sharpened.

TABLE V: Continuous authentication methods using iris recognition

Type	Method	Algorithm	Participants	Advantages	Drawbacks	Performance	Ref
Model-Based	Phase-based iris recognition	Patented Model	ICE Dataset	Low FAR, high TAR	Needs precision	FAR: 0.0001%, TAR: 99.9%	[105]
Handcrafted	Laplacian pyramids feature extraction	Laplacian Pyramids	Not specified	Reliable method	Limited adaptability	TAR: 98%, FAR: 0.01%	[106]
Segmentation	Processing degraded iris images	Not specified	UBIRIS Dataset	Works on degraded	Poor image struggles	Acc: 90.4%	[107], [108]
Normalization	Off-angle iris correction	Novel Techniques	CASIA-IrisV3	Handles angles	Computationally heavy	TAR: 94.5%	[109]
Deep Learning	CNN-based feature extraction	CNNs	IITD Dataset	High accuracy	Needs large data	Acc: 98.8%, FAR: 0.003%	[110]
Domain Adaptation	Cross-sensor iris with GANs	GANs	ND-IRIS-0405	Works across sensors	Complex training	TAR: 96%	[111]
Lightweight DL	Mobile iris recognition	Not specified	Mobile Datasets	Mobile-friendly	Hardware limits	Acc: 91.2%, TAR: 93%	[112]
Multi-Task	Joint segmentation & extraction	Multi-Task Learning	CASIA-Thousand	Robust, high TAR	Complex model	TAR: 97.6%	[113]
Attention	Spatial attention iris recognition	Attention Mech.	MICHE-I Dataset	High TAR, low FAR	High computation	TAR: 98.3%, FAR: 0.002%	[114]
Contactless	NIR-based iris recognition	Not specified	IIIT-Contactless	High accuracy	Needs NIR hardware	Acc: 99.1%	[115]

4) ECG and EEG Features as Biometrics

The use of electroencephalography (EEG) and electrocardiography (ECG) for biometric authentication is an emerging issue due to their anti-spoofing and uniqueness capabilities. EEG monitors brain activity, and ECG monitors heart activity. Since these physiological traits cannot simply be impersonated, they work effectively for continuous authentication. Marcel and Millán [116] designed an EEG based system for use in authentication, comparing brain waves for beta and alpha, and reached 91% accuracy for a custom corpus. Similarly, Hosseinzadeh et al. [117] used ECG for authentication with a correlation-based matcher, reaching an EER of 2.5% for the PhysioNet corpus. As noted, both EEG and ECG can work individually as single biometric modalities. Others experimented with combining EEG and ECG for enhanced security in terms of use in verification. Riera et al. [118] used EEG spectral features and ECG time domain features and attained a 95.3% TAR and a 3.2% FAR for a corpus of 50 subjects. Kaliappan et al. [119] utilized deep feature fusion and attained an EER of 1.8% for use with the AMIGOS corpus. As can be seen, combining modalities boosts accuracy. The latest work used larger datasets and machine learning algorithms. Zhang et al. [120] utilized CNNs for EEG/ECG feature extraction, attaining 96.5% accuracy for the DEAP corpus. Similarly, Arnau-González et al. [121] have utilized RNNs for the analysis of temporal features and attained a TAR of 97% and a FAR of 2% for use with the DREAMER corpus. Such works show deep learning's potential for biometric verification accuracy and scalability. Works have combined EEG/ECG with additional biometric features. Priya et al. [122] designed a system merging EEG, eye blink, and voice, with 1.2% EER in a fusion corpus. Similarly, Zhang et al. [123] merged EEG, ECG, and gait, with 98.4% TAR and 0.5% FAR in a multimodal corpus. All these works enhance system robustness and reliability, especially for continuous verification.

B. Behavioral Biometrics

Behavioral biometrics introduces a different failure mode: behavior drifts even when identity stays constant. Typing rhythm, mouse dynamics, and touchscreen gestures change with fatigue, injury, stress, and device form factor, so static templates age quickly and require periodic adaptation. This creates a methodological challenge for the literature as well: a 2024 scoping review screened 14,179 records and included 122 studies, yet only 7 of 122 provided enough detail for replication and only 5.5% reported testing on demographic groups, which weakens the credibility of "low EER" claims when deployed across diverse users. Consequently, challenges such as fairness, longitudinal stability, and reproducibility should be derived and discussed as first-order issues for behavioral CA, not treated as secondary limitations [45]. The following modes of behavioral biometrics are used for continuous authentication.

1) Touch Dynamics

Touch dynamics have emerged as a prevalent technique for smart device user authentication by analyzing user behavior with touches, swipes, and taps on touchscreens. It's an ongoing, transparent user authentication method based on individual behavior trends. Several algorithms and techniques have been researched and developed for accuracy and reliability in touch-based authentication methodologies. Sae-Bae et al. [124] proposed a five-finger gesture and motion multi-touch scheme for information collection. They utilized Dynamic Time Warping (DTW) for comparison and attained 90% accuracy with an EER of 2% to 5% in a 34-subject collection. In contrast, Rauen et al. [125] examined us button press and scroll behavior, using a Random Forest model for classification and attaining 96.26% to 99.68% accuracy with a FAR of 3.15% and a False Rejection Rate FRR of 9.13%. Long-term continuous authentication, where a system monitors users over time, has also been a concern for most studies. Frank et al. [126] proposed a system examining

TABLE VI: Continuous authentication methods using ECG and EEG features as biometrics

Type	Method	Algorithm	Participants	Advantages	Drawbacks	Performance	Ref
EEG-Based	Alpha & beta wave ID	Not specified	20 subjects	Unique, spoof-proof	Needs EEG hardware	Acc: 91%	[116]
ECG-Based	ECG signal authentication	Correlation	PhysioNet	Unique heart pattern	Needs ECG hardware	EER: 2.5%	[117]
Multimodal (EEG+ECG)	Spectral + time feature fusion	Not specified	50 participants	More secure	Complex system	TAR: 95.3%, FAR: 3.2%	[118]
Multimodal (EEG+ECG)	Deep learning fusion	Deep Learning	AMIGOS	Low EER, deep learning	Needs big data, high computation	EER: 1.8%	[119]
EEG & ECG	CNN-based feature extraction	CNN	DEAP	High accuracy	Needs labeled data	Acc: 96.5%	[120]
EEG & ECG	Temporal features via RNNs	RNNs	DREAMER	High TAR, low FAR	Complex processing	TAR: 97%, FAR: 2%	[121]
Multimodal	EEG + blink + voice ID	Not specified	Hybrid dataset	Robust, reliable	High complexity	EER: 1.2%	[122]
Multimodal	EEG + ECG + gait fusion	Not specified	Multimodal dataset	Highly reliable	Needs multiple sensors	TAR: 98.4%, FAR: 0.5%	[123]

swipe behavior, using KNN and SVMs for classification and attaining 97% accuracy with an EER of 4.3% in a 30-subject collection. Similarly, Meng et al. [127] utilized deep learning for touch-based authentication, attaining a TAR of 98.2% and a FAR of 1.8% with a custom collection. Others have combined touch dynamics with additional behavior biometrics to improve accuracy. Liu et al. [128] proposed a model using an accelerometer and touch gesture, with 95.7% accuracy and an EER of 3.1% when trained and evaluated over a 50-subject collection. Mahfouz et al. [129] went further by combining touch dynamics and pressure, achieving 96.8% accuracy and a FAR of 2.7% over a big-data corpus. Others have focused on scaling touch-based authentication to larger audiences and diverse environments. Bajaber et al. [130] compared touch dynamics performance across device types with varying screen dimensions, achieving 93.5% accuracy over the TOUCHALYTICS corpus. Others regard ensemble approaches, such as gradient boosting and random forests, as effective for improving classification accuracy in touch-based authentication. Touch dynamics achieves strong short-window accuracy in many studies, yet the dominant deployment challenge is behavioral drift combined with device heterogeneity. Touch features shift with screen size, posture, fatigue, and interaction context, so thresholds calibrated on one device or one period can inflate false rejections when the user's routine changes. This makes model update policy part of the authentication method, rather than an implementation detail. Adaptive weighting in multimodal CA provides a practical mitigation because it can down-weight touch signals when reliability drops and shift emphasis to other passive channels.

2) *Stylometry Dynamics*

Stylometric identification techniques scan a person's idiosyncratic writing style by examining factors like sentence structure, term use, and writing behavior to confirm their identity. Stylometric techniques apply to short and long writings, using machine learning to detect such trends across a writer's works. Brocardo et al. [131] proposed a stylometry-based scheme for user authentication by decomposing writings into shorter segments to extract salient information. Simple (e.g., use of characters and terms) and complex (e.g., N-gram analysis) features were considered in decomposing writings to extract salient information using the SVM algorithm, an EER between 9.98% and 21.45% in two datasets, Twitter and Enron, was attained. In experiments, lexical and N-gram feature combinations can maximize stylometric analysis, according to experiments. Bhargava et al. [132] continued such work by researching specific operations in writings. 3,057 tweets underwent processing through machine algorithms, including SVM, KNN, Random Forest, and Multilayer Perceptron (MLP) with a 94.38% accuracy in classification, their scheme showed that combining a variety of classifiers can classify effectively short, informal writings. Stylometric identification recently adopted deep and composite approaches to maximize accuracy. Toshevska and Gievska [133] proposed a system using CNNs to analyze sentence-writing behavior. Training a model on a custom email dataset attained an EER of 7.3%. Similarly, Almlawi et al. [134] proposed a composite model combining RNNs with an attention mechanism for long-writing stylometric analysis, achieving 96.7% accuracy in IMDB review datasets. All such experiments reveal neural networks can capture complex stylometric features for authentication. Other works have blended stylometry with other performance improvement approaches. Stylometric analysis with topic modeling, mixing traditional lexical and syntactic features with Latent Dirichlet Allocation (LDA), achieved an EER of 8.4% for a Reddit corpus [135]. In another publication, a mix of social media and email corpus was analyzed via stylometric analysis using transformer-based architectures like BERT, with 97.2% accuracy [136]. Cross-domain stylometric analysis, writing variation, and dataset variation have also been tackled. Schaetti and Savoy [137] developed a scheme to address such variation via domain adaptation, with an EER of 12.5% when modeling between articles and blogs. Stylometry is attractive for continuous identity inference during text production, yet its reliability depends strongly on task type and content constraints. Short-form writing (e.g., messages) yields sparse stylistic evidence, while topic changes can dominate lexical features and mimic user change. Segment-based approaches reduce sparsity but increase latency, which delays intruder detection. For this reason, stylometry is best analyzed as a complementary dimension in a multi-dimensional identity model, rather than a standalone continuous authenticator.

3) Keystroke Dynamics

Keystroke pattern analysis is an established technique for user authentication, utilizing individuals typing habits. Factors such as key press events, key press duration, and key press interval fall under keystroke style categories. By collecting and comparing these factors, systems can accurately differentiate between and authenticate ongoing use. Earlier and current implementations have gone a long way in enhancing accuracy and efficiency. Joyce and Gupta [138] initially researched keystroke dynamics for user authentication through typing pace analysis. In experiments with 33 subjects typing a uniform paragraph, the system attained a FAR of 0.25% and a FRR of 16.36%. This initial study proved keystroke dynamics feasible for authentication in theory. Following its application, keystroke-based authentication was extended to smartphones by Gascon et al. [139]. They developed a continuous keystroke-based system for smartphones, utilizing 300 subjects typing short sentences (with background-captured finger motion) and SVM for comparison; experiments attained a 92% TPR and a 1% FPR, confirming keystroke dynamics viable for smartphone use. In following studies, newer techniques to improve accuracy and reduce rejection have been researched. Several algorithms for keystroke analysis were evaluated in a benchmarked corpus with 51 subjects in a study by Killourhy and Maxion [140]. Their experiments attained an 8% EER via digraph analysis and distance measurement. Similarly, Ayeswarya and Singh [43] incorporated keystroke features with a user's probabilistic model for continuous authentication improvement, with an EER of 5.5% over a custom corpus of 53 subjects. Integration with deep learning techniques boosted keystroke pattern recognition performance, too. Alpar [141] developed a system using CNNs for feature extraction in temporal and local dimensions for keystroke sequences, achieving 96.5% TPR and 0.7% FPR over 200 subjects, this technique outperforms most traditional keystroke methods. Almohamade [142] also designed a model combining RNNs and ensemble, with a mere 3.2% EER over a large corpus. Finally, keystroke pattern transferability between platforms and environments has been studied. Banerjee et al. [143] analyzed this transferability between desktop and mobile platforms, with 91.8% TPR and 2.1% FPR. In conclusion, keystroke dynamics have been proposed for use across a range of platforms.

4) Eye Movement

Behavioral biometric features of eye movements and blinks show significant potential for continuous user authentication. These methods analyze patterns of eye fixation, saccades, and blinking behavior, leveraging the uniqueness of individual ocular activities for secure authentication systems. Early and recent studies have demonstrated the effectiveness of these features in achieving high accuracy and low error rates. Zhang et al. [144] objects (middle and eight edges) using eye-tracking equipment. Their experimental results validated the utility of these features for authentication, setting the foundation for future research in this domain. Sluganovic et al. [145] extended this concept by analyzing subjects' screen focus and recording eye movements. In a large subject group, the system reached 88.73% accuracy and 10.61% EER, proving eye motions a reliable alternative for continuous authentication. Recent works focus on improving accuracy and dependability in eye-based authentication. Ayeswarya and Singh [43] explored a system using eye blink features for authentication, detecting and comparing blink patterns during authentication. Testing with the CEW dataset reached 98.4% accuracy, proving eye blink patterns a reliable biometric. Similarly, Javed et al. [146] proposed a scheme combining eye motion and blink features. Their system reached 96.7% TAR and 1.2% FAR with the EMOT dataset, proving combined eye-based features work effectively. Other works have proposed new techniques for the analysis of eye motion. Zemblys et al. [147] used deep neural networks (i.e., CNNs) for spatiotemporal feature extraction via eye-tracking, reaching 5.6% EER with a 50-subject dataset. Yang et al. [148] used combined gaze estimation and eye fixation analysis, reaching 97.2% accuracy with a mixed simulation-real dataset. All these works confirm how deep and machine learning techniques are improving performance of eye-based techniques for authentication.

C. Context-Aware Authentication

Context-aware authentication systems monitor a plethora of user behavior and environment factors such as IP addresses, device, OS, GPS location, battery and network consumption, web browsing, and web activity in an ongoing manner to authenticate and verify a user's identity in real-time. By tracking contextual factors, such as these, in real-time, the systems seek to detect normal and anomalous behavior, enhancing security and minimizing unauthorized access. These systems have been grouped into several categories, including location-aware, time-aware, device-aware, network-aware, environment-aware, activity-aware, and usage-aware, and several such categories have been sequentially proposed in literature, with Sbeyti [149] suggesting an implicit authentication mechanism utilizing a user activity pattern. In such a mechanism, a system monitors behavior such as where files have been accessed, operations performed, network access times, and involved IP addresses. In experiments with eight subjects, the system demonstrated efficacy with 90% accuracy, a 13.7% FAR, and an 11% FRR. This demonstrates how combining contextual factors enables efficient continuous authentication. Gomi et al. [150] proposed a web-browser-based authentication mechanism with an analysis of web-browser activity, including IP addresses, URLs, and access times, using linear regression (LR). In experiments with 1,000 subjects, such a mechanism attained 85% accuracy and an EER of 0.03%, proving that web-browser behavior could serve to identify a user. Mahbub et al. [151] utilized app-use behavior for CA, monitored the duration of use of a specific app, and utilized Hidden Markov Models (HMMs) for classification. In two experiments with datasets UMDAA-02 and Securacy, the system performed well with a 94% TAR and 5.2% FAR for UMDAA-02 and a 91% TAR and 6.1% FAR for Securacy. In other work, app use can make an authentication system smarter,

TABLE VII: Context-aware authentication methods and performance metrics

Method	Description	Contextual Parameters	Performance	Advantages	Drawbacks	Ref
Location-Based Auth.	Uses GPS, Wi-Fi, IP for ID verification	GPS, IP, Wi-Fi, cellular data	Acc: 93.5%, EER: 1.8%	Hard to fake	Signal loss issues	[152]
Time-Based Auth.	Verifies via time-based patterns	Access time, session duration	EER: 2–7%, TAR: 90%	Adapts to habits	Spoofing risks	[154]
Device-Based Auth.	Uses device data for authentication	Device ID, OS, hardware behavior	Acc: 96%, TAR: 93%	Seamless integration	Device dependency	[153]
Network-Based Auth.	Analyzes IP, traffic patterns	IP, traffic, VPN usage	TAR: 90%, FAR: 3%	Real-time monitoring	False positives risk	[155]
Environmental Context Auth.	Uses ambient factors like light, noise	Temperature, light, noise data	Acc: 88%, EER: 5%	Non-intrusive	Environmental sensitivity	[68], [156]
Activity-Based Auth.	Tracks physical behavior for ID	Gait, gestures, typing, app use	TAR: 94%, FAR: 5%	Continuous security	Behavioral variability	[151]
Usage Pattern Auth.	Uses device interaction patterns	App usage, browsing, network	Acc: 95%, FAR: 2%	Leverages user habits	Privacy & data needs	[157]

according to its theme. In the most recent work, extended context-aware authentication incorporated hybrid techniques. Cui et al. [152] combined GPS information with network and battery use behavior, with 93.5% accuracy and an EER of 1.8% with a custom dataset. Similarly, Gupta [153] designed a system combining browsing behavior with device-related parameters with training and prediction through ensemble techniques with 95.2% accuracy and a FAR of 2.1%, its performance outscored traditional techniques. In these studies, combining diverse contextual information sources boosts an authentication system's accuracy and robustness. As context-aware authentication continues to mature, it's becoming increasingly capable of offering secure, CA. Future research should focus on integrating additional contextual data streams, optimizing hybrid models, and addressing challenges such as privacy concerns and system scalability. Context-aware and multimodal CA reduces single-sensor fragility, yet it creates new integration challenges that directly follow from the design. Fusion improves robustness when one channel degrades, but it also expands the attack surface and complicates calibration because each modality has distinct noise patterns and failure costs. Recent work that fuses keystroke dynamics and gait through context-driven scoring reports 98.25% accuracy with 2.35% EER, illustrating the upside of adaptive weighting, but such gains depend on reliable context signals and careful handling of missing modalities. Therefore, fusion should be analyzed together with "fallback behavior" (what happens when signals disappear), not only with accuracy metrics [44].

D. Multi-dimensional identity construction

Multi-dimensional identity construction can be defined as the process of integrating heterogeneous evidence (biometrics, behavior, device state, and context) into a single, continuously updated trust representation that supports risk-scored decisions rather than one-off checks [158]. This framing becomes concrete in immersive workspaces where identity is inferred from task-bound signals, such as keyboard typing plus virtual hand movements and dwell time, achieving about 95% average identification accuracy (11/15 participants) with 0.41% FAR and 4.02% FRR in one evaluation [159]. Evidence diversity also matters in real-world wearables because models must separate identity from routine motion; a smartwatch study reported ¿1000 h of data from 60 participants, showing 0.29 EER in controlled settings and 0.7 EER under real-world conditions [160]. Touch-and-motion identity signals on smartphones contribute another dimension, where HMOG-based continuous authentication on 100 subjects reached roughly 99.0–99.2% accuracy and an EER of 1.25% [161]. Behavioral identity evidence can also be extracted from interaction dynamics in adversarially diverse scenarios; a mouse-dynamics study explicitly evaluated continuous authentication under two distinct gaming contexts to stress-test stability across tasks [162]. Physiological dimensions strengthen identity construction when captured passively; a deep-learning PPG method reported 99.5% (BIDMC), 99.6% (MIMIC), and 99.2% (CapnoBase) accuracies, highlighting how cardiac signatures can act as high-discriminability signals under benchmark conditions [163]. Practical constraints still shape which dimensions are usable on-device; low-frequency multi-channel PPG at 25 Hz with 4 s windows achieved 88.11% average test accuracy, 2.76% EER, and reduced sensor power consumption by 53% versus 512 Hz [164]. Security-oriented synthesis remains essential because multimodal identity pipelines create new attack surfaces; a 2025 review emphasizes missing dataset standardization and calls for security-first reporting using FAR/FRR/EER while explicitly mapping spoofing, replay, and presentation threats [165]. Privacy constraints further affect what "multi-dimensional" can safely mean in deployment; a 2024 survey organizes privacy-preserving biometrics and stresses persistent trade-offs between privacy protection, security, and recognition performance across modalities [166]. Context-aware designs attempt to retain multiple dimensions without exposing raw traces; a mobile proposal explicitly combines context awareness with privacy-preserving continuous authentication goals to reduce unnecessary data disclosure while keeping risk sensitivity [167]. Multi-dimensional construction is also visible in cross-modal identity learning, where camera-based PPG and fingerprints are fused using cross-modal attention to align both signals into a unified latent space for verification [168]. Interpretability now functions as an additional "dimension" for operational trust, since decision transparency supports auditing and tuning; an explainable CNN–LightGBM approach reported 98.7% average accuracy and 2.07% EER on ExtraSensory while using LIME to expose feature influence for genuine vs. impostor decisions [169].

IV. OPERATIONAL CHALLENGES

The challenges summarized below arise from identifiable properties of the methods discussed in Section 3. Physiological traits tend to raise concerns around template compromise severity and spoof resistance; behavioral traits primarily suffer from drift, device heterogeneity, and evaluation reproducibility; context-aware fusion reduces single-modality brittleness but increases system complexity, attack surface, and dependence on reliable sensor availability. Resource constraints are not a generic issue either: recent measurements on resource-constrained devices show authentication pipelines can be reduced from 2700 to 2100 CPU cycles, with runtime dropping from 61.2 ms to 42.3 ms and energy from 21.3 mJ to 19.8 mJ, highlighting that energy and latency trade-offs are measurable and should be reported alongside FAR/FRR/EER. This linkage keeps the challenge discussion evidence-driven and avoids repeating generic limitations [170]. Integrating novel solutions has consistently presented major obstacles for both developers and managers. Foremost among these challenges is ensuring user acceptance, which is critical for the successful adoption of robust identity protocols and multi-factor authentication. Implementing MFA solutions demands a meticulous and detailed strategy, particularly since many of the difficulties emerge from the very opportunities and advantages they offer.

A. Usability

User authentication poses significant usability challenges that arise from three key perspectives (task efficiency, task effectiveness, and user preference) collectively [22]. Task efficiency captures the time taken to register or log in [171]. In contrast, task effectiveness measures the number of attempts for success, reflecting how well users recall or input credentials. Preference shapes which approach individuals favor, underscoring the need for user-centric systems [172]. As noted in Alahmadi et al. [173], friction in authentication routines often fuels user dissatisfaction, leading them to circumvent security guidelines. Demographic factors amplify these tensions. Younger users input PINs or graphical credentials more swiftly Kausar et al. [174], while older adults often need more time for similar tasks. Studies by Qazi et al. [175] and De Andrés et al. [176] suggest gender variance matters less for login performance than expected. Cognitive factors have a role in shaping experiences, too. Verbally strong users perform best with textual approaches, while graphical prompts suit others. Password-reliant systems risk issues if poorly designed; organized passphrases or prompts can reduce user frustration. User authentication complexity extends even to device-related concerns. Small or touchscreen keyboards cause typos and slow typing, making handhelds cumbersome for textual passwords [176], [177]. Other studies note similar efficiency issues, and as Adeniran et al. [178] and Yusop et al. [179] highlight, many platforms avoid newer methods (vs. passwords/PINs) for this reason. Multi-factor authentication boosts security via tokens, biometrics, or one-time codes, but complexity must be added carefully to avoid discouraging use. Baseer and Charumathi [180] emphasize balancing usability and security, critical for biometrics like ECG (best in static environments [181]) and smartphone camera-based face/iris recognition (Garea-Llano and Morales-Gonzalez [182]), which show potential but raise data transmission concerns. Lone and Mir [183] found biometrics enable fast logins and higher satisfaction on Android, but enterprise deployment and training carry higher costs. Ethical factors compound complexity: not all users can access biometric systems e.g., those with limb loss or sensory impairments. Despite these challenges, user acceptance determines an authentication method's success. Furuberg and Øseth [184] stress prioritizing user experience drives adoption. Overly convoluted processes (e.g., long, frequently changed passwords) push users to risky behaviors like storing credentials insecurely. Usability improvements include simpler PINs or visual aids, though solutions must remain threat-resilient. Some researchers explore novel designs, such as gamification, story-based prompts, and graphical interactions, to speed adoption and improve usability [185], [186]. However, caution is needed: new solutions can introduce drawbacks like memorability issues or privacy risks. Moreover, Safder [44] notes uniform designs rarely meet diverse user needs. Traditional methods like the username-password model will coexist with emerging biometrics, adaptive MFA, and device-specific interfaces. The field must adapt to rapid tech change without neglecting legal and ethical factors tied to data privacy and inclusivity. Ultimately, managing this balance requires cross-disciplinary collaboration. security experts, UX designers, policymakers, and end-users must co-create robust, accessible practices, ensuring innovation does not compromise usability or fairness.

B. Integration challenges

Integration challenges remain despite developers addressing usability concerns. Most consumer MFA solutions are heavily hardware-centric, complicating broader organizational convergence. Merging physical and IT security offers efficiency and compliance gains but faces hurdles: chief among them is unifying security teams and upgrading legacy access systems not designed for interoperability. Specific studies highlight limitations of mixing old and new components. For instance, Surve et al. [187] reported bridging older card-based entry with modern biometrics often demands specialized hardware adaptors, raising costs and prolonging deployment. Additionally, integrating non-native biometric sensors is problematic when existing frameworks lack standardized interfaces [188]. Consequently, many enterprises struggle to accommodate new biometric devices, a difficulty compounded by needing continuous system-wide updates. For multi-biometrics (multiple factors in parallel), Inverso et al. [189] note added architectural and performance considerations, concurrent verification pathways may delay or require software backend reengineering.

Vendor dependence is another key concern: enterprise MFA products are often isolated ecosystems with minimal flexibility for adopting unfamiliar hardware [190]. Nguyen and Beijnon [191] found most vendors offer closed interfaces, making new sensor integration costly or unfeasible without extensive custom development. This proprietary nature raises trust and reliability questions, especially for organizations relying on black-box solutions. Limited transparency complicates auditing data flows and security measures [192] and fosters risks from software updates or vendor lock-in. Meanwhile, Sun et al. [193] recommends "biometrics independence", frameworks adapting to multiple sensor technologies and manufacturers to meet interoperability standards. Openness in both hardware and software can mitigate these issues. Fourné [194] have noted a growing call for open-source MFA components, although mainstream adoption remains slow. Ultimately, organizations must weigh trade-offs between proven, vendor-specific solutions and customizable, transparent alternatives. This decision should account for upfront integration costs, long-term sustainability, upgrade paths, and third-party trustworthiness.

C. Security and Privacy

An MFA framework is a digital ecosystem incorporating critical components: sensors, data storage, processing units, and communication channels [195]. Each element faces attacks of varying scales, from simple replay attempts to sophisticated adversarial exploits [196]. Since privacy depends on robust security at every stage, the first layer of concern focuses on the input device itself [197]. Ensuring only authorized controllers handle sensitive personal data is pivotal, as it relates to a primary risk: data spoofing. Specifically, attackers may inject fraudulent data the MFA system accepts as genuine [198]. This risk escalates with greater biometric use, as attackers can analyze sensor technology and hardware to identify effective spoofing materials. Ideally, system architects secure the environment; if unfeasible, they should at least evaluate possible spoofing vectors early in the design process. The risk of capturing physical or electronic patterns, replayed to the MFA system, must be tackled systematically, often via timestamps or other measures to neutralize replay attacks [199]. Unfortunately, biometric spoofing can be relatively straightforward to implement [200]. While biometrics enhance MFA performance, they also expand the attack surface for intruders.

Another major threat is data theft during transmission between the sensor and processing or storage unit. If communication channels from input to database lack adequate protection, attackers can intercept sensitive data [201]. Developers must ensure robust security measures, including encryption and secure transfer protocols, at every point to resist such threats [202]. An additional concern is theft of secret data samples [200]. For knowledge-based factors, zero-knowledge approaches are vital; without them, an attacker obtaining the user's secret immediately compromises the system. Biometrics demand greater protection, as they cannot be replaced if compromised. Security protocols must safeguard biometric data during capture, transmission, storage, and processing [200]. Data storage is another potential single point of failure, especially when databases use centralized architectures [203], [204]. Moreover, some remote systems communicating with the database lack authorization to access personal information, underscoring the need for isolation and irreversible encryption [205]. Location-based attacks (e.g., GPS jamming/spoofing) undermine MFA by producing false time and location data, with similar vulnerabilities in cellular and WLAN location services [206], [207]. Finally, as an IT system, MFA must maintain sufficient throughput to handle authentication request volumes [208]. A system processing one biometric match per hour but needing 100 becomes infeasible, regardless of security improvements [209]. To mitigate these risks, careful hardware selection, system capacity planning, and a dedicated penetration testing environment are essential. Many organizations now rely on external audits to identify emerging vulnerabilities and guide strategic improvements. Ultimately, continuous assessments and updates remain critical to ensure an MFA system delivers a secure environment in practice.

D. Modality-Specific Issues

In real-life environments, authentication mechanisms must align with a user's current state and activity, as no single mechanism works for all users in all settings. Continuous authentication techniques relying on physiological factors struggle to become ubiquitous. Fingerprints require occasional active scans, counterintuitive to CA, which aims to passively authenticate users without specific actions [43]. Fingerprint technology cannot enable continuous, unobstructed authentication, so its use is compromised in environments where full attention isn't assured [210], [211]. Voice-based CA also faces limitations: it depends on constant speech, making it uncomfortable for quiet users or those in speech-impractical environments [212]. Interruptions to speech, plus the intrusion of constant audio monitoring, raise privacy concerns [213]. Moreover, background noise and speech variation reduce the reliability and specificity of voice-dependent systems in settings needing unobtrusive security [214].

Face and iris recognition have potential for CA but require the device to remain focused on the user's face. Yet they face significant user acceptance hurdles, as constant camera monitoring feels intrusive [215]. Users find the collection of facial and eye data uncomfortable, leading to resistance [216]. Additionally, lighting and obstructions disrupt these techniques, reducing reliability in varied environments [217]. These weaknesses underscore the need to balance security with user comfort and privacy to make biometric systems feasible [218, 219]. Motion-based CA, using gait analysis to identify users via walking behavior, also has obstacles. Jogging or even light exercise can alter gait, reduce recognition accuracy and cause authentication failures [220]. Since it relies on repetitive behavior, it's less reliable in scenarios with varied physical activity, harming dependability [10], [221]. Worse, gait analysis is impacted by shoes, state of the ground, and carried items, introducing randomness and authentication complications [222]. These factors make motion-based systems less reliable in environments demanding high accuracy and adaptability [223], [224].

Context-aware techniques relying solely on GPS also have weaknesses. GPS-based CA verifies location but fails if a device is hijacked in that area. In such cases, the system cannot distinguish between the legitimate user and a physical impersonator [225], [226]. Location restrictions lock out legitimate users who step outside defined areas, inconveniencing them and compromising usability. This inability to authenticate users via location undermines GPS-dependent systems' security [227]. Online search history and web browsing-dependent CA is even more challenging. Techniques lack a technical framework for real use, specifically in terms of real-time adaption to changing behavior [228]. Training algorithms to adapt to new data (e.g., changed behavior or new websites) while maintaining accuracy is a major challenge. Without strong frameworks to manage this variation, these techniques can't provide reliable security, reducing their effectiveness in CA [229]. Inability to have strong approaches for managing changing behavior of a user renders search history-dependent techniques less effective [230], [231]. All CA techniques have weaknesses limiting their suitability for specific users. Finger and voice recognition demand active user input, conflicting with passive CA goals. Face and iris recognition face low acceptance and environmental issues; motion-based systems struggle with activity variation. GPS-based systems fail at device theft in target locations and exclude valid users from predefined areas. Search-history-based techniques lack the technical robustness to manage changing user behavior effectively. These gaps highlight the need for multi-modal systems, combining multiple techniques, to balance security and usability, ensuring flexibility across user scenarios.

E. Other Issues

From a usability viewpoint, MFA introduces a range of pragmatic concerns, varying in kind and severity across biometric approaches. Perhaps the most critical issue is compromised accuracy in recognizing, with security and usability implications. High FAR can break security through unauthorized access, and high FRR infuriates through continuous rejection of valid access [232]. Experiments like Shah et al. [233] show even slight recognition inaccuracies erode user trust and discourage MFA use. Environmental variation and changes in user behavior over time exacerbate these accuracy issues, making consistent performance challenging [22], [234]. Another key challenge is the lack of uniform protocols and standards for continuous authentication. Organizations like the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) have promulgated standards for authentication usability and cryptographic protocols, but not for CA [235]. Without such standards, implementing and assessing CA systems is harder, determining enrollment duration (when user behavior is analyzed and modeled) is critical to balancing security and usability. In case the period of enrollment is not long enough, fails to capture enough user behavior, creating vulnerabilities [236]. On the other hand, when it's too long, access will be delayed, and it will have a negative impact on a user [237]. In addition, uniform standards for deciding when a device must lock upon unauthorized access must be designed to ensure security actions occur uniformly in any system [238], [239]. Without them, disparate CA systems can't integrate, hindering scalability across environments [240].

Power consumption is a key MFA usability concern, especially in handheld gadgets like smartphones. MFA frameworks use sensors, such as proximity sensors, light sensors, gyroscopes, barometers, accelerometers, and digital compasses, to track continuous behavior and physiological indications [242]. These sensors and data processing drain batteries quickly, limiting widespread use [243]. Beyond this, CA raises user security and privacy concerns. Users will not utilize such frameworks when constant information dissemination is involved, especially when data can be intercepted and abused [244], [245]. Strong encryption and security measures are essential but add complexity and requirements. Integrating CA into existing security frameworks also demands significant software and hardware modifications, requiring time and investment [235], [246].

User acceptance and trust are critical for CA systems to work effectively. Users must perceive CA as reliable, unobtrusive, and useful for adoption. Negative experiences, like false rejections or battery use, lead users to abandon CA. Trust requires improving (CA's) technical performance and transparency in data collection, use, and protection [247]. Transparent privacy policies and user awareness can ease concerns and build positive perceptions [248]. Studies by Fleury and Chaniaud [249], involving evaluation and design with users, can yield effective continuous acceptance solutions supporting groups' requirements and expectations. Despite CA's strong security potential, it faces significant usability barriers: reduced recognition accuracy, lack of uniform protocols, high power use, privacy concerns, and user trust requirements. Overcoming these via ongoing research is critical for CA to deliver strong security without sacrificing usability. When these barriers are addressed, CA can become a viable, universally adopted security tool in real-life scenarios.

V. FUTURE OF MFA INTEGRATION

The future of multi-factor authentication is shaped by its widespread use in industries and availability in consumer goods of biometric service in terms of increased availability in goods and industries' acceptance. Scholars and early adopters are working to insert new sensors in MFA platforms in an attempt to seek security improvement with no usability loss. Behavior analysis transitioned from analysis of simple typing behavior to complex techniques including gesture and gait analysis, using accelerometer data for creating profiles through behavior [18], [40]. It can integrate seamlessly with text-based authentication, supporting continuous authentication through observation of device-user behavior [12], [241]. Telecommunication technology such as beam-forming, in terms of Multiple-Input and Multiple-Output (MIMO) technology, is under consideration for authenticating user tokens through identifying sources of a signal [32]. All these approaches have increased physical-layer security, but with demand for improvement in terms of infrastructure in terms of wireless and integration

TABLE VIII: Future of MFA integration

Method	Description	Advantages	Drawbacks	Ref
Behavior Detection	Tracks typing, gestures, gait	Secure, seamless	Variable, Inaccurate	[18], [40]
Beam-Forming	Uses MIMO for localization	Precise ID	Complex, Costly	[32], [31]
OCS	Identifies vehicle occupants	Secure, personalized	Unreliable, Inconsistent	[27], [17]
ECG	Authenticates via heart signals	Hard to fake	Wearable, Inconsistent, Costly	[35], [16]
EEG	Uses brain waves for ID	Unique, secure	Unpopular, Variable, Impractical	[35], [16]
DNA	Uses DNA for authentication	Ultimate security	Slow, Ethical, Costly	[24], [13]

TABLE IX: Evaluation of emerging MFA integration methods

Method	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Behavior Detection	High	High	Moderate	High	High	Moderate
Beam-Forming Techniques	Moderate	High	Low	High	Moderate	Low
Occupant Classification Systems (OCS)	High	Moderate	High	High	High	Moderate
Electrocardiographic (ECG) Recognition	Moderate	High	Low	High	Moderate	High
Electroencephalographic (EEG) Recognition	Low	Very High	Low	High	Low	Very High
DNA Recognition	Low	Extremely High	Very Low	Very High	Low	Very High

in terms of hardware [31]. Another development is Occupant Classification Systems (OCS) in automobiles, through use of sensors for occupant presence and occupant identification through weight and postures, offering personalized security and function in automotive environments [27], [17]. Electrocardiographic (ECG) and Electroencephalographic (EEG) recognition is taking biometric security to a new level through heart and brain waves offering high security and individualized user authentication [35], [16]. While ECG recognition offers a level of security with the advantage of being difficult to mimic, it requires specialized wearable devices and can be intrusive for users. Similarly, EEG recognition provides uniqueness but faces challenges in user acceptance and practicality due to the need for non-invasive headsets and the complexity of brain wave analysis. DNA recognition stands out as the pinnacle of biometric security with its unparalleled uniqueness, although its application is currently limited by high costs, invasiveness, and ethical concerns [24], [13]. As these advanced authentication methods continue to develop, they must address challenges related to data privacy, user acceptability, and the technical limitations of integrating multiple authentication factors into cohesive and user-friendly systems.

VI. CONCLUSION

This survey emphasizes the growing need for more advanced authentication methods that move beyond traditional single-factor approaches. The strategies for continuous authentication, combined with multiple identity factors, offer great potential for reducing data breaches and improving user convenience. Key takeaways focus on finding the right balance between security, privacy, user acceptance, and the challenges of integrating multi-modal systems. As cyber threats continue to grow in sophistication, continuous authentication is becoming a critical component in protecting digital assets and personal data. With thoughtful design and thorough testing, organizations and researchers can unlock the benefits of continuous, context-aware identity verification across various digital interactions.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No. 92267204, Grant No.92467201), Key R&D Program of Shandong Province (Grant No. 2024CXPT039), and funded by China Scholarship Council.

REFERENCES

[1] D. Miller, L. Abed Rabho, P. Awondo, M. de Vries, M. Duque, P. Garvey et al., *The global smartphone: Beyond a youth technology*. UCL Press, 2021.

[2] A. Zielonka, M. Woźniak, S. Garg, G. Kaddoum, M. J. Piran, and G. Muhammad, “Smart homes: How much will they support us? A research on recent trends and advances,” *IEEE Access*, vol. 9, pp. 26388–26419, 2021.

[3] C. P. Andriotis and K. G. Papakonstantinou, “Managing engineering systems with large state and action spaces through deep reinforcement learning,” *Reliability Engineering & System Safety*, vol. 191, p. 106483, 2019.

[4] X. Wang, Z. Yan, R. Zhang, and P. Zhang, “Attacks and defenses in user authentication systems: A survey,” *Journal of Network and Computer Applications*, vol. 188, p. 103080, 2021.

[5] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, “User authentication on mobile devices: Approaches, threats and trends,” *Computer Networks*, vol. 170, p. 107118, 2020.

[6] D. Köhler, E. Klieme, M. Kreuseler, F. Cheng, and C. Meinel, “Assessment of remote biometric authentication systems: another take on the quest to replace passwords,” in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 2021, pp. 22–31.

[7] V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "A comprehensive study on passwordless authentication," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2022, pp. 1266–1275.

[8] M. A. Al Kabir and W. Elmedany, "An overview of the present and future of user authentication," in *2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, 2022, pp. 10–17.

[9] A. Suokas, "Privileged Accounts Protection with Multi-factor Authentication," 2023.

[10] P. Bansal and A. Ouda, "Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics," *Computers*, vol. 13, p. 103, 2024.

[11] D. Temoshok, Y.-Y. Choong, R. Galluzzo, M. LaSalle, A. Regenscheid, D. Proud-Madruga, et al., "NIST SP 800-63-4: Digital Identity Guidelines," National Institute of Standards and Technology, Gaithersburg, MD, 2025.

[12] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey," *Information Fusion*, vol. 66, pp. 76–99, 2021.

[13] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors*, vol. 21, p. 6163, 2021.

[14] A. M. Mostafa, M. Ezz, M. K. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani et al., "Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication," *Applied Sciences*, vol. 13, p. 10871, 2023.

[15] M. J. Rooney, "An Empirical Assessment of the Use of Password Workarounds and the Cybersecurity Risk of Data Breaches," Nova Southeastern University, 2023.

[16] M. Wang, S. Wang, and J. Hu, "Cancellable template design for privacy-preserving EEG biometric authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3350–3364, 2022.

[17] G. Singh, G. Bhardwaj, S. V. Singh, and V. Garg, "Biometric identification system: security and privacy concern," *Artificial intelligence for a sustainable industry 4.0*, pp. 245–264, 2021.

[18] N. H. C. Kamaruddin and M. F. Zolkipli, "The Role of Multi-Factor Authentication in Mitigating Cyber Threats," *Borneo International Journal*, vol. 7, pp. 35–42, 2024.

[19] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A systematic survey of multi-factor authentication for cloud infrastructure," *Future Internet*, vol. 15, p. 146, 2023.

[20] S. L. Burton, "Advancing Cybersecurity: Strategic Insights Into Multifactor Authentication," *Organizational Readiness and Research: Security, Management, and Decision Making*, pp. 247–282, 2025.

[21] I. Ahmed and A. Asghar, "Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare," *International Journal of Responsible Artificial Intelligence*, vol. 13, pp. 1–12, 2023.

[22] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Computers and Electrical Engineering*, vol. 119, p. 109485, 2024.

[23] T. Bisztray, "Investigating Privacy Aspects of Identity Management: From Data Protection Impact Assessment for Biometric Applications to Privacy-Centric Password Testing," 2023.

[24] K. Coombs, "Perspectives of Cybersecurity Risks in DNA Data Storage Environment," Capella University, 2024.

[25] T. Kumar, S. Bhushan, P. Sharma, and V. Garg, "Examining the Vulnerabilities of Biometric Systems: Privacy and Security Perspectives," in *Leveraging Computer Vision to Biometric Applications*, Chapman and Hall/CRC, 2024, pp. 34–67.

[26] A. M. Abdulkareem and A. Gordon, "Evaluating the Usability and User Acceptance of Biometric Authentication in Different Applications," *Quarterly Journal of Emerging Technologies and Innovations*, vol. 8, pp. 1–10, 2023.

[27] G. Abdelkader, K. Elgazzar, and A. Khamis, "Connected vehicles: Technology review, state of the art, challenges and opportunities," *Sensors*, vol. 21, p. 7712, 2021.

[28] S. Oduri, "Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era," *International Journal of Innovative Research in Science Engineering and Technology*, vol. 13, pp. 13632–13640, 2024.

[29] L. D. Chhibbar, S. Patni, S. Todi, A. Bhatia, and K. Tiwari, "Enhancing security through continuous biometric authentication using wearable sensors," *Internet of Things*, vol. 28, p. 101374, 2024.

[30] J. Solano, L. Camacho, A. Correa, C. Deiro, J. Vargas, and M. Ochoa, "Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications," *International Journal of Information Security*, vol. 20, pp. 181–197, 2021.

[31] Y. Cahyaningrum, "Evaluation of System Access Security in The Implementation of MultiFactor Authentication (MFA) in Educational Institutions," *Journal of Practical Computer Science*, vol. 4, pp. 11–19, 2024.

[32] M. L. Rathod and A. Meera, "Modeling of a Smart Antenna System with Adaptive Beam Forming Technology," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 767–772.

[33] O. A. Farayola, O. L. Olorunfemi, and P. O. Shoetan, "Data privacy and security in it: a review of techniques and challenges," *Computer Science & IT Research Journal*, vol. 5, pp. 606–615, 2024.

[34] P. M. S. Sánchez, J. M. J. Valero, A. H. Celdrán, G. Bovet, M. G. Pérez, and G. M. Pérez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," *IEEE Communications Surveys & Tutorials*, vol. 23, pp. 1048–1077, 2021.

[35] A. B. Tatar, "Biometric identification system using EEG signals," *Neural Computing and Applications*, vol. 35, pp. 1009–1023, 2023.

[36] S. Rostamzadeh, A. Abouhossein, S. Vosoughi, S. B. Gendeshmin, and R. Yarahmadi, "Stress influence on real-world driving identified by monitoring heart rate variability and morphologic variability of electrocardiogram signals: the case of intercity roads," *International journal of occupational safety and ergonomics*, vol. 30, pp. 252–263, 2024.

[37] M. Kokila and S. Reddy, "Authentication, Access Control and Scalability models in Internet of Things Security-A Review," *Cyber Security and Applications*, p. 100057, 2024.

[38] J. Abrera, "Data Privacy and Security in Cloud Computing: A Comprehensive Review," *Journal of Computer Science and Information Technology*, vol. 1, pp. 01–09, 2024.

[39] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide*, 1st Ed., Cham: Springer International Publishing, vol. 10, pp. 10–5555, 2017.

[40] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment," *Sensors*, vol. 24, p. 3575, 2024.

[41] N. Zeeshan, M. Bakyt, N. Moradpoor, and L. La Spada, "Continuous Authentication in Resource-Constrained Devices via Biometric and Environmental Fusion," *Sensors*, vol. 25, p. 5711, 2025.

[42] P. T. Tran-Truong, M. Q. Pham, H. X. Son, D. L. T. Nguyen, M. B. Nguyen, K. L. Tran, et al., "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," *Journal of Systems Architecture*, vol. 162, p. 103402, 2025.

[43] R. M. Saqib, A. S. Khan, Y. Javed, S. Ahmad, K. Nisar, I. A. Abbasi et al., "Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security," *Intelligent Automation & Soft Computing*, vol. 32, 2022.

[44] S. Ayeswarya and K. J. Singh, "A comprehensive review on secure biometric-based continuous authentication and user profiling," *IEEE Access*, vol. 12, pp. 82996–83021, 2024.

[45] O. L. Finnegan, J. W. White Iii, B. Armstrong, E. L. Adams, S. Burkart, M. W. Beets, et al., "The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review," *Systematic Reviews*, vol. 13, p. 61, 2024.

[46] D. Boshoff and G. P. Hancke, "A classifications framework for continuous biometric authentication (2018–2024)," *Computers & Security*, vol. 150, p. 104285, 2025.

[47] T. A. Busey, N. Heise, R. A. Hicklin, B. T. Ulery, and J. Buscaglia, "Characterizing missed identifications and errors in latent fingerprint comparisons using eye-tracking data," *PloS one*, vol. 16, p. e0251674, 2021.

[48] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," *IEEE Internet of Things Journal*, vol. 8, pp. 65–84, 2020.

[49] S. Ayeswarya and K. J. Singh, "A comprehensive review on secure biometric-based continuous authentication and user profiling," *IEEE Access*, 2024.

[50] W. Safder, "PASSWORD SECURITY, AN ANALYSIS OF AUTHENTICATION METHODS," ed, 2024.

[51] F. Binbeshr, K. C. Siong, L. Yee, M. Imam, A. A. Al-Saggaf, and A. A. Abudaqa, "A systematic review of graphical password methods resis-

tant to shoulder-surfing attacks," *International Journal of Information Security*, vol. 24, pp. 1–22, 2025.

[52] V. Zimmermann, "From the quest to replace passwords towards supporting secure and usable password creation," 2021.

[53] M. Jubur, P. Shrestha, and N. Saxena, "An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools," *ACM Computing Surveys*, 2025.

[54] M. Lodder, "Token Based Authentication and Authorization with Zero-Knowledge Proofs for Enhancing Web API Security and Privacy," 2023.

[55] H. R. M. H. Hamid, N. W. Nordin, N. Y. Abdullah, W. H. W. Ismail, and D. Abdullah, "Two Factor Authentication: Voice Biometric and Token-Based Authentication," in *Applied Problems Solved by Information Technology and Software*, Springer, 2024, pp. 27–35.

[56] M. Schink, A. Wagner, F. Unterstein, and J. Heyszl, "Security and trust in open source security tokens," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 176–201, 2021.

[57] T. Sun, N. He, J. Xiao, Y. Yue, X. Luo, and H. Wang, "All Your Tokens are Belong to Us: Demystifying Address Verification Vulnerabilities in Solidity Smart Contracts," arXiv preprint arXiv:2405.20561, 2024.

[58] S. Singh, S. Sharma, M. Awasthi, S. Rawat, and Y. Chanti, "Advancements of Emerging Technologies in Biometrics Authentication," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 2024, pp. 1–7.

[59] P. Aithal, "Implementation of Voice Biometric System in the Banking Sector," *International Journal of Applied Engineering and Management Letters (IJAEML)*, vol. 8, pp. 120–127, 2024.

[60] H. Gururaj, B. Soundarya, S. Priya, J. Shreyas, and F. Flammini, "A Comprehensive Review of Face Recognition Techniques, Trends and Challenges," *IEEE Access*, 2024.

[61] V. Upadhyaya, "Advancements in Computer Vision for Biometrics Enhancing Security and Identification," in *Leveraging Computer Vision to Biometric Applications*, Chapman and Hall/CRC, 2025, pp. 260–292.

[62] J. Rose, A. Zabin, and T. Bourlai, "On Assessing the Impact of Ocular Pathologies on the Performance of Deep Learning Ocular Based Recognition Systems in the Visible and NIR Bands," in *Face Recognition Across the Imaging Spectrum*, Springer, 2024, pp. 233–252.

[63] A. K. Jain, A. A. Ross, K. Nandakumar, and T. Swearingen, "Iris Recognition," in *Introduction to Biometrics*, Springer, 2024, pp. 175–214.

[64] G. K. Kyeremeh, M. Abdul-Al, R. Qahwaji, and R. Abd-Alhameed, "Verification technology for finger vein biometric," arXiv preprint arXiv:2405.11540, 2024.

[65] H. M. Ahmed, D. Elsheweikh, and S. Shaban, "Security system based on hand geometry and palmprint for user authentication in E-correction system," *International Journal of Information Technology*, vol. 16, pp. 1783–1799, 2024.

[66] S. Li, L. Fei, B. Zhang, X. Ning, and L. Wu, "Hand-based multimodal biometric fusion: A review," *Information Fusion*, p. 102418, 2024.

[67] P. Rad, G. Dorai, and M. Jozani, "From Seaweed to Security: The Emergence of Alginate in Compromising IoT Fingerprint Sensors," arXiv preprint arXiv:2404.02150, 2024.

[68] M. H. Memon, J.-P. Li, I. Memon, and Q. A. Arain, "GEO matching regions: multiple regions of interests using content based image retrieval based on relative locations," *Multimedia Tools and Applications*, vol. 76, pp. 15377–15411, 2017.

[69] M. Saideh, J.-P. Jamont, and L. Vercouter, "Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things," *Sensors*, vol. 24, p. 4621, 2024.

[70] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digital Communications and Networks*, vol. 8, pp. 422–435, 2022.

[71] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, "Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering," Available at SSRN, 2024.

[72] I. Traore, *Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*. Igi Global, 2011.

[73] L. Ibanez-Lissen, J. M. De Fuentes, L. Gonzalez-Manzano, and N. Anciaux, "Continuous Authentication Leveraging Matrix Profile," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 2024, pp. 1–13.

[74] I. Stylios and S. Aegean, "Behavioral biometrics for continuous authentication: security and privacy issues," University of the Aegean, Greece, 2023.

[75] M. F. Hasan, F. Ashfaq, A. A. Chowdhury, S. I. Hamim, and M. Rahmani, "Dynamic authentication protocols for advanced security in federated metaverse systems," Brac University, 2024.

[76] M. O. Abolarinwa, "Enhanced Local Binary Pattern with Chinese Remainder Theorem and Swarm Intelligent Technique for Face Recognition System," Kwara State University (Nigeria), 2022.

[77] L. Lu, J. Yu, Y. Chen, and Y. Wang, "Vocallock: Sensing vocal tract for passphrase-independent user authentication leveraging acoustic signals on smartphones," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, pp. 1–24, 2020.

[78] B. Alharbi and H. S. Alshanbari, "Face-voice based multimodal biometric authentication system via FaceNet and GMM," *PeerJ Computer Science*, vol. 9, p. e1468, 2023.

[79] F. Abbaas and G. Serpen, "Evaluation of biometric user authentication using an ensemble classifier with face and voice recognition," arXiv preprint arXiv:2006.00548, 2020.

[80] M. Stokkenes, R. Ramachandra, A. Mohammadi, S. Venkatesh, K. Raja, P. Wasnik et al., "Smartphone Multi-modal Biometric Presentation Attack Detection," in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*, Springer, 2023, pp. 521–544.

[81] H. Fereidooni, J. König, P. Rieger, M. Chilese, B. Gökbakan, M. Finke et al., "AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms," arXiv preprint arXiv:2302.02740, 2023.

[82] A. Alshardan, A. Kumar, M. Alghamdi, M. Maashi, S. Alahmari, A. A. Alharbi et al., "Multimodal biometric identification: leveraging convolutional neural network (CNN) architectures and fusion techniques with fingerprint and finger vein data," *PeerJ Computer Science*, vol. 10, p. e2440, 2024.

[83] C. Zhang, Y. Zhao, Y. Huang, M. Zeng, S. Ni, M. Budagavi et al., "Facial: Synthesizing dynamic talking face with implicit attribute learning," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2021, pp. 3867–3876.

[84] A. K. Yadav, R. Pateriya, N. K. Gupta, P. Gupta, D. K. Saini, and M. Alahmadi, "Hybrid Machine Learning Model for Face Recognition Using SVM," *Computers, Materials & Continua*, vol. 72, 2022.

[85] P. A. Thomas and K. Preetha Mathew, "A broad review on non-intrusive active user authentication in biometrics," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 339–360, 2023.

[86] J. Han and B. Bhanu, "Individual recognition using gait energy image," *IEEE transactions on pattern analysis and machine intelligence*, vol. 28, pp. 316–322, 2005.

[87] K. Shiraga, Y. Makihara, D. Muramatsu, T. Echigo, and Y. Yagi, "Geinet: View-invariant gait recognition using a convolutional neural network," in *2016 international conference on biometrics (ICB)*, 2016, pp. 1–8.

[88] Z. Wu, Y. Huang, L. Wang, X. Wang, and T. Tan, "A comprehensive study on cross-view gait based human identification with deep cnns," *IEEE transactions on pattern analysis and machine intelligence*, vol. 39, pp. 209–226, 2016.

[89] R. Zhang, D. Yin, Z. Zhou, Z. Cao, F. Meng, and B. Hu, "Improving cross-view gait recognition with generative adversarial networks," *Electrical Engineering and Computer Science (EECS)*, vol. 3, pp. 43–47, 2019.

[90] W. Zeng, C. Wang, and F. Yang, "Silhouette-based gait recognition via deterministic learning," *Pattern recognition*, vol. 47, pp. 3568–3584, 2014.

[91] Z. Qin, Y. Liu, P. Ji, D. Kim, L. Wang, R. I. McKay et al., "Fusing higher-order features in graph neural networks for skeleton-based action recognition," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, pp. 4783–4797, 2022.

[92] H. Chao, K. Wang, Y. He, J. Zhang, and J. Feng, "GaitSet: Cross-view gait recognition through utilizing gait as a deep set," *IEEE transactions on pattern analysis and machine intelligence*, vol. 44, pp. 3467–3478, 2021.

[93] T. Huang, X. Ben, C. Gong, W. Xu, Q. Wu, and H. Zhou, "GaitDAN: Cross-view Gait Recognition via Adversarial Domain Adaptation," *IEEE Transactions on Circuits and Systems for Video Technology*, 2024.

[94] W. Cheng, X. Yan, and Y. Luo, "Gaitstc: A Pure Spatial-Temporal Convolution Network For Skeleton-Based Gait Recognition," in *2024 4th International Conference on Neural Networks, Information and Communication (NNICE)*, 2024, pp. 759–765.

[95] M. Gadaleta and M. Rossi, "Idnet: Smartphone-based gait recognition with convolutional neural networks," *Pattern Recognition*, vol. 74, pp. 25–37, 2018.

[96] R. N. Yousef, A. T. Khalil, A. S. Samra, and M. M. Ata, "Proposed methodology for gait recognition using generative adversarial network with different feature selectors," *Neural Computing and Applications*, vol. 36, pp. 1641–1663, 2024.

[97] R. Ghosh, "A Faster R-CNN and recurrent neural network based approach of gait recognition with and without carried objects," *Expert Systems with Applications*, vol. 205, p. 117730, 2022.

[98] C. Wang, Y. Gao, Y. Li, and M. Zhang, "GaitParse: Gait Parsing Algorithm with Self-Supervised Fine-Tuning for Gait Recognition," in *Proceedings of the 2023 9th International Conference on Communication and Information Processing*, 2023, pp. 85–92.

[99] C. Shen, S. Yu, J. Wang, G. Q. Huang, and L. Wang, "A Comprehensive Survey on Deep Gait Recognition: Algorithms, Datasets, and Challenges," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2024.

[100] A. Ray-Dowling, *Evaluating Multi-Modality Mobile Behavioral Biometric Fusion Using Public Datasets*. Clarkson University, 2023.

[101] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Annual Norwegian computer science conference*, 2007, pp. 19–21.

[102] E. Ellavarason, R. Guest, F. Deravi, R. Sanchez-Riello, and B. Corsetti, "Touch-dynamics based behavioural biometrics on mobile devices–a review from a usability and performance perspective," *ACM Computing Surveys (CSUR)*, vol. 53, pp. 1–36, 2020.

[103] W. Liu, C. Zhang, H. Ma, and S. Li, "Learning efficient spatial-temporal gait features with deep learning for human identification," *Neuroinformatics*, vol. 16, pp. 457–471, 2018.

[104] D. Kumar and R. Verma, "A CNN-RF Hybrid Model for Cross View Gait Recognition Method using CASIA-B Cross," in *2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, 2024, pp. 156–162.

[105] J. Daugman, "New methods in iris recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, pp. 1167–1175, 2007.

[106] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, pp. 1348–1363, 1997.

[107] H. Proença and L. A. Alexandre, "Toward noncooperative iris recognition: A classification approach using multiple signatures," *IEEE transactions on pattern analysis and machine intelligence*, vol. 29, pp. 607–612, 2007.

[108] Z. G. A. Hasan, "Iris Recognition Method for Non-cooperative Images," in *International Conference on Micro-Electronics and Telecommunication Engineering*, 2023, pp. 275–288.

[109] Z. Yan, L. He, Y. Wang, Z. Sun, and T. Tan, "Flexible iris matching based on spatial feature reconstruction," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2021.

[110] M. Omran and E. N. AlShemmary, "An iris recognition system using deep convolutional neural network," in *Journal of Physics: Conference Series*, 2020, p. 012159.

[111] D. Kerrigan, M. Trokielewicz, A. Czajka, and K. W. Bowyer, "Iris recognition with image segmentation employing retrained off-the-shelf deep neural networks," in *2019 International Conference on Biometrics (ICB)*, 2019, pp. 1–7.

[112] S. Ahmad and B. Fuller, "Unconstrained iris segmentation using convolutional neural networks," in *Computer Vision–ACCV 2018 Workshops: 14th Asian Conference on Computer Vision, Perth, Australia, December 2–6, 2018, Revised Selected Papers 14*, 2019, pp. 450–466.

[113] Y. Yin, S. He, R. Zhang, H. Chang, X. Han, and J. Zhang, "Deep learning for iris recognition: a review," arXiv preprint arXiv:2303.08514, 2023.

[114] K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep learning for iris recognition: A survey," *ACM Computing Surveys*, vol. 56, pp. 1–35, 2024.

[115] K. Liang, J. Chen, T. He, W. Wang, A. K. Singh, D. B. Rawat et al., "Review of the Open Datasets for Contactless Sensing," *IEEE Internet of Things Journal*, 2024.

[116] S. Marcel and J. d. R. Millán, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE transactions on pattern analysis and machine intelligence*, vol. 29, pp. 743–752, 2007.

[117] M. Hosseinzadeh, B. Vo, M. Y. Ghafour, and S. Naghipour, "Electrocardiogram signals-based user authentication systems using soft computing techniques," *Artificial Intelligence Review*, vol. 54, pp. 667–709, 2021.

[118] J. J. Riera, T. Ogawa, T. Goto, A. Sumiyoshi, H. Nonaka, A. Evans et al., "Pitfalls in the dipolar model for the neocortical EEG sources," *Journal of neurophysiology*, vol. 108, pp. 956–975, 2012.

[119] B. Kaliappan, B. V. Sudalaiyadumperumal, and S. Thalavaipillai, "Affective analysis in machine learning using AMIGOS with Gaussian expectation-maximization model," *Int J Reconfigurable & Embedded Syst*, vol. 13, pp. 201–209, 2024.

[120] Y. Zhang, J. Chen, J. H. Tan, Y. Chen, Y. Chen, D. Li et al., "An investigation of deep learning models for EEG-based emotion recognition," *Frontiers in neuroscience*, vol. 14, p. 622759, 2020.

[121] P. Arnau-González, S. Katsigiannis, M. Arevalillo-Herráez, and N. Ramzan, "BED: A new data set for EEG-based biometrics," *IEEE Internet of Things Journal*, vol. 8, pp. 12219–12230, 2021.

[122] K. S. Priya, S. Vasanthi, R. Nithyanandhan, G. Jeyasheeli, M. Karthiga, and C. Pandi, "Blink talk: A machine learning-based method for women safety using EEG and eye blink signals," *Measurement: Sensors*, vol. 28, p. 100810, 2023.

[123] X. Zhang, L. Yao, C. Huang, T. Gu, Z. Yang, and Y. Liu, "DeepKey: A multimodal biometric authentication system via deep decoding gaits and brainwaves," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 11, pp. 1–24, 2020.

[124] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "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, pp. 977–986.

[125] Z. I. Rauen, F. Anjomshoa, and B. Kantarci, "Gesture and sociability-based continuous authentication on smart mobile devices," in *Proceedings of the 16th ACM International Symposium on Mobility Management and Wireless Access*, 2018, pp. 51–58.

[126] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE transactions on information forensics and security*, vol. 8, pp. 136–148, 2012.

[127] W. Meng, W. Li, and D. S. Wong, "Enhancing touch behavioral authentication via cost-based intelligent mechanism on smartphones," *Multimedia Tools and Applications*, vol. 77, pp. 30167–30185, 2018.

[128] L. Liu, Z. Cao, and T. Li, "FaceTouch: Practical Face Touch Detection with a Multimodal Wearable System for Epidemiological Surveillance," in *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, 2023, pp. 13–26.

[129] A. Mahfouz, H. Mostafa, T. M. Mahmoud, and A. Sharaf Eldin, "M2auth: A multimodal behavioral biometric authentication using feature-level fusion," *Neural Computing and Applications*, vol. 36, pp. 21781–21799, 2024.

[130] A. Bajaber, M. A. Fadel, and L. A. Elrefaei, "Evaluation of Deep Learning Models for Person Authentication Based on Touch Gesture," *Comput. Syst. Sci. Eng.*, vol. 42, pp. 465–481, 2022.

[131] M. L. Brocardo, I. Traore, S. Saad, and I. Woungang, "Authorship verification for short messages using stylometry," in *2013 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2013, pp. 1–6.

[132] M. Bhargava, P. Mehndiratta, and K. Asawa, "Stylometric analysis for authorship attribution on twitter," in *Big Data Analytics: Second International Conference, BDA 2013, Mysore, India, December 16–18, 2013, Proceedings 2*, 2013, pp. 37–47.

[133] M. Toshevska and S. Gievska, "A review of text style transfer using deep learning," *IEEE Transactions on Artificial Intelligence*, vol. 3, pp. 669–684, 2021.

[134] S. Almlawi, J. Fang, and J. Li, "Enhancing Sentiment Analysis Using MCNN-BRNN Model with BERT," in *2023 3rd International Conference on Electronic Information Engineering and Computer Communication (EIECC)*, 2023, pp. 574–579.

[135] G. O. Adebayo, "Multimodal stylometry: A novel approach for authorship identification," 2024.

[136] G. Bonomi, "Deep Learning Techniques for Authorship Attribution of Literary Texts: Adapting a BERT-Based Model for Analyzing Il Fiore and Detto d'Amore," ed, 2024.

[137] N. Schaetti and J. Savoy, "Comparison of Visualisable Evidence-based Authorship Attribution Methods using Recurrent Neural Networks," 2020.

[138] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," *Communications of the ACM*, vol. 33, pp. 168–176, 1990.

[139] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," 2014.

[140] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *2009 IEEE/IFIP international conference on dependable systems & networks*, 2009, pp. 125–134.

[141] O. Alpar, "Biometric keystroke barcoding: A next-gen authentication framework," *Expert Systems with Applications*, vol. 177, p. 114980, 2021.

[142] S. S. Almohamade, "Continuous authentication of users to robotic technologies using behavioural biometrics," University of Sheffield, 2022.

[143] S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *Journal of Pattern recognition research*, vol. 7, pp. 116–139, 2012.

[144] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *proceedings of the acm on interactive, mobile, wearable and ubiquitous technologies*, vol. 1, pp. 1–22, 2018.

[145] I. Sluganovic, M. Roeschlin, K. B. Rasmussen, and I. Martinovic, "Analysis of reflexive eye movements for fast replay-resistant biometric authentication," *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, pp. 1–30, 2018.

[146] M. Javed, Z. Zhang, F. H. Dahri, and A. A. Laghari, "Real-time deepfake video detection using eye movement analysis with a hybrid deep learning approach," *Electronics*, vol. 13, p. 2947, 2024.

[147] R. Zemblys, D. C. Niehorster, O. Komogortsev, and K. Holmqvist, "Using machine learning to detect events in eye-tracking data," *Behavior research methods*, vol. 50, pp. 160–181, 2018.

[148] M. Yang, Y. Gao, L. Tang, J. Hou, and B. Hu, "Wearable eye-tracking system for synchronized multimodal data acquisition," *IEEE Transactions on Circuits and Systems for Video Technology*, 2023.

[149] H. Sbeyti, "Mobile user authentication based on user behavioral pattern (MOUBE)," *International Journal of Computer Science and Security (IJCSS)*, vol. 10, p. 1, 2016.

[150] H. Gomi, S. Yamaguchi, K. Tsubouchi, and N. Sasaya, "Continuous authentication system using online activities," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 522–532.

[151] U. Mahbub, J. Komulainen, D. Ferreira, and R. Chellappa, "Continuous authentication of smartphones based on application usage," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, pp. 165–180, 2019.

[152] D. Cui, Z. Wang, P. Liu, S. Wang, Z. Zhang, D. G. Dorrell et al., "Battery electric vehicle usage pattern analysis driven by massive real-world data," *Energy*, vol. 250, p. 123837, 2022.

[153] K. Gupta, "Machine learning-based device type classification for IoT device re-and continuous authentication," 2022.

[154] M. A. Hassan, Z. Shukur, and M. K. Hasan, "An improved time-based one time password authentication framework for electronic payments," *Int. J. Adv. Comput. Sci. Appl*, vol. 11, pp. 359–366, 2020.

[155] Y.-C. Tian and J. Gao, "Network Security and Privacy Architecture," in *Network Analysis and Architecture*, Springer, 2023, pp. 361–402.

[156] D. Dasgupta, A. Roy, and A. Nag, *Advances in user authentication*. Springer, 2017.

[157] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location," *IEEE Systems Journal*, vol. 11, pp. 513–521, 2016.

[158] Y. Baseri, A. Senhaji Hafid, D. Makrakis, and H. Fereidouni, "Privacy-Preserving Federated Learning Framework for Risk-Based Adaptive Authentication," arXiv, 2025.

[159] G. Kang, J. Park, and Y.-G. Kim, "Continuous behavioral biometric authentication for secure metaverse workspaces in digital environments," *Systems*, vol. 13, p. 588, 2025.

[160] N. Al-Naffakh, N. Clarke, F. Li, and P. Haskell-Dowland, "Real-world continuous smartwatch-based user authentication," *The Computer Journal*, vol. 68, pp. 717–733, 2025.

[161] M. K. Jangir, S. K. Dayama, and P. Sundar, "HybridTouch: A Robust Framework for Continuous User Authentication by GAN-Augmented Behavioral Biometrics on Mobile Devices," *Journal of Information Technology Management*, vol. 17, pp. 108–129, 2025.

[162] R. Dave, M. Handoko, A. Rashid, and C. Schoenbauer, "From Clicks to Security: Investigating Continuous Authentication via Mouse Dynamics," arXiv, 2024.

[163] L. Wan, K. Liu, H. A. Mengash, N. Alruwais, M. Al Duhayyim, and K. Venkatachalam, "Deep learning-based photoplethysmography biometric authentication for continuous user verification," *Applied Soft Computing*, vol. 156, p. 111461, 2024.

[164] W. Shao, Z. Liang, R. Zhang, R. Fang, N. Miao, E. Kourkchi, et al., "Know Me by My Pulse: Toward Practical Continuous Authentication on Wearable Devices via Wrist-Worn PPG," arXiv, 2025.

[165] D. Aguilar, A. Martínez-Cruz, K. A. Ramírez-Gutiérrez, and M. Morales-Sandoval, "PPG-based biometric authentication: A review on architectures, datasets, attacks and security challenges," *Computational and Structural Biotechnology Journal*, vol. 28, pp. 511–528, 2025.

[166] S. M. Arman, T. Yang, S. Shahed, A. Al Mazroa, A. Attiah, and L. Mohaisen, "A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions," *Computers, Materials & Continua*, vol. 78, pp. 2087–2110, 2024.

[167] S. Jacob, P. Vinod, and V. G. Menon, "Context-aware privacy-preserving continuous authentication on mobile environments," *Security and Privacy*, vol. 8, 2025.

[168] X. X. Zheng, M. M. Ur Rahma, B. Taha, M. Masood, D. Hatzinakos, and T. Y. Al-Naffouri, "Multimodal Biometric Authentication Using Camera-Based PPG and Fingerprint Fusion," arXiv, 2024.

[169] G. H. Silva de Carvalho, D. Kaur, I. Woungang, and A. Anpalagan, "Novel Explainable CNN-LightGBM Model for Smartphone Continuous Authentication," SSRN, 2025.

[170] N. Zeeshan, M. Bakyt, N. Moradpoor, and L. La Spada, "Continuous Authentication in Resource-Constrained Devices via Biometric and Environmental Fusion," *Sensors*, vol. 25, p. 5711, 2025.

[171] W. Sheng and X. Li, "Multi-task learning for gait-based identity recognition and emotion recognition using attention enhanced temporal graph convolutional network," *Pattern Recognition*, vol. 114, p. 107868, 2021.

[172] E.-S. M. El-Kenawy, S. Mirjalili, A. A. Abdelhamid, A. Ibrahim, N. Khodadadi, and M. M. Eid, "Meta-heuristic optimization and keystroke dynamics for authentication of smartphone users," *Mathematics*, vol. 10, p. 2912, 2022.

[173] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: A qualitative study of SOC analysts' perspectives on security alarms," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 2783–2800.

[174] N. Kausar, I. U. Din, M. A. Khan, A. Almogren, and B.-S. Kim, "GRA-PIN: A graphical and PIN-based hybrid authentication approach for smart devices," *Sensors*, vol. 22, p. 1349, 2022.

[175] A. Qazi, N. Hasan, O. Abayomi-Alli, G. Hardaker, R. Scherer, Y. Sarker et al., "Gender differences in information and communication technology use & skills: a systematic review and meta-analysis," *Education and Information Technologies*, pp. 1–34, 2022.

[176] P. De Andrés, R. Gimeno, and R. M. de Cabo, "The gender gap in bank credit access," *Journal of Corporate Finance*, vol. 71, p. 101782, 2021.

[177] J. Sadik and S. Ruoti, "A Large-Scale Survey of Password Entry Practices on Non-Desktop Devices," arXiv preprint arXiv:2409.03044, 2024.

[178] T. C. Adeniran, R. G. Jimoh, E. U. Abah, N. Faruk, E. Alozie, and A. L. Imoize, "Vulnerability Assessment Studies of Existing Knowledge-Based Authentication Systems: A Systematic Review," *Sule Lamido University Journal of Science & Technology*, vol. 8, pp. 34–61, 2024.

[179] M. I. M. Yusop, N. H. Kamarudin, N. H. S. Suhaimi, and M. K. Hasan, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, 2025.

[180] S. Baseer and K. Charumathi, "Multi-Factor Authentication: A User Experience Study," Available at SSRN 4840295, 2024.

[181] J. Kim, G. Yang, J. Kim, S. Lee, K. K. Kim, and C. Park, "Efficiently updating ECG-based biometric authentication based on incremental learning," *Sensors*, vol. 21, p. 1568, 2021.

[182] E. Garea-Llano and A. Morales-Gonzalez, "Framework for biometric iris recognition in video, by deep learning and quality assessment of the iris-pupil region," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 6517–6529, 2023.

[183] S. A. Lone and A. Mir, "Smartphone-based biometric authentication scheme for access control management in client-server environment," *Int J Inf Technol Comput Sci*, vol. 14, pp. 34–47, 2022.

[184] I. L. Furuberg and M. Øseth, "From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication," NTNU, 2023.

[185] S. An, C. F. Cheung, and K. W. Willoughby, "A gamification approach for enhancing older adults' technology adoption and knowledge transfer: A case study in mobile payments technology," *Technological Forecasting and Social Change*, vol. 205, p. 123456, 2024.

[186] A. P. Umejiaku, P. Dhakal, and V. S. Sheng, "Balancing password security and user convenience: Exploring the potential of prompt models for password generation," *Electronics*, vol. 12, p. 2159, 2023.

[187] P. P. Surve, O. Brodt, M. Yampolskiy, Y. Elovici, and A. Shabtai, "SoK: Security Below the OS–A Security Analysis of UEFI," arXiv preprint arXiv:2311.03809, 2023.

[188] B. T. Alabdulwahab, "The Meaning, Development and Evaluation of Natural User Interface in Education: An Empirical Study with Pen-Based Interaction," 2024.

[189] O. Inverso, E. Tomasco, B. Fischer, S. La Torre, and G. Parlato, "Bounded verification of multi-threaded programs via lazy sequentialization," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 44, pp. 1–50, 2021.

[190] N. Karim, H. Kanaker, W. Abdulraheem, M. Ghaith, E. Alhroob, and A. Alali, "Choosing the right MFA method for online systems: A comparative analysis," *International Journal of Data and Network Science*, vol. 8, pp. 201–212, 2024.

[191] D. Nguyen and B. Beijnon, "The data subject and the myth of the 'black box' data communication and critical data literacy as a resistant practice to platform exploitation," *Information, Communication & Society*, vol. 27, pp. 333–349, 2024.

[192] D. Harauzek, "Cloud Computing: Challenges of cloud computing from business users perspective-vendor lock-in," ed, 2022.

[193] Z. Sun, Q. Li, Y. Liu, and Y. Zhu, "Opportunities and challenges for biometrics," *China's e-Science Blue Book 2020*, pp. 101–125, 2021.

[194] M. Fourné, "Human Factors in Open Source Security," Universitätsbibliothek, 2024.

[195] P. Jain, H. Pötter, A. J. Lee, and D. Mósse, "Mafia: Multi-layered architecture for iot-based authentication," in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2020, pp. 199–208.

[196] N. A. Karim, O. A. Khashan, H. Kanaker, W. K. Abdulraheem, M. Alshinwan, and A.-K. Al-Banna, "Online banking user authentication methods: a systematic literature review," *Ieee Access*, vol. 12, pp. 741–757, 2023.

[197] C. Dong, F. Jiang, S. Chen, and X. Liu, "Continuous authentication for uav delivery systems under zero-trust security framework," in *2022 IEEE International Conference on Edge Computing and Communications (EDGE)*, 2022, pp. 123–132.

[198] R. Vasudev, N. Harini, and M. Neethu, "Multi-Factor Authentication System With ID Card Credentials For Secure Transactions," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1–8.

[199] M. Fanti, *Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA*. 2023.

[200] A. Muir, K. Brown, and A. Girma, "Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks," in *Proceedings of the Future Technologies Conference*, 2024, pp. 597–607.

[201] R. Kovač, "Threat Report T22021," 2021.

[202] V. Business, "2024 Data Breach Investigations Report," 2024.

[203] A. Vempati, "Analyzing the Nexus between Cyberaggression and Cybersecurity Insider Threat Dynamics," Purdue University, 2024.

[204] M. N. Al-Mhiqani, R. Ahmad, Z. Zainal Abidin, W. Yassin, A. Hassan, K. H. Abdulkareem et al., "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," *Applied Sciences*, vol. 10, p. 5208, 2020.

[205] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an improved understanding of human factors in cybersecurity," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, 2019, pp. 338–345.

[206] U. Rauf, F. Mohsen, and Z. Wei, "A taxonomic classification of insider threats: Existing techniques, future directions & recommendations," *Journal of Cyber Security and Mobility*, vol. 12, pp. 221–252, 2023.

[207] H. İ. Aslan and C. Choi, "VisGIN: Visibility graph neural network on one-dimensional data for biometric authentication," *Expert Systems with Applications*, vol. 237, p. 121323, 2024.

[208] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *Journal of Information Security and Applications*, vol. 82, p. 103748, 2024.

[209] E. C. P. Neto, H. Taslimasa, S. Dadkhah, S. Iqbal, P. Xiong, T. Rahman et al., "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," *Internet of Things*, vol. 26, p. 101209, 2024.

[210] E. Ritter, "Your Voice Gave You Away: The Privacy Risks of Voice-Inferred Information," *Duke LJ*, vol. 71, p. 735, 2021.

[211] W. Lee, J. J. Seong, B. Ozlu, B. S. Shim, A. Marakhimov, and S. Lee, "Biosignal sensors and deep learning-based speech recognition: A review," *Sensors*, vol. 21, p. 1399, 2021.

[212] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," *Risk Management*, vol. 22, pp. 239–309, 2020.

[213] J. L. Kröger, L. Gellrich, S. Pape, S. R. Brause, and S. Ullrich, "Personal information inference from voice recordings: User awareness and privacy concerns," *Proceedings on Privacy Enhancing Technologies*, 2022.

[214] I. B. A. Ouahab, L. Elaachak, M. Bouhorma, Y. A. Alluhaidan, and B. Zafar, "Voice Biometric Technology: Enhancing Public Safety and Security in Smart Cities," in *2024 Mediterranean Smart Cities Conference (MSCC)*, 2024, pp. 1–6.

[215] A. B. Rubin, "A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine," *Rich. JL & Tech.*, vol. 27, p. 1, 2020.

[216] A. Gallardo, C. Choy, J. Juneja, E. Bozkir, C. Cobb, L. Bauer et al., "Speculative privacy concerns about AR glasses data collection," *Proceedings on Privacy Enhancing Technologies*, 2023.

[217] R. V. Petrescu, "Face recognition as a biometric application," *Journal of Mechatronics and Robotics*, vol. 3, p. 237.257, 2019.

[218] T.-K. Ghazali and N.-H. Zakaria, "Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment," *Journal of Computers (Taiwan)*, 2018.

[219] P. Piccolotto and P. Maller, "BIOMETRICS FROM THE USER POINT OF VIEW: DERIVING DESIGN PRINCIPLES FROM USER PERCEPTIONS AND CONCERNS ABOUT BIOMETRIC SYSTEMS," *Intel Technology Journal*, vol. 18, 2014.

[220] D. Sethi, S. Bharti, and C. Prakash, "A comprehensive survey on gait analysis: History, parameters, approaches, pose estimation, and future work," *Artificial Intelligence in Medicine*, vol. 129, p. 102314, 2022.

[221] E. J. Harris, I.-H. Khoo, and E. Demircan, "A survey of human gait-based artificial intelligence applications," *Frontiers in Robotics and AI*, vol. 8, p. 749274, 2022.

[222] M. L. Shuwandy, A. Jouda, M. Ahmed, M. M. Salih, Z. Al-qaysi, A. Alamoodi et al., "Sensor-Based Authentication in Smartphone; a Systematic Review," *Journal of Engineering Research*, 2024.

[223] S. Park and G. Ryu, "Motion-Based User Authentication for Enhanced Metaverse Security," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 34, pp. 493–503, 2024.

[224] A. Z. Zaidi, C. Y. Chong, Z. Jin, R. Parthiban, and A. S. Sadiq, "Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 191, p. 103162, 2021.

[225] G. Cho, S. Kwag, J. H. Huh, B. Kim, C.-H. Lee, and H. Kim, "Towards usable and secure location-based smartphone authentication," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021, pp. 1–16.

[226] A. Alabdulatif, R. Samarasinghe, and N. N. Thilakarathne, "A Novel Robust Geolocation-Based Multi-Factor Authentication Method for Securing ATM Payment Transactions," *Applied Sciences*, vol. 13, p. 10743, 2023.

[227] I. Ullah, D. Adhikari, H. Khan, M. S. Anwar, S. Ahmad, and X. Bai, "Mobile robot localization: Current challenges and future prospective," *Computer Science Review*, vol. 53, p. 100651, 2024.

[228] A. G. Martín, M. Beltrán, A. Fernández-Isabel, and I. M. de Diego, "An approach to detect user behaviour anomalies within identity federations," *computers & security*, vol. 108, p. 102356, 2021.

[229] O. Olukoya, "Assessing frameworks for eliciting privacy & security requirements from laws and regulations," *Computers & Security*, vol. 117, p. 102697, 2022.

[230] G. Reshma, B. Prasanna, H. N. Murthy, T. Murthy, S. Parthiban, and M. Sangeetha, "Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment," *Soft Computing*, pp. 1–20, 2023.

[231] P. Khanpara, K. Lavingia, R. Trivedi, S. Tanwar, A. Verma, and R. Sharma, "A context-aware internet of things-driven security scheme for smart homes," *Security and Privacy*, vol. 6, p. e269, 2023.

[232] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art," *Cluster Computing*, vol. 19, pp. 455–474, 2016.

[233] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "LCDA: lightweight continuous device-to-device authentication for a zero trust architecture (ZTA)," *Computers & Security*, vol. 108, p. 102351, 2021.

[234] S. G. Persiani, B. Kobas, S. C. Koth, and T. Auer, "Biometric data as real-time measure of physiological reactions to environmental stimuli in the built environment," *Energies*, vol. 14, p. 232, 2021.

[235] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, “Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations,” *Journal of network and computer applications*, vol. 209, p. 103540, 2023.

[236] S. M. Amft, “On the usability of authentication security communication,” 2024.

[237] S. Gupta, C. Maple, B. Crispo, K. Raja, A. Yautsiukhin, and F. Martinelli, “A survey of human-computer interaction (HCI) & natural habits-based behavioural biometric modalities for user recognition schemes,” *Pattern Recognition*, vol. 139, p. 109453, 2023.

[238] G. Zhao, Y. Jiao, J. Zhuo, Y. Chen, C. Ju, and Y. Wang, “Continuous Authentication of Smartphones Based on Screen-Touch Trajectories,” *Journal of Networking and Network Applications*, vol. 4, pp. 102–108, 2024.

[239] B. Ying, N. R. Mohsen, and A. Nayak, “Efficient authentication protocol for continuous monitoring in medical sensor networks,” *IEEE Open Journal of the Computer Society*, vol. 2, pp. 130–138, 2021.

[240] P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom, and H. Olufowobi, “Survey of interoperability challenges in the internet of vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 22838–22861, 2022.

[241] A. Ali, “Securing IoT connectivity: The role of Multi-Factor Authentication (MFA) in strengthening Cyber defense,” ed, 2022.

[242] I. Gharbi, F. Taia-Alaoui, H. Fourati, N. Vuillerme, and Z. Zhou, “Transportation Mode Detection Using Learning Methods and Self-Contained Sensors,” *Sensors*, vol. 24, p. 7369, 2024.

[243] A. A. Bangash, “Cost-effective Strategies to Develop Energy-Efficient Mobile Applications,” 2023.

[244] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, “Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions,” *Information Fusion*, vol. 102, p. 102060, 2024.

[245] R. Zahid, A. Altaf, T. Ahmad, F. Iqbal, Y. A. M. Vera, M. A. L. Flores et al., “Secure data management life cycle for government big-data ecosystem: Design and development perspective,” *Systems*, vol. 11, p. 380, 2023.

[246] S. Aftabjahani, R. Kastner, M. Tehranipoor, F. Farahmandi, J. Oberg, A. Nordstrom et al., “Special session: Cad for hardware security-automation is key to adoption of solutions,” in *2021 IEEE 39th VLSI Test Symposium (VTS)*, 2021, pp. 1–10.

[247] P. M. A. B. Estrela, R. d. O. Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. d. S. Júnior, “A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications,” *Sensors*, vol. 21, p. 4212, 2021.

[248] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, “An overview of privacy-enhancing technologies in biometric recognition,” *ACM Computing Surveys*, vol. 56, pp. 1–28, 2024.

[249] S. Fleury and N. Chaniaud, “Multi-user centered design: acceptance, user experience, user research and user testing,” *Theoretical Issues in Ergonomics Science*, vol. 25, pp. 209–224, 2024.