International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Continuous User Authentication on Mobile Devices

Chris Gilbert[1], Mercy Abiola Gilbert[2]
[1]Professor, Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University/chrisgilbertp@gmail.com/cabilimi@tubmanu.edu.lr
[2]Instructor, Department of Guidance and Counseling/College of Education/William V.S. Tubman University/mercyabiola92@gmail.com/moke@tubmanu.edu.lr

Abstract— *With mobile devices playing an increasingly central role in everyday life, securing them without making things difficult for users is more important than ever. Traditional methods like passwords, Personal Identification Numbers (PINs), or patterns are limited: they require user effort, can be cumbersome on small screens, and don't adapt to changes in how or where devices are used. Continuous user authentication (CUA) offers a new way forward. Instead of relying on a single login event, CUA continuously monitors how users interact with their devices—such as the way they type, swipe, or move—to verify their identity on the fly. This reduces the amount of time a device stays unlocked without re-checking that's using it, helping prevent unauthorized access.In this paper, we explore how CUA can blend various biometric signals, behavioral data, and contextual cues to create more adaptive, efficient, and user-friendly security measures. We discuss different biometric approaches, show why flexible and incremental modeling is important, and explain how privacy-preserving techniques can protect user data. We also highlight the need for common benchmarks and standards, as well as collaboration across technical, legal, and usability fields, so that CUA systems are not only safe and accurate, but also respectful of user privacy and easy to use. Our findings and recommendations aim to guide researchers, developers, and policymakers toward continuous authentication methods that truly fit the evolving mobile environment.*

Keywords— *Continuous user authentication, behavioral biometrics, mobile security, user-centered authentication, contextual cues, incremental learning, privacy preservation, biometric benchmarking, adaptive thresholds, human-device interaction.*

I. INTRODUCTION

The rapid proliferation of mobile devices has underscored the pressing need to ensure robust security measures without compromising usability (Hassan et al., 2024). Traditional authentication methods—such as passwords, PINs, or pattern locks—present several shortcomings in this regard. They are heavily reliant on explicit user input, which can be cumbersome on small screens, and often fail to adapt to the dynamic conditions inherent in mobile usage. As a result, users frequently encounter periodic logins that not only prove intrusive but also create vulnerabilities, as adversaries can exploit intervals when the device remains accessible without re-authentication (Jaime et al., 2023; Gilbert & Gilbert, 2024a).

In recent years, researchers have explored a wide array of strategies to address these limitations. Biometrics-based methods, including keystroke dynamics (Islam, 2023; Gilbert & Gilbert, 2024c), facial recognition (Fontem, 2024; Gilbert & Gilbert, 2024b), and voice-based authentication (Allioui & Mourdi, 2023; Gilbert & Gilbert, 2024d), have attracted considerable attention. Such approaches leverage innate or behavioral characteristics to streamline authentication processes and enhance user experience. Empirical studies show that these biometric methods can reduce the frequency of manual logins, improve recognition accuracy, and lower error rates (Mallick & Nath, 2024; Gilbert & Gilbert, 2024e). However, challenges persist. Environmental factors, sensor variability, evolving user behavior, and concerns over privacy and user acceptance necessitate ongoing refinement of these techniques (Islam, 2023). The literature indicates that while biometrics can mitigate reliance on traditional passwords, a robust solution demands continuous verification that seamlessly integrates into the user's natural interaction patterns (Hassan et al., 2024; Gilbert & Gilbert, 2024f).

Building on these insights, this work explores continuous user authentication (CUA) on mobile devices. Our aim is to reduce dependence on fixed login events and minimize the "exposure time"—the interval during which a device remains accessible without re-authenticating the user. By adopting a continuous monitoring approach grounded in behavioral biometrics (e.g., keystroke patterns), we strive to create a more adaptive, transparent, and efficient authentication framework (Jaime et al., 2023; Gilbert & Gilbert, 2024g). Specifically, this paper sets out to:

I. Propose a CUA mechanism that incorporates keystroke-based behavioral biometrics with minimal user intrusion.
II. Demonstrate how continuous authentication can effectively decrease exposure time, thus lowering the risk of unauthorized access.
III. Examine how continuous authentication can function in tandem with existing security measures, reinforcing overall device protection.

By doing so, this study contributes to the broader discourse on mobile security and delivers insights that can inform the design, implementation, and refinement of effective CUA systems for an evolving digital landscape.

The diagram illustrates the transition from traditional authentication methods to the emergence of Continuous User Authentication (CUA) by addressing key challenges, benefits, and its adoption across industries. Traditional methods, such as passwords, face significant shortcomings, including security vulnerabilities like phishing and user experience issues, such as forgotten credentials. These limitations have paved the way for CUA, a more dynamic approach that continuously verifies user identity during device interactions. CUA offers notable benefits, including enhanced security through real-time monitoring and an improved user experience by reducing reliance on static passwords. However, its adoption depends

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

heavily on user acceptance and trust. Industries such as finance, healthcare, and e-commerce stand out as key sectors where CUA can add substantial value, reinforcing security and improving usability. Despite its potential, CUA is not without challenges. Privacy concerns related to continuous data collection and the complexity of integrating such systems into existing infrastructures are significant barriers. Addressing these challenges requires a feedback loop that refines the system based on user trust, acceptance, and operational performance. This iterative process ensures that CUA evolves into a robust and widely accepted solution for modern authentication needs.

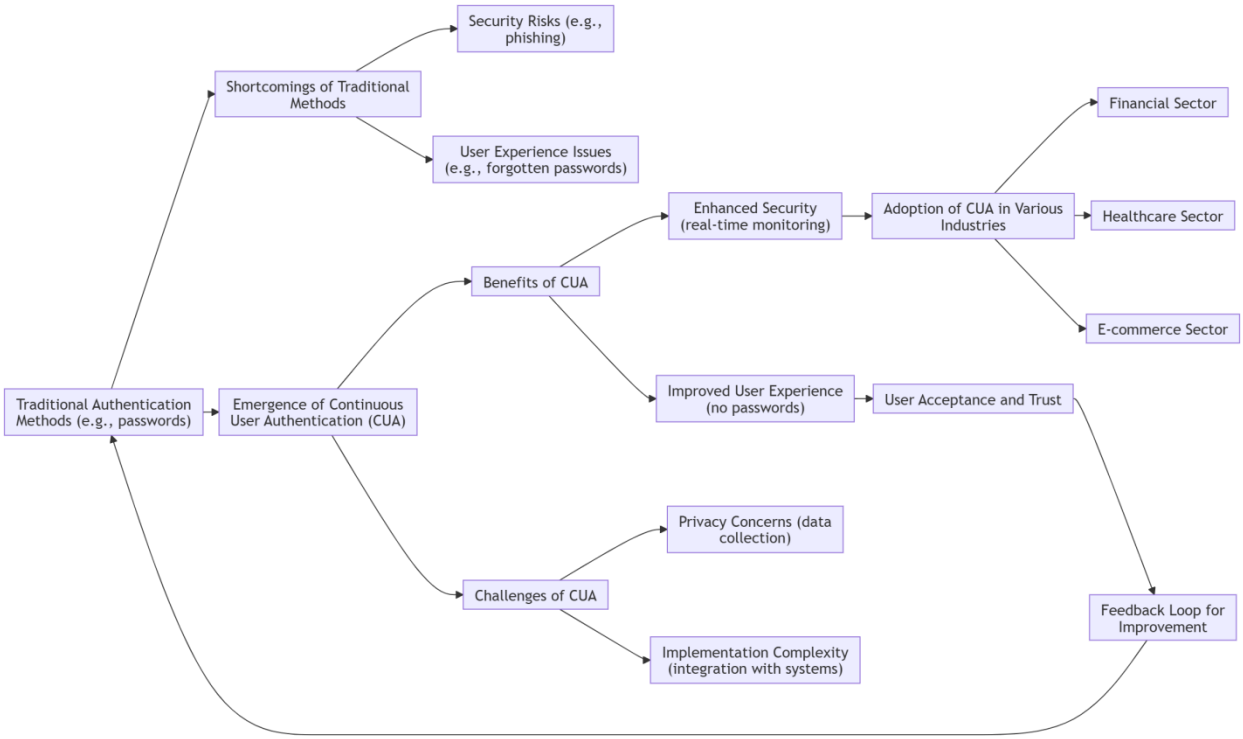

Figure 1: Evolution from passwords to continuous user authentication.

II. The Need for Continuous User Authentication

The critical importance of continuous authentication becomes evident when considering the volume of sensitive data stored on mobile devices and the frequency with which these devices are shared among multiple users (Stylios et al., 2021; Gilbert & Gilbert, 2024i). According to a recent industry report by Verizon (Fontem, 2024; Gilbert & Gilbert, 2024h), 79% of IT professionals perceive mobile devices as potential security risks, emphasizing the urgency of more adaptive and persistent safeguards.

Central to our approach is the concept of exposure time—the duration a device remains accessible following an initial login, without additional verification. Studies in continuous authentication have shown that reducing this interval can significantly lower the potential attack surface (Hassan et al., 2024; Gilbert & Gilbert, 2024k). By continuously verifying a user's identity through subtle behavioral cues, such as typing cadence or application interaction patterns, CUA seeks to shrink exposure time toward zero. For instance, if a user's interaction deviates markedly from established behavioral profiles, the system can initiate a re-authentication prompt or restrict access, preempting unauthorized use (Jimmy, 2024; Gilbert & Gilbert, 2024j).

Moreover, CUA complements existing security solutions. Traditional measures—ranging from application-level protections to OS hardening and encryption—focus on securing the environment and data at rest or in transit. Continuous authentication adds another layer by monitoring the user's identity dynamically (Shafik, 2024; Gilbert & Gilbert, 2024n). Empirical findings suggest that integrating CUA with these measures can detect anomalies more effectively; thwarting unauthorized actions even when the underlying system components remain uncompromised (Olweny, 2024; Gilbert & Gilbert, 2024l). Ultimately, this synergy aligns with industry priorities and responds to the complex security demands of modern mobile ecosystems.

In essence, continuous user authentication is neither a stand-alone fix nor an incremental improvement; it is a foundational shift that emphasizes ongoing user verification. By ensuring that only the rightful owner continues to interact with the device, CUA enhances user trust, mitigates risks, and offers a scalable, user-centered approach to mobile security (Obi et al., 2024; Gilbert & Gilbert, 2024m).

The pie chart illustrates the distribution of challenges associated with implementing Continuous User Authentication (CUA) systems. The largest segment, accounting for 43%, highlights privacy concerns, emphasizing issues related to continuous data collection and storage.

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

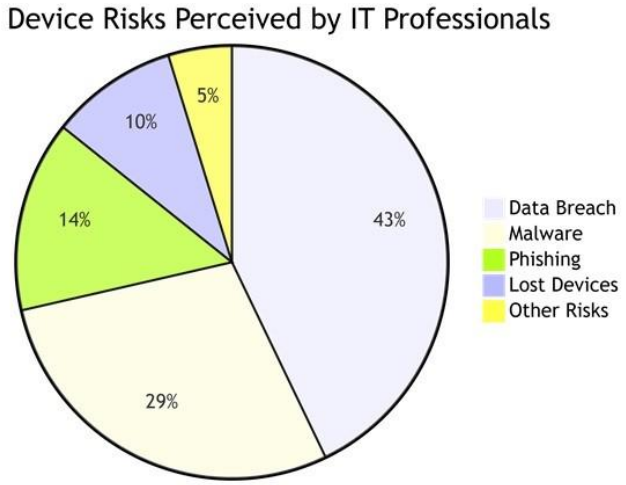

Figure 2: Mobile device risk perceptions by IT professionals.

This demonstrates the critical need to address data protection and user trust. The second-largest portion, 29%, represents integration challenges. This reflects the technical difficulties of incorporating CUA into existing systems and infrastructure, which often require significant adjustments and interoperability efforts. Another 14% pertains to user acceptance barriers, underscoring the importance of ensuring that users are comfortable with and trust CUA systems. This involves addressing concerns about intrusiveness and transparency. The remaining segments are divided between performance issues (10%), which relate to the reliability and accuracy of authentication processes, and legal compliance requirements (5%), reflecting the need to meet regulatory standards such as GDPR and HIPAA. Together, these factors underscore the complexity of deploying CUA solutions, highlighting the need for a balanced approach that considers technical performance, user experience, privacy, and regulatory compliance.

III. Research Methodologies

This body of research adopts a multifaceted methodological framework that integrates biometric analysis, machine learning, behavioral modeling, and privacy-preserving techniques. The overarching aim is to establish authentication systems on mobile devices that operate continuously, remain minimally intrusive, and adapt to dynamic user and environmental conditions.

I. Biometric Modalities and Continuous Verification Approaches:

The study contrasts classic biometric methods, which rely on periodic verification through static biometric samples (e.g., a single fingerprint scan or a captured facial image), with feature-based approaches, which continuously extract and analyze evolving biometric or behavioral attributes. Biometric indicators range from fingerprint recognition (including integration with motion sensors and exploration of touchless techniques) to facial and iris recognition methods that incorporate advanced modeling (3D structures, thermal patterns) and robust segmentation algorithms. Each modality is examined in light of accuracy, susceptibility to environmental factors, computational overhead, and user convenience (Gupta, Buriro & Crispo, 2018; Gilbert & Gilbert, 2024o).

II. Behavioral Biometrics and Implicit Authentication Frameworks:

Moving beyond static credentials such as passwords or PINs, the research emphasizes behavioral biometrics—touch gestures, keystroke rhythms, application usage patterns, and navigation habits—as continuous, unobtrusive signals. The proposed architecture involves data pre-processing and normalization to account for device heterogeneity; feature extraction to identify discriminative behavioral traits (e.g., gesture curvature, typing latency); and incremental modeling, wherein machine learning or deep learning algorithms adapt a user's behavioral profile over time. Adaptive decision thresholding is introduced to dynamically refine authentication criteria based on real-time feedback, ensuring timely responses to anomalous behavior (Dahia, Jesus & Pamplona Segundo, 2020).

III. Context-Aware Authentication Mechanisms:

Recognizing that user interactions do not occur in isolation, the study incorporates contextual factors—including device orientation, location, movement patterns, and ambient conditions—into authentication models. By applying machine learning-based activity recognition (e.g., random forest classifiers) to sensor data, the system modulates authentication rigor according to the complexity or uncertainty of the prevailing context. The methodology underscores the need for standardized datasets, well-defined performance benchmarks (e.g., EER, accuracy percentages), and transparent comparison protocols to facilitate reproducibility and cumulative knowledge building (The et al., 2016; Gilbert & Gilbert, 2024o).

IV. Privacy, Ethics, and Regulatory Compliance:

Given that continuous authentication techniques require ongoing data collection, the methodologies place significant emphasis on ethical and privacy considerations. Informed consent, anonymization, data minimization, and compliance with frameworks like GDPR are integrated into the design process. Proposed solutions advocate for the incorporation of privacy-by-design principles, secure enclaves, differential privacy, and federated learning approaches to prevent data misuse and bolster user trust (Gonzalez-Manzano, Fuentes & Ribagorda, 2019).

V. Evaluative Strategies, Benchmarking, and Longitudinal Studies:

To rigorously assess proposed solutions, the research encourages comprehensive user studies, employing both controlled experiments and field deployments that simulate various attack scenarios (e.g., mimicry attempts, insider threats). By advocating for the creation of standardized benchmarks and shared datasets, the methodologies aim to establish baseline performance metrics. Comparisons against these benchmarks enable the community to discern meaningful improvements, validate new approaches, and identify avenues

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

for refinement. Such longitudinal evaluations reveal how authentication mechanisms respond to evolving user behavior, changes in environmental conditions, and the introduction of novel sensor modalities (Al-Naji & Zagrouba, 2020; Gilbert & Gilbert, 2024p; Opoku-Mensah, Abilimi & Boateng, 2013).

VI. Interdisciplinary Collaboration and Real-World Application:

Recognizing the complexity of continuous authentication, the methodologies underscore the value of collaborations with industry partners, hardware manufacturers, operating system developers, and policy experts. These partnerships facilitate real-world deployments on prototype devices, generating insights into performance under resource constraints (battery life, processing overhead) and guiding iterative enhancements. Engagement with standardization bodies and interdisciplinary working groups helps establish consistent evaluation frameworks and fosters consensus on best practices (Hernández-Álvarez et al., 2020; Gilbert & Gilbert, 2024q).

In sum, the methodologies detailed across this research portfolio present a holistic and evolving toolkit for realizing continuous, context-aware, and behaviorally informed mobile authentication solutions. They call for synergy between technical rigor and ethical stewardship, standardization efforts, user-centric evaluations, and interdisciplinary discourse to meet the security, usability, and privacy demands of contemporary mobile ecosystems.

TABLE 1: Research Methodologies

Aspect	Description
Biometric Modalities and Continuous Verification Approaches	Contrasts static verification methods (e.g., single fingerprint scan) with continuous feature-based methods. Covers biometric indicators like fingerprint recognition, facial recognition, and iris recognition. Examines factors such as accuracy, environmental susceptibility, computational overhead, and user convenience.
Behavioral Biometrics and Implicit Authentication Frameworks	Focuses on unobtrusive signals like touch gestures, keystroke rhythms, and application usage. Involves data pre-processing, feature extraction, incremental modeling, and adaptive decision thresholding to refine real-time responses.
Context-Aware Authentication Mechanisms	Incorporates contextual data (e.g., device orientation, location, movement, ambient conditions) using machine learning-based activity recognition. Highlights the need for standardized datasets and performance benchmarks.
Privacy, Ethics, and Regulatory Compliance	Emphasizes ethical considerations like informed consent, anonymization, data minimization, and compliance with regulations (e.g., GDPR). Advocates privacy-by-design principles and advanced privacy-preserving techniques (e.g., federated learning).
Evaluative Strategies, Benchmarking, and Longitudinal Studies	Promotes rigorous assessment through user studies, controlled experiments, and field deployments. Encourages development of standardized benchmarks and shared datasets for meaningful comparisons and refinement of authentication mechanisms.
Interdisciplinary Collaboration and Real-World Application	Stresses collaboration with industry, hardware manufacturers, OS developers, and policy experts for real-world deployments. Supports iterative enhancements, consistent evaluation frameworks, and consensus on best practices.

This table provides a structured summary of the methodological framework for developing and evaluating Continuous User Authentication (CUA) systems.

IV. Biometric-Based Approaches

Biometric-based continuous user authentication (CUA) methods utilize unique physiological or behavioral characteristics to verify identity over time. By continuously analyzing attributes such as fingerprint patterns, facial features, or iris textures, these approaches aim to reduce user reliance on manual logins and improve overall security and convenience (Sailema, Olivares & Delicado, 2022). Current research generally divides biometric-based CUA into two categories: (1) classic approaches, which rely on static snapshots or samples at fixed intervals, and (2) feature-based approaches, which dynamically extract evolving behavioral attributes from ongoing user interactions (Hussain, 2021). Such distinctions are crucial because feature-based methods often adapt better to changes in user behavior and environmental conditions, potentially increasing long-term system reliability.

Despite their promise, biometric modalities differ significantly in terms of accuracy, robustness, and usability. For example, while fingerprints are relatively stable and well-understood, environmental factors like moisture or sensor quality can affect recognition accuracy (Huan et al., 2020; Gilbert & Gilbert, 2024t). Facial recognition, though convenient and hands-free, may struggle under poor lighting conditions or with substantial variations in user appearance (Nag, 2019; Gilbert & Gilbert, 2024u). Iris recognition excels in terms of stability and distinctiveness, yet requires careful image acquisition and may be sensitive to user positioning (Zhang et al., 2017; Gilbert & Gilbert, 2024s). Comparative studies have shown that performance trade-offs often depend on application scenarios: devices that require rapid, hands-free verification may favor facial or iris-based methods, while those necessitating precise identification in variable conditions might lean toward fingerprint-based solutions (Ayeswarya & Norman, 2019; Gilbert & Gilbert, 2024r).

In addition, the field has yet to reach consensus on standardized evaluation protocols. Common datasets, performance benchmarks (such as Equal Error Rate or False Acceptance/False Rejection Rates), and environmental testing conditions would facilitate direct comparisons and guide practitioners in modality selection. Preliminary efforts in this direction include international competitions and open datasets for face and fingerprint recognition (Ayeswarya & Singh, 2024), but similar benchmarking resources for continuous, multi-modal CUA remain limited.

Fingerprint Recognition

Fingerprint recognition has long been a cornerstone of biometric authentication due to its high uniqueness and user familiarity. Classic approaches prompt fingerprint scans periodically, verifying the user's identity each time the device is accessed. This practice can be inconvenient in contexts demanding continuous verification. Feature-based strategies address this issue by integrating adaptive thresholds and signal processing techniques, enabling the system to refine the user's

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

fingerprint profile over time and reduce the reliance on frequent scanning (SHAKIR, 2020; Gilbert & Gilbert, 2024u).

Challenges persist in dealing with varying sensor quality, environmental conditions, and noise. To address these, researchers have introduced frameworks conceptually similar to “MobileTouch” and “Accel-UC” (Lawrence, 2024; Gilbert & Gilbert, 2024v), where accelerometer or gyroscope readings are combined with fingerprint data to capture richer interaction patterns. Benchmarking efforts, such as those reported by the FVC (Fingerprint Verification Competition) series (Ayeswarya, & Singh, 2024; Gilbert & Gilbert, 2024w), provide standardized datasets and performance metrics. However, continuous authentication scenarios require further methodological consensus, including testing with longitudinal datasets and simulating real-world conditions.

Touchless fingerprint techniques represent another promising frontier. Leveraging device cameras and integrated motion sensors, they initiate fingerprint capture only when user presence is detected, thereby enhancing both usability and security. Although preliminary experiments have shown encouraging results, rigorous comparative evaluations and standard benchmarks are needed to ensure that touchless solutions match or exceed the reliability of traditional fingerprint readers (Lawrence, 2024; Gilbert, Oluwatosin & Gilbert, 2024).

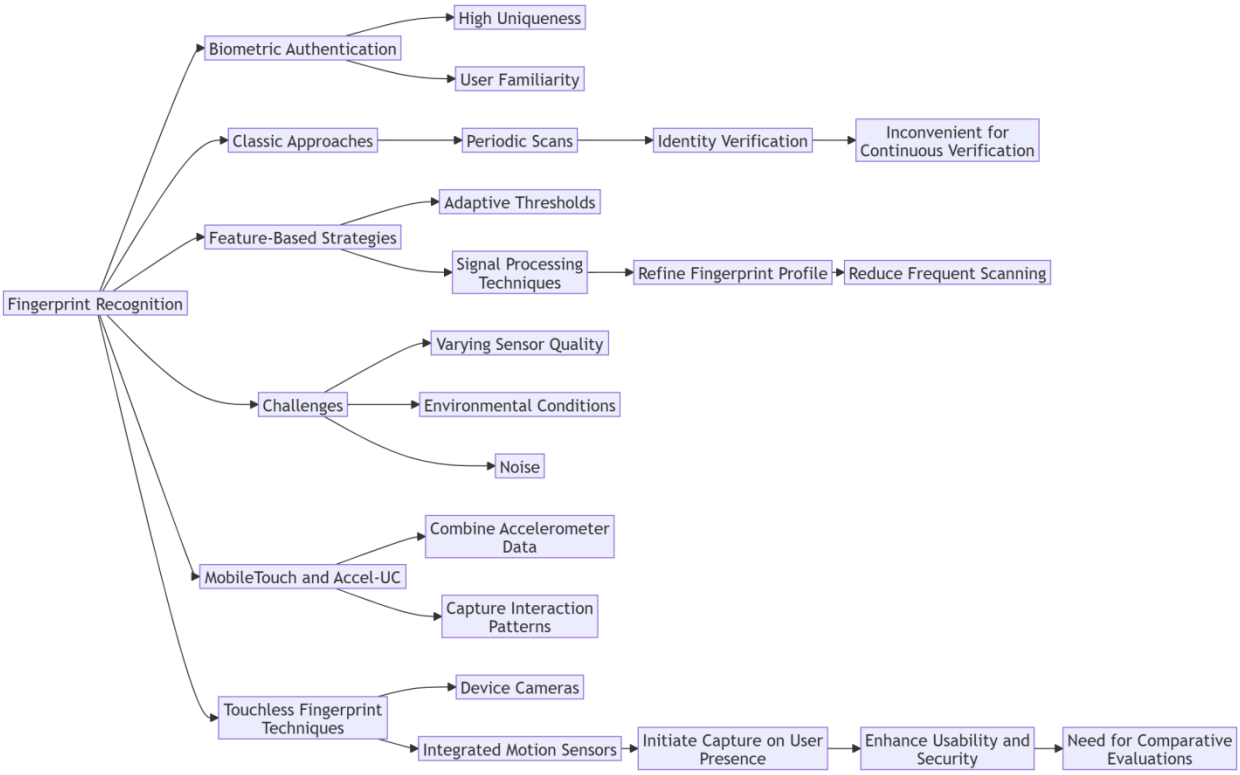

Figure 3: Fingerprint recognition methods and their challenges.

The diagram provides a detailed perspective on fingerprint recognition within the context of biometric authentication, focusing on its strengths, approaches, challenges, and advancements. Fingerprint recognition stands out for its high uniqueness and familiarity to users, making it a widely trusted biometric method. Traditional approaches rely on periodic scans to verify identity, but these can be inconvenient for continuous authentication. To address this, feature-based strategies have been developed, utilizing adaptive thresholds and signal processing techniques to refine fingerprint profiles, thereby reducing the need for frequent scans.

However, several challenges persist, such as variations in sensor quality, environmental conditions, and noise, all of which can affect accuracy and reliability. Innovations have sought to overcome these obstacles, with systems like MobileTouch and Accel-UC combining accelerometer data to capture richer interaction patterns. Furthermore, touchless fingerprint techniques leverage device cameras and integrated motion sensors to initiate fingerprint capture based on user presence, enhancing both usability and security.

Despite these advancements, there is a growing need for comparative evaluations to validate the effectiveness of these newer methods against traditional approaches. The progression of fingerprint recognition from static verification to more adaptive, seamless methods highlights its potential to meet the demands of continuous user authentication.

Facial Recognition

Facial recognition is inherently appealing due to its non-intrusive nature and the ubiquity of front-facing cameras on mobile devices. Classic methods rely on periodic image snapshots, but feature-based approaches incorporate richer data—such as 3D facial modeling, texture descriptors, and thermal mapping—to achieve more robust and continuous

verification (Patidar et al., 2024). These enhancements help distinguish genuine users from imposters using photographs, masks, or deepfake-style spoofing attempts (Pradeep Kumar, 2023; Abilimi & Yeboah, 2013; Gilbert, Auodo & Gilbert, 2024).

Still, facial recognition must contend with variable lighting, changes in user appearance, and privacy concerns. Studies have reported performance degradation in low-light scenarios and when users change hairstyles, wear glasses, or grow facial hair. Privacy-preserving techniques like homomorphic encryption and differential privacy (Kumar, 2023) are under exploration to ensure that raw facial data cannot be misused. Standardized facial recognition benchmarks (example, LFW (Kumar, 2023), IJB-C (Patidar et al., 2024; Gilbert, 2021), exist, but they generally target static verification rather than continuous monitoring. Establishing dedicated continuous authentication benchmarks and protocols would help quantify improvements in adaptive facial recognition algorithms over time.

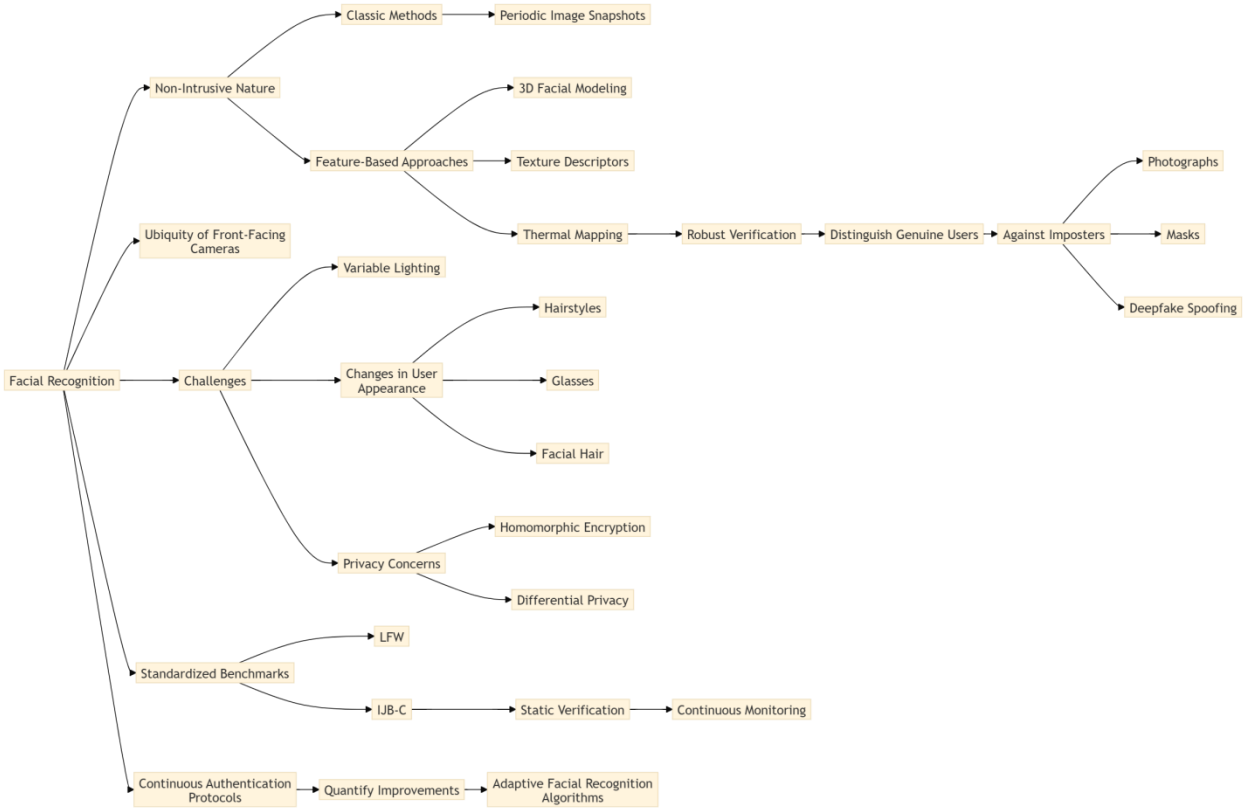

Figure 4: Facial recognition process and challenges overview

The diagram illustrates the key aspects, challenges, and advancements in facial recognition technology, particularly for biometric authentication. Facial recognition is valued for its non-intrusive nature and the widespread availability of front-facing cameras on mobile devices. Traditional, or classic, methods involve periodic image snapshots, which have limitations in dynamic environments. More advanced, feature-based approaches incorporate 3D facial modeling, texture descriptors, and thermal mapping. These improvements enhance verification robustness, enabling systems to distinguish genuine users from imposters who might use photographs, masks, or even deepfake techniques for spoofing.

Despite its advantages, facial recognition faces several challenges. Variable lighting conditions and changes in user appearance—such as differences in hairstyles, wearing glasses, or facial hair—can affect accuracy and reliability. Additionally, privacy concerns are a major issue, prompting the adoption of privacy-preserving techniques like homomorphic encryption and differential privacy to protect user data.

To improve facial recognition systems, standardized benchmarks such as LFW and IJB-C have been developed. These benchmarks are used to evaluate and compare performance in static verification scenarios. However, there is a need to extend these efforts to continuous monitoring systems, which require adaptive facial recognition algorithms. Such advancements would enable better quantification of improvements and foster the creation of reliable continuous authentication protocols that can seamlessly operate under diverse and evolving conditions.

Iris Recognition

Iris recognition capitalizes on the stable, intricate patterns formed in early fetal development that remain largely unchanged throughout an individual's life. Historical research, including pioneering work by Daugman (Bowyer & Burge, 2016), and segmentation improvements by Wildes (Okokpujie et al., 2018), laid a strong foundation. Techniques for iris boundary detection and segmentation—like "snake" or active contour algorithms—emerged in the late 1980s and 1990s

(Mesejo et al., 2016; Gilbert, 2012), enabling accurate isolation of the iris from surrounding eye features and supporting reliable feature extraction.

For continuous authentication, iris recognition can integrate with video-based eye-tracking to verify identity unobtrusively as users naturally interact with their devices (Modi, 2011). This reduces the need for explicit prompts and can handle subtle variations in lighting or user positioning (Ali, 2024; Gilbert, 218). Despite these advantages, challenges remain: stable image acquisition under real-world conditions is non-trivial, and computational overheads must be managed to ensure practical deployment (Gill et al., 2024; Abilimi & Yeboah, 2013). Although standardized iris datasets (example, CASIA-Iris, BioSec) and evaluation protocols exist (Khade et al., 2021), continuous authentication systems require extended longitudinal studies and tests under diverse environmental conditions.

Towards a Comparative Understanding of Biometric Modalities

While fingerprint, facial, and iris recognition each offer distinct advantages, no single biometric modality is universally superior for continuous authentication. External factors (lighting, motion, user behavior), device form factors, and application requirements all influence the suitability of a given modality (Gilbert, 2022; Fernandes et al., 2019; Abilimi et al., 2013). To advance the state of the art, future research should focus on:

- Establishing common benchmarking standards, including datasets and performance metrics tailored for continuous CUA scenarios.
- Conducting comparative analyses that quantify trade-offs in accuracy, computational overhead, latency, and user satisfaction.
- Incorporating longitudinal datasets to evaluate how well each modality adapts to evolving user habits and environmental conditions over time (Bui-Tien et al., 2024).

By grounding these efforts in rigorous empirical evaluations, standardized protocols, and credible references, the research community can better understand the nuanced interplay of multiple biometric modalities and drive toward more robust, versatile, and user-friendly continuous authentication solutions (Mulligan, 2024).

TABLE 2: Biometric-Based Approaches

Section	Key Description	Challenges/Limitations	Future Directions
Biometric-Based CUA	Utilizes physiological or behavioral characteristics (e.g., fingerprint, facial, iris) to verify identity over time.	Differences in accuracy, robustness, and usability; environmental factors affecting sensor performance.	Establish standard datasets, performance benchmarks, and protocols for continuous evaluation.
Fingerprint Recognition	Relies on unique fingerprint patterns. Feature-based strategies integrate with motion sensors for richer interaction data.	Susceptible to moisture, sensor variability, and environmental noise. Requires longitudinal testing under real-world conditions.	Development of touchless fingerprint systems using integrated motion sensors and cameras for improved usability and security.
Facial Recognition	Analyzes facial features, incorporating advanced modeling techniques (e.g., 3D, thermal mapping) for continuous verification.	Struggles with lighting, appearance changes, and privacy concerns. Risk of spoofing via masks or deepfake-style techniques.	Introduce adaptive algorithms and privacy-preserving techniques like homomorphic encryption and differential privacy.
Iris Recognition	Capitalizes on the stable patterns of the iris. Integrates video-based eye-tracking for unobtrusive verification.	Requires precise image acquisition; computational overheads limit real-world deployment.	Focus on lightweight algorithms for stable acquisition and extend longitudinal studies to account for diverse environmental conditions.
Towards Comparison	Highlights trade-offs between modalities, e.g., fingerprint (stable, precise), facial (hands-free), and iris (highly unique).	No single modality is universally superior; performance varies with environmental and user factors.	Conduct comparative studies quantifying trade-offs (e.g., accuracy, latency) across modalities and develop hybrid/multi-modal systems.

This table summarizes the different biometric-based approaches to CUA, outlining their descriptions, challenges, and potential areas for improvement.

V. Behavioral Patterns for Authentication

Behavioral patterns have emerged as a promising avenue for continuous user authentication (CUA) in mobile contexts (Ayeswarya & Singh, 2024). Unlike traditional credentials—such as passwords or PINs—behavioral indicators can be captured implicitly as users naturally interact with their devices (Gupta et al., 2023). Touch gestures, typing rhythms, application usage patterns, and navigation habits all generate data streams that enable ongoing verification. By relying on these subtle cues, behavioral-based CUA aims to reduce user interruptions, improve overall usability, and enhance security (Gupta et al., 2023; Yeboah & Abilimi 2013). As mobile applications continue to evolve, the ability to leverage these patterns offers both new opportunities and challenges for creating seamless, user-centric authentication frameworks.

Yet, despite growing interest, the practical implementation of behavioral-based CUA remains an active area of research. Much of the existing literature has focused on isolated modalities, such as keystroke dynamics or touch gestures, and often requires explicit user engagement (Fan, 2023; Abilimi & Adu-Manu, 2013). Moreover, few studies have thoroughly validated their methods through large-scale user studies or long-term field deployments. Addressing these gaps demands both methodological rigor and close attention to ethical considerations—ensuring that user data is handled responsibly, transparently, and in compliance with prevailing regulations.

Integrating Behavioral Cues via Standardized APIs:

Realizing the full potential of behavioral-based CUA requires robust infrastructure support. Mobile operating system

developers and device manufacturers should provide well-documented application programming interfaces (APIs) that grant secure, controlled access to sensor inputs and user interaction logs. Ensuring that data collection is grounded in informed consent, anonymization, and compliance with frameworks such as the General Data Protection Regulation (GDPR) will be essential for maintaining user trust. Enhanced transparency around data usage, along with user-friendly consent interfaces, can foster broader acceptance and a willingness to participate in continuous authentication schemes (Ayeswarya & Singh, 2024).

Proposed Implicit Behavior-Based Architecture:

To advance beyond theory, we propose a holistic architecture designed to operate unobtrusively in the background. Rather than relying on explicit authentication prompts, the system continuously monitors user interactions across multiple granular levels:

I. Data Pre-Processing and Normalization: Raw sensor data (example accelerometer, gyroscope, touchscreen coordinates) is normalized to mitigate device heterogeneity and environmental variations (Lupión et al., 2021).
II. Feature Extraction: Relevant behavioral features—such as gesture curvature, typing latency, pressure sensitivity, and micro pauses—are distilled from the normalized signals. Evidence suggests that combining multiple features can improve authentication accuracy and resilience (Wang, 2022).
III. Incremental Modeling and Classification: Machine learning or deep learning models update the user's behavioral profile over time. This incremental learning approach adapts to evolving user patterns, device upgrades, and changes in routine, thereby maintaining accuracy over longer periods (Martín et al., 2021; Abilimi et al., 2015).
IV. Adaptive Decision Thresholding: Thresholds for re-authentication or fallback security checks are dynamically adjusted based on continuous feedback loops. This ensures that the system can respond quickly to anomalies, such as suspected account takeovers, while minimizing false alarms (Kepkowski, 2023).

Validation and Empirical Assessment:

While the proposed architecture is conceptually sound, its effectiveness must be substantiated with empirical evidence. Future research should conduct comprehensive user studies to evaluate the system under realistic conditions—across diverse user populations, varying device types, and extended usage durations. Field experiments, for example, can examine authentication accuracy, false acceptance/rejection rates, and latency. Similarly, user acceptance studies can illuminate how participants perceive privacy, intrusiveness, and trustworthiness when continuously monitored. These insights will guide refinements, inform best practices, and ensure that the technology meets real-world security and usability requirements (Freigang, Schlenker & Köhler, 2018).

Privacy, Ethics, and Compliance:

Adopting a behavior-based approach raises important privacy and ethical considerations. Behavioral data may inadvertently reveal sensitive information about users' habits, schedules, or personal attributes. Thus, privacy-preserving techniques—such as differential privacy, on-device processing, and secure enclaves—should be incorporated to limit data exposure. Additionally, compliance with legal standards (example, GDPR, CCPA) and adherence to established ethical guidelines are paramount. Collaboration with legal experts, ethicists, and user advocacy groups will help establish guidelines for transparent data handling, informed consent, and robust user control over personal information (Felzmann et al., 2020).

Toward a More Secure and User-Friendly Future:

Behavioral-based CUA has the potential to fundamentally shift authentication paradigms, delivering a continuous, context-aware, and user-aligned security layer. By building on existing research and addressing current gaps—especially the need for experimental validation and detailed privacy measures—this approach can offer a credible alternative to traditional authentication, enhancing trust, convenience, and resilience against sophisticated attacks Adam (Hammoudeh, Alrawashdeh & Alsulaimy, 2024; Kwame, Martey & Chris, 2017).

Ongoing research will need to reconcile competing demands: stringent security, minimal user burden, and robust privacy safeguards. As technology and regulations evolve, so will the strategies for harnessing behavioral patterns. Ultimately, this line of inquiry can lead to authentication solutions that not only protect sensitive information but also respect individual rights and user comfort in an increasingly mobile and data-rich world.

The diagram outlines the process and challenges associated with implementing behavioral patterns for continuous user authentication (CUA). It begins by emphasizing the role of user interaction data, such as touch gestures, typing rhythms, application usage patterns, and navigation habits, as the foundation for authentication. These behavioral signals are continuously collected and analyzed to generate data streams that facilitate ongoing verification within a user-centric framework. The goal is to minimize user interruptions while ensuring seamless authentication.

However, the implementation of CUA faces several challenges. Isolated modalities require greater user engagement, which calls for methodological rigor and ethical considerations to ensure the system is effective and trustworthy. Integration via standardized APIs is critical to streamline the process. This involves securing informed consent from users, anonymizing their data to protect privacy, and building trust through transparency.

The diagram highlights the necessity of balancing technical sophistication with user-friendliness and ethical practices. By addressing these implementation challenges, CUA systems can become more reliable, adaptable, and widely accepted.

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

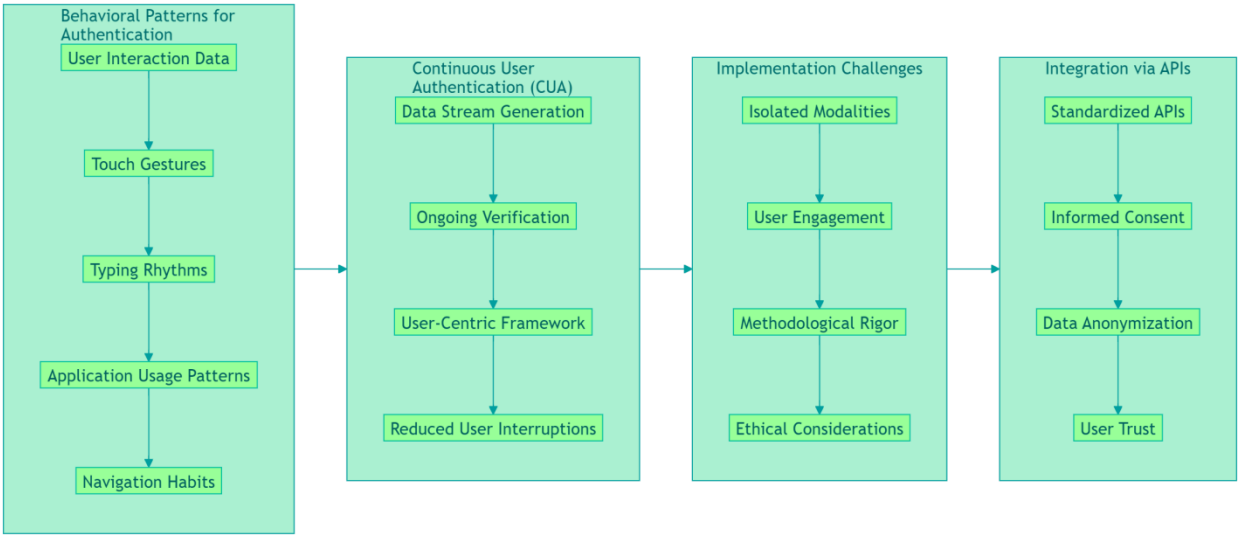

Figure 6: Behavioral patterns enhance mobile user authentication security.

A Framework for Behavioral-Based Continuous Authentication

The behavioral-based CUA system can be thought of as a process that takes in raw data from a user's interactions with their device and transforms it into a reliable, privacy-friendly way to verify their identity continuously (Bansal & Ouda, 2024). This process involves five key stages:

I. Pre-Processing and Normalization

The system starts with raw data from sensors (like touchscreens, accelerometers, or gyroscopes). This data can vary a lot depending on the device or environment. To make it consistent and usable, the system cleans and normalizes the data, reducing the impact of differences like screen size or external noise.

II. Feature Extraction

Once the data is normalized, the system looks for specific patterns in how the user interacts with the device. For example, it might analyze how they swipe, type, or apply pressure on the screen. These patterns are distilled into key features, such as the curvature of gestures or the time it takes to press a key, which serve as unique "behavioral fingerprints."

III. Incremental Modeling and Classification

The system uses machine learning to create and update a profile of the user's behavior over time. It adapts as the user's habits evolve—like if they get a new device or change their routine. This ongoing learning helps keep the system accurate and responsive.

IV. Adaptive Decision Thresholding

To decide whether to take action (like asking for a password), the system sets thresholds for what counts as "normal" behavior. These thresholds aren't fixed—they adjust dynamically based on feedback. For example, if the system detects something unusual (like a different typing rhythm), it might tighten security or ask the user to re-authenticate.

V. Privacy and Compliance

Because this system relies on personal data, it's designed to handle information responsibly. Data collection is done transparently, with user consent, and follows strict privacy regulations like GDPR. Techniques like anonymization and processing data directly on the device are used to protect sensitive information.

VI. Context-Aware Authentication

Traditional authentication systems typically rely on static verification methods—such as entering a password once at login—to confirm a user's identity. While this initial verification grants comprehensive access for the session's duration, it neglects the evolving context of device usage and user behavior (Wang., 2021). As a result, these methods leave periods of vulnerability where unauthorized individuals can exploit continuous access without encountering additional checkpoints. Over the past decade, researchers have begun to address this shortcoming through continuous user authentication (CUA) mechanisms that verify identity on an ongoing basis, rather than relying solely on intermittent or one-time inputs (Ayeswarya & Singh, 2024).

Building on CUA, context-aware authentication on mobile devices (CAAM) extends verification processes by incorporating environmental and behavioral cues—such as user activity, device movement, location, and environmental conditions—to dynamically adjust authentication requirements (Dionísio, 2020). For example, CAAM might enforce stricter verification protocols when unusual user behavior (e.g., atypical gait, sudden device orientation changes) or unfamiliar environments (example, an unknown Wi-Fi network or GPS coordinates) are detected (Netscher, 2016). Conversely, it can reduce user burdens in more predictable scenarios, allowing seamless access under routine conditions.

Preliminary Evidence and Potential Improvements:

Initial experiments have explored the benefits of CAAM by employing activity recognition algorithms from machine learning. For instance, internal tests using a random forest classifier to analyze accelerometer-derived activity features have shown preliminary gains in authentication accuracy compared to baseline CUA methods, potentially lowering the

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

chances of unauthorized access. Although these early findings are promising, they remain exploratory. Future studies should report standardized metrics such as accuracy percentages, Equal Error Rates (EER), and comparisons to established benchmarks. For example, controlled experiments using publicly available datasets (example, WISDM or mHealth datasets) and following common evaluation protocols could provide clear, quantitative evidence of CAAM's efficacy and facilitate reproducibility (Al-Worafi, 2024).

Addressing Legal and User Acceptance Concerns:

Beyond technical performance, the long-term viability of CAAM hinges on its compliance with legal and ethical standards, as well as user acceptance. Privacy regulations—such as the EU's General Data Protection Regulation (GDPR) and sector-specific guidelines like HIPAA (for healthcare)—demand transparent data handling, secure storage, and rigorous consent procedures. CAAM implementations must embed privacy-by-design principles, utilizing data minimization, anonymization, and encryption to meet regulatory demands (Benyahya et al., 2022). Future work should investigate how differential privacy, federated learning, and policy-based access control can ensure that sensitive contextual data remain protected.

User acceptance poses another significant challenge. While CAAM can reduce the inconvenience of repeated logins, continuous and context-aware monitoring may raise concerns about intrusiveness and lack of control. Empirical user studies—leveraging survey instruments, focus groups, and controlled field trials—can help identify user thresholds for comfort, trust, and perceived intrusiveness. For example, researchers could employ the Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT) to systematically evaluate factors influencing user acceptance (Alyoussef, 2022). Likewise, iterative design processes that incorporate user feedback, transparency features (e.g., dashboards showing what data are collected and why), and user-configurable privacy settings can help foster trust and promote more widespread adoption.

Toward a Comprehensive, Multidisciplinary Framework:

The implementation of CAAM requires a multifaceted approach that integrates technical innovation with socio-legal awareness. Collaboration among legal scholars, privacy advocates, psychologists, usability researchers, policymakers, and security engineers is necessary to craft guidelines that ensure these systems are both effective and socially palatable. Multidisciplinary working groups and standards organizations (example, ISO/IEC JTC 1/SC 27 for security techniques) can help define metrics, develop best practices, and create certification schemes for vendors and developers (Dwivedi et al., 2024).

By coupling quantitative evaluation of system performance with in-depth exploration of legal compliance and user perception, the research community can chart a path toward robust, context-aware continuous authentication solutions (Ametefe et al., 2024). Such frameworks would not only reinforce the security of mobile devices but also respect legal constraints, honor user expectations, and adapt seamlessly to the diverse contexts in which mobile technologies are deployed.

TABLE 3: Summary of Context-Aware Authentication

Aspect	Description
Traditional Authentication	Relies on static verification methods (e.g., passwords) granting session-wide access, leaving periods of vulnerability due to lack of dynamic re-verification.
Context-Aware Authentication (CAAM)	Extends continuous user authentication (CUA) by dynamically adjusting verification requirements using environmental and behavioral cues (e.g., user activity, device movement, location).
Examples of Dynamic Adjustment	Enforces stricter protocols for unusual behavior (e.g., atypical gait, sudden orientation changes) or unfamiliar environments, while reducing user burden in predictable scenarios.
Preliminary Evidence	Initial machine learning-based tests (e.g., random forest classifiers analyzing accelerometer data) showed potential for improving accuracy compared to baseline CUA methods.
Future Improvements	Calls for standardized metrics (e.g., EER, accuracy percentages), use of public datasets (e.g., WISDM, mHealth), and adherence to evaluation protocols for reproducibility.
Legal and Ethical Compliance	Must adhere to GDPR, HIPAA, and other standards by embedding privacy-by-design principles such as data minimization, anonymization, and encryption.
Privacy-Preserving Techniques	Differential privacy, federated learning, and policy-based access control to ensure sensitive data protection.
User Acceptance Challenges	Concerns about intrusiveness and lack of control; mitigated by transparency, user feedback, and customizable privacy settings.
User Studies and Tools	Leverages tools like TAM (Technology Acceptance Model) and UTAUT to evaluate user trust, comfort, and perceptions of intrusiveness.
Implementation Framework	Requires a multidisciplinary approach involving technical innovation, legal scholars, psychologists, usability researchers, and engineers.
Collaboration Needs	Standards organizations (e.g., ISO/IEC JTC 1/SC 27) must define metrics, best practices, and certification schemes to ensure effective implementation.
Final Objective	To create robust, context-aware authentication solutions that improve security, respect legal and ethical standards, and adapt to diverse user and environmental conditions.

VII. Challenges and Limitations

Implementing continuous user authentication (CUA) on mobile devices requires overcoming a host of interrelated challenges spanning technical, behavioral, and organizational domains. Traditional approaches, such as single sign-on (SSO) or intermittent re-authentication, minimize user inconvenience but leave sessions vulnerable once initial checks are passed. Studies indicate that attackers can exploit these gaps, gaining unauthorized access during periods of uninterrupted use. Additionally, emerging threats include mimicry attacks, where adversaries replicate a user's biometric traits, underscoring the fragility of static or infrequent verification methods (Mirkovic, 2013).

The core difficulty lies in striking a balance between stringent security and practical usability. While intermittent authentication may seem convenient, it often proves

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

insufficient against sophisticated threats. For instance, an adversary might wait for a device to be unlocked and then operate within the authenticated session unchallenged. Similarly, purely biometric approaches risk compromise if high-quality replicas or leaked biometric templates enter the threat landscape. Without continuous assessment, even the most advanced biometric techniques can be circumvented (Aaby, 2024).

Enterprise scenarios further complicate the picture. Employers may hold physical or remote access rights to organizational devices, potentially bypassing protective measures that rely solely on static credentials or easily replicated biometrics (Putman, 2021). These conditions highlight the need for adaptive authentication strategies that re-verify users over time, respond to shifting contexts, and preserve trust across evolving operational environments.

Addressing these challenges necessitates a holistic rethinking of CUA. Integrating multiple biometric modalities can increase spoofing resistance, while machine learning-driven anomaly detection can continuously monitor behavioral cues—such as typing patterns, gesture dynamics, and application usage—to identify deviations from established baselines. Incorporating external contextual signals (example, geolocation data, network characteristics, or proximity to trusted devices) offers additional security layers (Sookhak et al., 2018). Simultaneously, privacy-preserving technologies (example, secure enclaves, homomorphic encryption, and differential privacy) ensure that sensitive biometric and behavioral data remain protected.

To refine and validate potential solutions, researchers must engage in rigorous experimental evaluation. Well-structured user studies and field trials should simulate mimicry scenarios, employer intrusions, and session hijacking attempts to measure real-world resilience. Collecting benchmark data and comparing performance against established metrics—such as Equal Error Rate (EER) or Receiver Operating Characteristic (ROC) curves—would enable the community to identify promising approaches and pinpoint areas needing improvement (Islam & Sufian, 2023). Defining clear research questions—for example, how combining specific biometric modalities influences EER under various environmental conditions—could guide future investigations. Establishing publicly available datasets and shared benchmarks would further accelerate progress by providing common reference points for different research teams (Mulligan, 2024).

Ultimately, collaboration between academia, industry, and standardization bodies is essential for advancing CUA technologies. By aligning on evaluation frameworks, exploring testable hypotheses, and encouraging data sharing, the field can move beyond conceptual prototypes toward robust, user-validated authentication systems (Trac et al., 2023). These efforts will help ensure that CUA solutions evolve into practical, trusted tools that deliver both heightened security and seamless user experiences in increasingly mobile-centric environments.

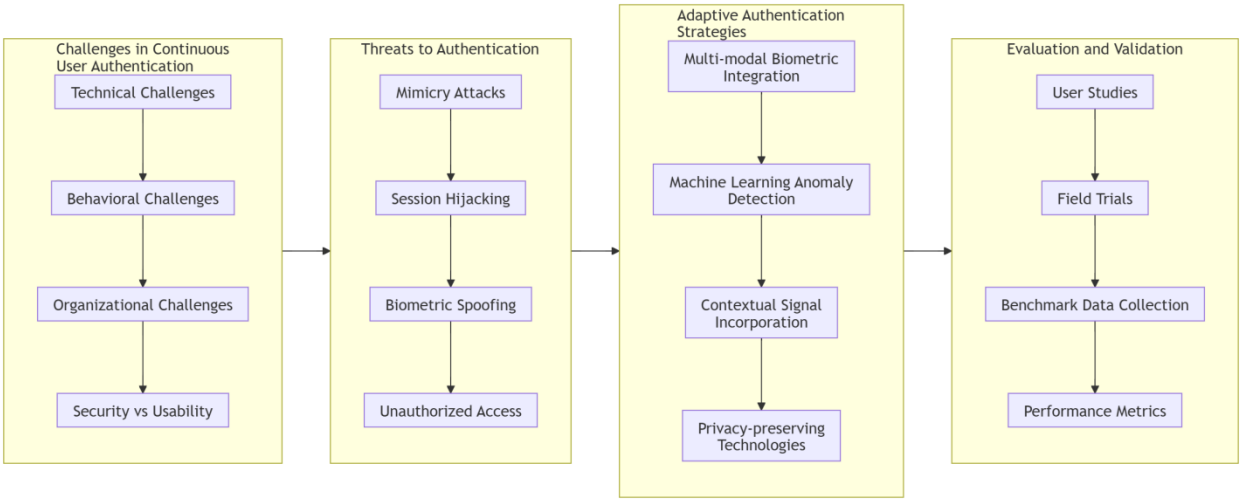

Figure 7: Challenges and solutions for CUA

The provided diagram breaks down key aspects of challenges, threats, strategies, and evaluation in continuous user authentication systems.

The first section highlights the challenges faced in implementing continuous authentication, categorized into technical, behavioral, and organizational domains. Technical challenges relate to the complexities of maintaining robust systems, while behavioral challenges involve the variability of user interactions. Organizational challenges arise from balancing security requirements with usability, often creating tension between stringent security and user convenience.

The second section focuses on threats to authentication systems, such as mimicry attacks, session hijacking, biometric spoofing, and other forms of unauthorized access. These threats underline the need for systems to evolve beyond static or basic authentication mechanisms to ensure ongoing protection against sophisticated attacks.

The third section presents adaptive authentication strategies designed to counter these threats. These strategies include multi-modal biometric integration, which combines multiple biometric indicators for improved accuracy; machine learning-based anomaly detection for identifying unusual patterns of

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

behavior; contextual signal incorporation to adjust security requirements dynamically based on environmental factors; and the use of privacy-preserving technologies to protect user data during these processes.

Finally, the last section addresses evaluation and validation methods for these systems. This includes conducting user studies to gather insights into real-world performance, field trials to test under varied conditions, benchmark data collection for standardized comparison, and the establishment of performance metrics to measure and refine the effectiveness of authentication systems over time.

In summary, the diagram outlines a comprehensive approach to developing, securing, and validating continuous user authentication systems, emphasizing the importance of balancing technological sophistication, user behavior, and privacy concerns.

VIII. Future Research Directions

The findings presented in this study identify multiple opportunities to advance continuous, touch-based user authentication methods. Moving forward, researchers should not only broaden the scope of inquiry but also establish well-defined research questions and benchmarks to guide iterative improvement. Below, we propose targeted directions that incorporate specific hypotheses, comparative baselines, and structured methodologies:

I. Diversifying User Populations and Interaction Contexts:

Proposed Hypothesis: Varying user demographics and physical conditions—such as reduced dexterity in elderly populations or altered interaction styles among children—will differentially impact the stability and accuracy of behavioral biometric models.

To test this hypothesis, future studies should incorporate diverse user groups and tasks, explicitly comparing authentication performance across cohorts. For instance, researchers might measure changes in Equal Error Rate (EER) or Receiver Operating Characteristic (ROC) curves when the same model is applied to standard adult users versus individuals with motor impairments. Establishing baseline datasets that reflect these varied populations and conditions would enable meaningful cross-study comparisons (Shaheen, 2023).

II. Expanding Activity Domains and Modalities:

Proposed Hypothesis: Integrating additional contextual features—such as device orientation, multi-touch gestures, or handwriting input—will improve authentication robustness and reduce susceptibility to mimicry attacks, particularly under variable environmental conditions.

Future experiments could quantify authentication accuracy gains relative to a baseline dataset containing only touch and swipe features. Researchers might use standardized metrics (example, EER, accuracy percentages) and publicly available datasets that include environmental annotations (example, lighting, device motion) to validate improvements. Testing incremental feature sets against a fixed baseline ensures that observed performance gains are attributable to the newly introduced modalities (Wu et al., 2021).

III. Industry Collaboration and Real-World Deployments:

Proposed Research Question: Under what real-world constraints (example, battery consumption, device memory, network latency) can continuous authentication systems maintain high accuracy without degrading user experience or computational efficiency? To answer this question, collaboration with hardware manufacturers and OS developers is essential.

Researchers could evaluate their methods on prototype devices or standardized testbeds, benchmarking performance against baseline models published in the literature. Quantitative results—such as average latency (milliseconds per authentication check) and energy expenditure (mAh consumed per hour of continuous authentication)—would offer concrete targets for improvement (Zhang et al., 2022; Opoku-Mensah, Abilimi & Amoako, 2013).

IV. Open-Source Data Collection and Community Engagement:

Proposed Hypothesis: Open benchmarks and baseline models will accelerate progress and enhance reproducibility in continuous user authentication research by making it easier to compare novel approaches against known standards.

To operationalize this, the community should agree on a core benchmark dataset, including a representative set of user behaviors and conditions. Establishing baseline performance metrics (example, an initial EER of 10% using a specified feature set and classification algorithm) provides a reference point for subsequent innovations. Researchers can then propose new models or features and directly assess whether their contributions offer statistically significant improvements over these benchmarks (Bender et al., 2022; Yeboah,Opoku-Mensah & Abilimi, 2013a).

V. In summary, advancing continuous, touch-based authentication requires more than broad conceptual directions; it demands testable hypotheses, defined performance metrics, and accessible benchmark datasets. By formulating explicit research questions—such as how additional modalities affect EER or how resource constraints impact user experience—and grounding future studies in standardized comparisons, the research community can collectively refine, validate, and scale user-centric authentication solutions. This systematic approach will ensure that progress is both incremental and evidence-based, ultimately contributing to secure, adaptive, and inclusive authentication frameworks that meet the needs of a diverse range of end-users and application scenarios.

In essence, these targeted directions encourage structured comparisons, community standards, and real-world validation—fostering an evidence-based, incremental approach to advancing continuous, touch-based authentication methods.

Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 158-173, 2025.

TABLE 4: Summary of the future research directions, incorporating the proposed hypotheses, research questions, methodologies, and benchmarks discussed

Direction	Proposed Hypothesis/Research Question	Suggested Methodology	Potential Benchmarks & Metrics	Expected Outcomes
1. Diversifying User Populations and Interaction Contexts	**Hypothesis:** Varying user demographics and physical conditions will affect the stability and accuracy of behavioral biometric models.	- Recruit diverse user cohorts (e.g., elderly, children, users with motor impairments). - Conduct comparative analyses using EER, ROC curves. - Deploy identical models across varying populations and tasks.	- Baseline datasets reflecting diverse demographics. - Established EER and ROC metrics for standard vs. specialized populations.	More inclusive models that remain accurate across a wider range of user conditions and abilities.
2. Expanding Activity Domains and Modalities	**Hypothesis:** Integrating new contextual features (orientation, multi-touch, handwriting) enhances robustness and reduces mimicry vulnerability, particularly under variable environments.	- Incremental feature addition experiments. - Use standardized metrics (EER, accuracy) to compare against a baseline dataset of touch/swipe-only features. - Incorporate environmental annotations (lighting, device motion) for controlled comparisons.	- A baseline set of features (touch/swipe only) for initial comparison. - Publicly available datasets with environmental context.	Improved authentication performance through richer input modalities and verified generalizability under diverse conditions.
3. Industry Collaboration and Real-World Deployments	**Research Question:** Under real-world constraints (battery life, memory, latency), how can continuous authentication maintain accuracy without degrading user experience or efficiency?	- Collaborations with hardware/OS manufacturers for testing prototypes. - Benchmark against literature-based models using testbeds. - Measure computational metrics (latency in ms, energy consumption in mAh/hour) and user satisfaction.	- Performance benchmarks for latency and energy use from industry-standard devices. - Comparative baselines from published literature.	Practical guidelines and design principles that balance authentication strength with resource constraints and UX.
4. Open-Source Data Collection and Community Engagement	**Hypothesis:** Open benchmarks and baseline models will accelerate progress and reproducibility, enabling straightforward comparisons of novel approaches to standard references.	- Establish a community-agreed, core benchmark dataset. - Define baseline EER, accuracy scores using standard features and classification models. - Invite researchers to submit improvements against these fixed baselines.	- A shared repository with a canonical dataset and a well-documented baseline model. - Public leaderboards or evaluation platforms.	Enhanced transparency, reproducibility, and continuous improvement driven by open, standardized evaluation frameworks.

IX. Conclusion

This study has introduced a conceptual framework and an initial prototype for continuous user authentication (CUA) on mobile devices, emphasizing touch-based interaction features at low and medium frequencies. In a preliminary user study involving a modest sample size (example, fewer than 20 participants) and limited interaction sessions, we recorded a comparatively high Equal Error Rate (EER), underscoring the nascent state of our approach. To contextualize this figure, established biometric modalities in more controlled conditions often achieve significantly lower EERs (example, under 5% for certain fingerprint or facial recognition systems) (Neal & Woodard, 2020; Yeboah, Opoku-Mensah & Abilimi, 2013b). In contrast, our initial EER—ranging from approximately 15% to 20%—suggests that substantial refinement and optimization are necessary before these methods become viable in everyday user scenarios (Himeur et al., 2021; Yeboah, Odabi & Abilimi Odabi, 2016)

Despite these early challenges, our results highlight several promising avenues for future enhancement. Increasing the quality and diversity of input data—potentially by incorporating additional sensors (such as cameras, microphones, or ambient light detectors)—can bolster both the richness and stability of extracted features. More sophisticated machine learning models, combined with advanced feature selection and dimensionality reduction techniques, may help reduce error rates and improve the robustness and adaptability of the system. These technical refinements, coupled with rigorous privacy-preserving measures, could yield more discriminative behavioral indicators and stronger user protections

The significance of this work lies in its potential to advance beyond static authentication toward a dynamic, user-centered paradigm. With further empirical validation—through larger-scale user studies, more comprehensive datasets, and comparative benchmarking against established authentication methods—researchers can better gauge the performance gains and practical trade-offs of continuous, behavior-based verification. Moreover, interdisciplinary collaborations that involve security experts, usability researchers, engineers, and legal scholars are essential to address the socio-technical and regulatory implications of such systems (Christopher, 2013)

As continuous user authentication matures, it stands to become a valuable tool in the growing repertoire of mobile security solutions. By building on the preliminary insights presented here and systematically addressing identified shortcomings, the research community can guide CUA toward scalable, real-world implementations. Ultimately, this evolution promises enhanced trust, improved usability, and heightened security for an increasingly mobile and interconnected society.

References

1. Aaby, P. (2024). *Advancing touch-based continuous authentication by automatically extracting user behaviours* (Doctoral dissertation).
2. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and

Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
3. Abilimi, C. A., & Adu-Manu, K. S. (2013). *Examining the impact of Information and Communication Technology capacity building in High School education in Ghana*. International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September - 2013
4. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. *International Journal of Engineering Research and Technology, 2(11), 50 - 59.*
5. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
6. Adam, M., Hammoudeh, M., Alrawashdeh, R., & Alsulaimy, B. (2024). A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access*.
7. Agarwal, A., Ramachandra, R., Venkatesh, S., & Prasanna, S. M. (2024). Biometrics in extended reality: a review. *Discover Artificial Intelligence, 4(1), 81*.
8. Ali, M. (2024). *A Novel Convolutional Neural Network Pore-Based Fingerprint Recognition System* (Doctoral dissertation, Concordia University).
9. Ali, S., & Khusro, S. (2016). Mobile phone sensing: A new application paradigm. *Indian Journal of Science and Technology, 9(19), 1-42*.
10. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors, 23(19), 8015*.
11. Al-Naji, F. H., & Zagrouba, R. (2020). A survey on continuous authentication methods in Internet of Things environment. *Computer Communications, 163, 109-133*.
12. Al-Worafi, Y. M. (2024). *Handbook of Complementary, Alternative, and Integrative Medicine: Education, Practice, and Research Volume 3: Research Evidence Based Clinical Practice*. CRC Press.
13. Alyoussef, I. Y. (2022). Acceptance of a flipped classroom to improve university students' learning: An empirical study on the TAM model and the unified theory of acceptance and use of technology (UTAUT). *Heliyon, 8(12)*.
14. Ametefe, D. S., Sarnin, S. S., Ali, D. M., Ametefe, G. D., John, D., & Hussin, N. (2024). Advancements and challenges in fingerprint presentation attack detection: a systematic literature review. *Neural Computing and Applications, 1-23*.
15. Ayeswarya, S., & Norman, J. (2019, March). Seamless Personal Authentication using Biometrics. In *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)* (Vol. 1, pp. 1-5). IEEE.
16. Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access.*
17. Bansal, P., & Ouda, A. (2024). Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics. *Computers, 13(4), 103*.
18. Bender, A., Schneider, N., Segler, M., Patrick Walters, W., Engkvist, O., & Rodrigues, T. (2022). Evaluation guidelines for machine learning tools in the chemical sciences. *Nature Reviews Chemistry, 6(6), 428-442*.
19. Benyahya, M., Collen, A., Kechagia, S., & Nijdam, N. A. (2022). Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. *Computers & Security, 122, 102904*.
20. Bingham, M. J. K. (2016). *Towards Effective Behavioural Biometrics for Mobile Devices* (Doctoral dissertation, Carleton University).
21. Bowyer, K. W., & Burge, M. J. (Eds.). (2016). *Handbook of iris recognition*. Springer London.
22. Bui-Tien, T., Nguyen-Chi, T., Le-Xuan, T., & Tran-Ngoc, H. (2024). Enhancing bridge damage assessment: Adaptive cell and deep learning approaches in time-series analysis. *Construction and Building Materials, 439, 137240*.
23. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.
24. Clarke, N. (2011). *Transparent user authentication: biometrics, RFID and behavioural profiling*. Springer Science & Business Media.
25. Dahia, G., Jesus, L., & Pamplona Segundo, M. (2020). Continuous authentication using biometrics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(4), e1365*.
26. Dionísio, M. S. G. (2020). *Leveraging the Transmedia Entertainment-Education Framework to Augment Tourists Awareness of Local Values* (Doctoral dissertation, Universidade NOVA de Lisboa (Portugal)).
27. Dwivedi, Y. K., Jeyaraj, A., Hughes, L., Davies, G. H., Ahuja, M., Albashrawi, M. A., ... & Walton, P. (2024). "Real impact": Challenges and opportunities in bridging the gap between research and practice–Making a difference in industry, policy, and society. *International Journal of Information Management, 102750*.
28. Fan, J. (2023). Evaluation and study of user interface with wearable devices based on computer vision: model based on VR keyboard and hand interaction.
29. Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and engineering ethics, 26(6), 3333-3361*.
30. Fernandes, R., Viana, S. D., Nunes, S., & Reis, F. (2019). Diabetic gut microbiota dysbiosis as an inflammaging and immunosenescence condition that fosters progression of retinopathy and nephropathy. *Biochimica Et Biophysica Acta (BBA)-Molecular Basis of Disease, 1865(7), 1876-1897*.
31. Fontem, O. (2024). *Strategies and Methods Used by Information Technology Security Professionals to Secure Cloud Access Infrastructure* (Doctoral dissertation, Walden University).
32. Freigang, S., Schlenker, L., & Köhler, T. (2018). A conceptual framework for designing smart learning environments. *Smart Learning Environments, 5, 1-17*.
33. Gadkar-Wilcox, W. (2017). Snapshots of authorship and authority in Vietnamese historical writing. *South East Asia Research, 25(1), 7-33*.
34. Gao, Y. (2021). *Transforming Earphones into a Secure and Ubiquitous Hearable Platform* (Doctoral dissertation, State University of New York at Buffalo).
35. Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., ... & Buyya, R. (2024). Modern computing: Vision and challenges. *Telematics and Informatics Reports, 100116*.
36. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's *The Road*. English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.
37. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. *The Educational Forum*, *83*(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.
38. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. *Educational Action Research*, *30*(5), 881–901. https://doi.org/10.1080/09650792.2021.1875856
39. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. *Kappa Delta Pi Record*, *58*(1), 14–19. https://doi.org/10.1080/00228958.2022.2005426
40. Gilbert, C. & Gilbert, M.A.(2024a).Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf
41. Gilbert, C. & Gilbert, M.A.(2024b).Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816
42. Gilbert, C. & Gilbert, M.A.(2024c).The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_

AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.
43. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.
44. Gilbert, C. & Gilbert, M.A.(2024e).Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf
45. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.
46. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.54
47. Gilbert, C., & Gilbert, M. A. (2024h).Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
48. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.
49. Gilbert, C. & Gilbert, M.A. (2024j).The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
50. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.
51. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, *9*(4), 205–219.
52. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, *5*(11), 889–907. https://www.ijrpr.com
53. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *9*(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013
54. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, *5*(11), 3235-3256. https://www.ijrpr.com.
55. Gilbert, C., & Gilbert, M. A. (2024p) .Cryptographic Foundations And Cybersecurity Implications Of Blockchain Technology. *Global Scientific Journals*,ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com
56. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science*, *9*(4), 238–251.
57. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.76
58. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.77
59. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews*, *5*(12), 507–533. https://www.ijrpr.com/
60. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5*(12), 1174–1191. Retrieved from www.ijrpr.com
61. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. *International Journal of Research Publication and Reviews*, *5*(12), 1149–1173. Retrieved from www.ijrpr.com
62. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. *Global Scientific Journal*, *12*(12). Retrieved from www.globalscientificjournal.com
63. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
64. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
65. Gonzalez-Manzano, L., Fuentes, J. M. D., & Ribagorda, A. (2019). Leveraging user-related internet of things for continuous authentication: A survey. *ACM Computing Surveys (CSUR), 52(3), 1-38*.
66. Gupta, S., Buriro, A., & Crispo, B. (2018). Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems, 2018, 2649598*.
67. Gupta, S., Maple, C., Crispo, B., Raja, K., Yautsiukhin, A., & Martinelli, F. (2023). A survey of human-computer interaction (HCI) & natural habits-based behavioural biometric modalities for user recognition schemes. *Pattern Recognition, 139, 109453*.
68. Haroon, H. (2022). *IMAGE-BASED OCCUPANCY SENSING AND PRIVACY IMPLICATIONS* (Master's thesis, Middle East Technical University).
69. Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S. R., Rehman, A. U., & Bharany, S. (2024a). Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity.
70. Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S. R., Rehman, A. U., & Bharany, S. (2024b). Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity.
71. Hernández-Álvarez, L., de Fuentes, J. M., González-Manzano, L., & Hernández Encinas, L. (2020). Privacy-preserving sensor-based continuous authentication and user profiling: a review. *Sensors, 21(1), 92*.
72. Himeur, Y., Alsalemi, A., Al-Kababji, A., Bensaali, F., Amira, A., Sardianos, C., ... & Varlamis, I. (2021). A survey of recommender systems for energy efficiency in buildings: Principles, challenges and prospects. *Information Fusion, 72, 1-21*.
73. Huan, L. Q., Nguyen, D. M., Pham, H. A., & Huynh-Tuong, N. (2020). Authentication in E-learning systems: Challenges and Solutions. *VNUHCM Journal of Engineering and Technology, 3(SI1), SI95-SI101*.
74. Hussain, A. (2021). *Flexible Content Authorization Using Digital Rights Management in Cloud Computing* (Master's thesis, University of Malaya (Malaysia)).
75. Islam, M. A., & Sufian, M. A. (2023). Employing AI and ML for Data Analytics on Key Indicators: Enhancing Smart City Urban Services and Dashboard-Driven Leadership and Decision-Making. In *Technology and Talent Strategies for Sustainable Smart Cities* (pp. 275-325). Emerald Publishing Limited.
76. Islam, M. O. (2023). *Equitable User Experience in Terms of Privacy and Security Settings* (Master's thesis, University of South-Eastern Norway).
77. Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023a). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors, 23(21), 8944.*
78. Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023b). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors, 23(21), 8944.*
79. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS), 2(1), 129-171*.

80. Kepkowski, M. M. (2023). *Privacy enhancing technologies for identity and access management* (Doctoral dissertation, Macquarie University).
81. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. *Inventions, 6(4), 65.*
82. Kumar, P. P. (2023). *Multiparty Collaboration in Edge Computing Systems.* Temple University.
83. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.
84. Lawrence, M. (2024). The Significance of Continuous User Authentication on Mobile Devices.
85. Leonard, L. C. (2017). Web-based behavioral modeling for continuous user authentication (CUA). In *Advances in Computers* (Vol. 105, pp. 1-44). Elsevier.
86. Lupión, M., Medina-Quero, J., Sanjuan, J. F., & Ortigosa, P. M. (2021). Dolars, a distributed on-line activity recognition system by means of heterogeneous sensors in real-life deployments—a case study in the smart lab of the university of Almería. *Sensors, 21(2), 405*.
87. Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News, 190(1), 1-69.*
88. Martín, G. A., Fernández-Isabel, A., Martín de Diego, I., & Beltrán, M. (2021). A survey for user behavior analysis based on machine learning techniques: current models and applications. *Applied Intelligence, 51(8), 6029-6055*.
89. Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2014). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17(3), 1268-1293*.
90. Mesejo, P., Ibáñez, O., Cordón, O., & Cagnoni, S. (2016). A survey on image segmentation using metaheuristic-based deformable models: state of the art and critical analysis. *Applied Soft Computing, 44, 1-29*.
91. Milton, L. C. (2015). *User behavioral modeling of web-based systems for continuous user authentication* (Doctoral dissertation, University of Maryland, College Park).
92. Mirkovic, J. (2013). *Usability, Security, and Mobility for Mobile Devices in Healthcare Information Systems.*
93. Modi, S. K. (2011). *Biometrics in identity management: Concepts to applications.* Artech House.
94. Mulligan, J. (2024a). Behavioural Biometrics: A Novel Approach to User Authentication in Information Systems Security.
95. Nag, A. K. (2019). A Survey on Computational Intelligence Techniques in User Identity Management.
96. Neal, T., & Woodard, D. (2020). Presentation attacks in mobile and continuous behavioral biometric systems. In *Securing Social Identity in Mobile Platforms: Technologies for Security, Privacy and Identity Management* (pp. 21-40).
97. Netscher, G. (2016). *Applications of machine learning to support dementia care through commercially available off-the-shelf sensing.* Berkeley: University of California.
98. Obi, O. C., Dawodu, S. O., Daraojimba, A. I., Onwusinkwue, S., Akagha, O. V., & Ahmad, I. A. I. (2024). Review of evolving cloud computing paradigms: security, efficiency, and innovations. *Computer Science & IT Research Journal, 5(2), 270-292*.
99. Okokpujie, K., Noma-Osaghae, E., John, S., & Ajulibe, A. (2018). An improved iris segmentation technique using circular Hough transform. In *IT Convergence and Security 2017: Volume 2* (pp. 203-211). Springer Singapore.
100. Olweny, F. (2024). Navigating the nexus of security and privacy in modern financial technologies. *GSC Advanced Research and Reviews, 18(2), 167-197*.
101. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst*, *4*, 50-57.
102. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760-769.
103. Patidar, P., Ngoon, T. J., Zimmerman, J., Ogan, A., & Agarwal, Y. (2024a). ClassID: Enabling Student Behavior Attribution from Ambient Classroom Sensing Systems. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 8(2), 1-28.*
104. Pradeep Kumar, P. (2023). *Multiparty Collaboration In Edge Computing Systems* (Doctoral dissertation, Temple University. Libraries). Putman, C. G. J. (2021). *A Requirements Based Selection Model for Future Proof Non-Intrusive Authentication Technologies in the Office* (Master's thesis, University of Twente).
105. Sailema, W. G. C., Olivares, T., & Delicado, F. (2022). Topologías en el Internet de las Cosas Médicas (IoMT), revisión bibliográfica. *Revista Tecnológica-ESPOL, 34(4), 120-136*.
106. Shafik, W. (2024). Shaping the Next Generation Smart City Ecosystem: An Investigation on the Requirements, Applications, Architecture, Security and Privacy, and Open Research Questions. In *Smart Cities: Innovations, Challenges and Future Perspectives* (pp. 3-52). Cham: Springer Nature Switzerland.
107. Shaheen, A. (2023). Computer-aided analysis of complex neurological data for age-based classification of upper limbs motor performance and radiomics-based survival prediction of brain tumors.
108. SHAKIR, M. T. (2020). *User authentication in public cloud computing through adoption of electronic personal synthesis behavior* (Doctoral dissertation).
109. Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2018). Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials, 21(2), 1718-1743*.
110. Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion, 66, 76-99*.
111. Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers & Security, 59, 210-235*.
112. Trac, J., Lee, J., Fok, K. H., Carrillo, B., & Farcas, M. (2023). CUA 2023 Annual Meeting Abstracts–Poster Session 8: Training/Education, Technology. *CUAJ, 17(6)*.
113. Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications, 188, 103080*.
114. Wang, Z. (2022). *Towards Ubiquitous User Authentication and Sensing Based on the Ear Canal and Toothprint Biometrics Using Ear Wearables.* The Florida State University.
115. Wu, C., He, K., Chen, J., Zhao, Z., & Du, R. (2021). Toward robust detection of puppet attacks via characterizing fingertip-touch behaviors. *IEEE Transactions on Dependable and Secure Computing, 19(6), 4002-4018*.
116. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A..(2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2*(7).
117. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.
118. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b).Automatic Biometric Student Attendance System: A Case Study Christian Service University College. *Journal of Engineering Computers & Applied Sciences,* 2(6), 117-121.
119. Yeboah T. & Abilimi C.A. (2013).*Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).
120. Zhang, D., Kang, Y., Zhou, L., & Lai, J. (2017). Continuous user authentication on touch-screen mobile phones: toward more secure and usable M-commerce. In *Internetworked World: 15th Workshop on e-Business, WeB 2016* (pp. 225-236). Springer International Publishing.
121. Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., ... & Luzcando, E. (2022). Practical adoption of cloud computing in power systems—Drivers, challenges, guidance, and real-world use cases. *IEEE Transactions on Smart Grid, 13(3), 2390-2411*.