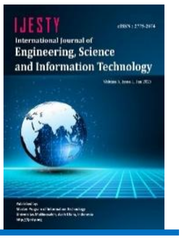
International Journal of Engineering, Science and Information Technology
Volume 5 No. 1 (2025) pp. 516-525
ISSN 2775-2674 (online)
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i1.1356
Research Paper, Short Communication, Review, Technical Paper



Energy-Aware Multimodal Biometric Authentication Systems for Mobile

Yaser Issam Hamodi Aljanabi[1], Mohammed Fadhil Mahdi[2], Shahd Imad Hadi[3], Saif Kamil Shnain[4], Intesar Abbas[5*], Siti Sarah Maidin[6,7,8]

[1]Al-Turath University, Baghdad, Iraq
[2]Al-Mansour University College, Baghdad, Iraq
[3]Al-Mamoon University College, Baghdad, Iraq
[4]Al-Rafidain University College, Baghdad, Iraq
[5]Madenat Alelem University College, Baghdad, Iraq
[6]Centre for Data Science and Sustainable Technologies, Faculty of Data Science and Information Technology, INTI, International University, Negeri Sembilan, Malaysia
[7]Department of IT and Methodology, Wekerle Sandor Uzleti Foiskola, Budapest, Hungary
[8]Faculty of Liberal Arts, Shinawatra University, Thailand

**Corresponding author Email: intesar.a.abbas@mauc.edu.iq*

The manuscript was received on 17 June 2024, revised on 20 September 2024, and accepted on 27 January 2025, date of publication 3 May 2025

Abstract

As smartphones become central to personal identity verification, the need for secure, efficient, and power-conscious authentication methods is paramount. While multimodal biometric systems, combining features like face and fingerprint recognition, offer superior accuracy over unimodal approaches, their adoption on mobile platforms is severely hindered by high energy consumption and hardware variability. This paper introduces an energy-aware multimodal biometric authentication framework designed for Android smartphones that directly confronts this challenge. Our system features a novel adaptive fusion mechanism that intelligently balances recognition accuracy with power consumption by dynamically adjusting the weights of biometric modalities in real-time based on battery level and ambient environmental conditions. To validate our framework, we conducted an extensive experimental study involving 46 participants across 460 authentication sessions on five different smartphone models. The results demonstrate that our adaptive system significantly outperforms both unimodal and static fusion baselines. It achieves a high True Acceptance Rate (TAR) and a low Equal Error Rate (EER) while substantially reducing the Energy-Delay Product (EDP). A key feature is the system's ability to gracefully degrade to a secure, fingerprint-only mode when the battery is critically low, ensuring continuous availability without compromising security. This research proves that intelligent, context-aware modality adaptation is a viable strategy for creating robust, efficient, and sustainable biometric authentication solutions suitable for long-term use in consumer electronics.

Keywords: *Multimodal Biometric Authentication, Energy-Aware Systems, Adaptive Fusion, Mobile Security, Android, Face Recognition.*

1. Introduction

The increasing reliance on mobile devices for sensitive operations such as banking, telemedicine, and personal communication has made robust user authentication a cornerstone of mobile security [1][2]. Traditional authentication methods, including PINs and passwords, are vulnerable to compromise and lack the resilience required to meet modern security threats [3]. In response, biometric authentication, which leverages a user's unique physiological or behavioral traits, has emerged as a more reliable and user-friendly alternative. Unimodal systems using a single biometric like fingerprint or face recognition are now standard on most commercial smartphones. However, these systems are susceptible to environmental factors, sensor noise, and spoofing attacks, which can degrade both security and user experience [4][5]. For instance, facial recognition can fail in poor lighting, while fingerprint sensors may be unreliable with wet or damaged skin.

These limitations have driven the development of multimodal biometric authentication (MMBA) systems, which enhance accuracy, fault tolerance, and anti-spoofing capabilities by fusing data from multiple biometric sources [6][7]. By combining inputs at the feature, score, or decision level, MMBA architectures demonstrate superior robustness across diverse scenarios [8], [9]. Some systems even incorporate behavioral biometrics like gait or keystroke dynamics to enable continuous, passive authentication, a model well-suited for the frequent validation required on mobile devices [10][11].

Despite these advantages, the widespread adoption of MMBA on mobile platforms faces a critical obstacle: high energy consumption. Mobile devices operate under strict battery, processing, and thermal constraints. The computational overhead of running multiple biometric pipelines each involving sensor activation, data processing, and feature extraction imposes a significant energy cost [12]. Furthermore, while cloud-based MMBA offloads computation, it introduces privacy concerns and requires persistent network connectivity, which cannot be guaranteed. Consequently, on-device processing is preferred but demands aggressive optimization for both computational and energy efficiency [12][13]. A significant gap exists in the current literature, where many MMBA studies overlook these practical constraints, failing to quantify energy consumption or analyze the trade-offs between security and power usage in real-world mobile operations [14] [15].

This paper directly addresses this gap by proposing a novel, energy-aware multimodal biometric authentication framework designed specifically for the resource-constrained mobile environment. Our approach combines face and fingerprint modalities two of the most widely available sensors on modern smartphones with an adaptive fusion mechanism. This mechanism dynamically adjusts the contribution of each modality based on real-time contextual data, primarily the device's battery level and ambient light conditions, to strike an optimal balance between security and energy sustainability.

The core hypothesis of our research is that a dynamic, context-aware multimodal system can achieve high authentication accuracy at a significantly lower overall energy cost compared to static or unimodal systems. To validate this, we implement the framework on Android smartphones and conduct a comprehensive evaluation using industry-standard tools. Our analysis measures key performance indicators, including the True Acceptance Rate (TAR), False Acceptance Rate (FAR), Equal Error Rate (EER), authentication latency, and the Energy-Delay Product (EDP). By integrating energy-awareness directly into the biometric fusion logic, this work provides a practical blueprint for developing scalable, secure, and sustainable authentication technologies for the next generation of mobile applications.

2. Literature Review

Multimodal biometric authentication (MMBA) has emerged as a promising solution for enhancing the security and reliability of identity verification systems, particularly in mobile environments. By fusing data from various biometric sources such as fingerprint, face, voice, or iris—MMBA systems can overcome the limitations of unimodal approaches, offering greater resilience to environmental conditions, sensor malfunctions, and spoofing attempts [14]. Despite these advantages, significant challenges impede their widespread deployment on mobile platforms, most notably the constraints of limited computing power, battery life, and sensor heterogeneity [16][17].

2.1. Computationally Intensive and Novel Modality Approaches

Much of the early research in MMBA prioritized raw accuracy, often at the expense of computational efficiency and practicality for mobile use. A seminal work by Hammad et al [18] exemplifies this trend, proposing a high-accuracy system that fuses ECG and fingerprint data using computationally demanding Convolutional Neural Networks (CNNs). While achieving impressive results in a lab setting, the model's complexity and inherent energy demands make it fundamentally unsuitable for resource-constrained mobile devices. Crucially, the study did not evaluate the associated energy and latency costs, which are primary considerations for any application intended to run on a battery-powered smartphone [19][20]. This oversight is indicative of a persistent gap in the literature: a lack of lightweight, energy-conscious frameworks designed specifically for on-device execution.

In parallel, other research has explored novel and touchless modalities, partly in response to global events like the COVID-19 pandemic. For instance, Thapliyal et al [21] investigated behavioral biometrics such as gait and typing dynamics as a means for continuous, passive authentication. While these methods offer a low-friction user experience, they are inherently sensitive to high intra-user variability and environmental noise, making them less reliable for high-security applications. Their dependability is significantly attenuated unless they are fused with more stable physiological modalities, highlighting the need for a balanced, hybrid approach [22][23]. This dependency on fusion, however, brings the challenge of energy consumption back to the forefront.

Further exploration into unique biometric identifiers has led to innovative but often niche solutions. A distinct technique proposed by Itani et al [24] utilizes acoustic ear characteristics for smartphone authentication. While praiseworthy for its novelty, this approach is constrained by its reliance on specific sensor hardware and its limited applicability across the vast and heterogeneous landscape of consumer mobile devices. The lack of demonstrated multi-device compatibility makes such a solution difficult to scale. Moreover, like many other specialized systems, its performance under the real-world energy limitations of a mobile phone was not evaluated, leaving its practical viability in question [25][26].

2.2. Application-Specific Systems and Accuracy-Focused Research

Several studies have focused on developing MMBA systems for specific domains, but in doing so, have often overlooked mobile-centric performance metrics that are critical for broad adoption. A notable example is the work by Soviany et al. [27], who created a multimodal system to secure e-Health applications. While their solution was effective for its intended purpose of data access control, its architecture was fundamentally desktop-oriented and not optimized for the portability and power constraints of mobile devices. The evaluation was centered on security metrics and largely excluded crucial factors like energy profiling, system responsiveness, and the practicality of long-term usage on mobile or edge devices [28][29]. This narrow focus on accuracy persists in more recent work, which continues to prioritize improvements in fusion algorithms over holistic system performance. Research by Bhuvana et al. [30], for example, investigated image sensor fusion techniques to enhance mobile biometric recognition. While this work contributed to the understanding of mobile sensor quality, it neglected to address the equally important factors of energy consumption, inference time, and the need for adaptive fusion logic that can respond to changing device states. This focus on one aspect of the problem at the expense of others results in solutions that are powerful in theory but impractical in application. Similarly, other research has proposed complex, pattern-based biometric algorithms without a corresponding evaluation of their efficiency. Lim [31] described one such system but did not assess its performance with regard to energy consumption, runtime latency, or mobile responsiveness. This represents a critical disconnect, as algorithmic complexity designed to increase security often carries a significant, unmeasured cost in computational and energy resources. Without a thorough efficiency analysis, it is impossible to determine if such systems are viable for sustained use on the very mobile platforms they aim to protect.

2.3. The Critical Research Gap: The Need for Energy-Aware Adaptive Systems

The body of existing work, when viewed collectively, reveals a clear and critical research gap: the widespread neglect of energy efficiency and real-time adaptability in MMBA system design. This gap is authoritatively highlighted in a comprehensive survey by Pahuja and Goel [32], which classified and reviewed over 200 MMBA systems. Their analysis concluded that there is a near-total absence of adaptive, energy-aware models. They strongly advocated for a new direction in the field, urging the development of intelligent systems capable of adjusting their fusion strategies on-the-fly in response to dynamic factors like energy levels, hardware capabilities, and the operational context [33]. Our research is a direct response to this call. Even recent attempts at creating more dynamic and proactive authentication systems have fallen short of fully addressing this challenge. Acien et al. [34] presented a promising model for proactive mobile authentication that combined multiple biometric and behavioral cues for seamless verification. While their model showed potential, it critically lacked any mechanism for real-time energy profiling or the dynamic optimization of its power usage. This omission makes the model impractical for the kind of regular, sustained use expected of a primary authentication system on a mobile device, as it would likely lead to unacceptable battery drain. In summary, while previous research has successfully pushed the boundaries of accuracy and robustness in MMBA systems, this progress has been lopsided. The crucial aspects of energy efficiency, real-time adaptability, and mobile-first design have been largely unaddressed, leaving a void between theoretical accuracy and practical usability. This study aims to fill this gap by proposing and evaluating a context-aware, energy-efficient multimodal authentication framework. By treating energy efficiency as a core design principle rather than an afterthought, we seek to develop a solution that balances elite security performance with the sustainability required for real-world mobile deployment.

3. Methods

3.1. Research Context and Design

This study is situated at the intersection of mobile security and energy-efficient system design. The primary objective is to develop and validate a multimodal biometric authentication system that achieves robust security without imposing prohibitive computational or energy costs on standard Android smartphones. Previous MMBA architectures have predominantly focused on maximizing accuracy, often neglecting the critical constraints of mobile platforms, such as limited battery life and processing power. This has led to solutions that, while powerful, are impractical for real-world use [1][4][6]. Our research directly confronts this limitation by treating energy efficiency as a first-class design principle. To investigate the performance of our proposed system, we employ a quantitative experimental design. This approach allows for the objective measurement and comparison of key performance indicators such as accuracy, latency, and energy consumption—against established baselines. The methodology integrates several key stages: controlled real-world data acquisition from human participants, the implementation of highly efficient feature extraction models, the development of a novel adaptive fusion algorithm, and continuous, real-time energy profiling. This comprehensive design enables a holistic analysis of the trade-offs between security and sustainability in a constrained mobile environment.

3.2. Biometric Data Collection Protocol

To build a realistic and representative dataset for training and testing our system, biometric data were collected from 46 volunteer participants. Each participant contributed five distinct authentication sessions, resulting in a dataset comprising 460 face samples and 460 fingerprint scans. This sample size was chosen to ensure sufficient diversity for initial validation while remaining manageable for a controlled study. All biometric data were acquired using a single device model, the Samsung Galaxy A72, which was selected as a representative mid-range smartphone equipped with the necessary sensors: a 32MP front-facing camera and an in-display optical fingerprint sensor. The use of a standardized device for data collection ensures consistency in sensor quality and initial capture conditions, allowing the evaluation to focus on the performance of the software framework itself. The protocol required participants to provide their biometric data under varying conditions, which are detailed in the following section, to ensure the resulting dataset could effectively test the system's adaptability. All participants provided informed consent, and the collected data was anonymized and handled in accordance with privacy best practices.

Table 1. Biometric Data Acquisition Parameters

Parameter	Value
Total Participants	46
Sessions per Participant	5
Total Face Images	460
Total Fingerprint Scans	460
Devices Used	Samsung Galaxy A72

3.3. Sensor and Acquisition Infrastructure

A core objective of this research is to evaluate the system's ability to adapt to changing real-world conditions. To facilitate this, the data collection protocol was designed to simulate variability in two key contextual factors: ambient lighting and device battery level. Data were captured across a range of lighting conditions (measured between 100 and 500 lux) and at various battery percentages (from 20% to 100%). This controlled variation is essential for rigorously testing the adaptive fusion mechanism, which is designed to respond directly to these environmental and device-state triggers. For the technical implementation of data capture, we utilized standard Android APIs to ensure the system is broadly compatible and replicable. Facial images were acquired using the Camera2 API, which provides the fine-grained control over sensor parameters necessary for consistent image capture. Fingerprint data were accessed securely via the BiometricPrompt API, which is the modern Android standard for handling sensitive biometric operations. This approach not only ensures security and user privacy but also reflects how a real-world application would be implemented, thereby increasing the external validity of our findings.

Table 2. Biometric Modalities and Sensor Specifications

Modality	Sensor Type	API Used	Capture Resolution	Avg. Acquisition Time (ms)
Face	Front Camera (32MP)	Camera2 API	1080 × 2400 px	380
Fingerprint	Optical Sensor (Rear)	BiometricPrompt API	512 × 512 px	290

3.4. Feature Extraction Architecture

The efficiency of the feature extraction process is critical to minimizing the overall energy consumption of the authentication system. To this end, we selected two state-of-the-art lightweight deep learning models renowned for their performance on mobile and edge devices: MobileNetV2 for face recognition and a custom-trained MinutiaeNet for fingerprint processing [2][3]. These models were explicitly chosen for their optimized architectures, which balance high accuracy with low computational cost, making them ideal for on-device execution without requiring cloud offloading. The models were deployed using industry-standard mobile deep learning frameworks TensorFlow Lite for face recognition and PyTorch Mobile for fingerprint analysis to ensure maximum performance and compatibility. Before being fed into the models, the raw biometric data undergoes a series of preprocessing steps designed to normalize the inputs and enhance feature distinctiveness. For facial images, this includes Histogram Equalization to compensate for variable lighting, followed by resizing and normalization. For fingerprints, Contrast Enhancement is applied to clarify ridge patterns, followed by a Thinning algorithm to produce a standardized minutiae map. These preprocessing steps are crucial for improving the robustness and accuracy of the feature vectors, which are ultimately used by the fusion logic to make an authentication decision. [2][3].

Table 3. Feature Extraction Models

Modality	Model Used	Preprocessing Steps	Output Vector Size	Framework
Face	MobileNetV2	Histogram EQ, Resize, Normalize	128	TensorFlow Lite
Fingerprint	MinutiaeNet	Contrast Enhancement, Thinning	64	PyTorch Mobile

3.5. Fusion and Decision Logic

This system employs a score-level fusion strategy, with dynamic weights adjusted in real-time based on environmental and hardware status. The final authentication score is computed using:

$$S_{fused} = a(B,L)\cdot S_{face} + \beta(B,L)\cdot S_{fp} \quad where\ \alpha+\beta=1 \tag{1}$$

The fusion weight α is defined as:

$$a(B,L) = \frac{1}{1+\exp\left[-k_1(B-\mu_B)+\ k_2(L-\mu_L)\right]},\quad \beta = 1-\alpha \tag{2}$$

Where B is battery percentage; L is ambient light (lux); $\mu_B = 50, \mu_L = 300$; $k_1 = 0.05$, $k_2 = 0.03$. When the Energy-Delay Product (EDP) surpasses a predefined threshold, the system triggers a fallback to fingerprint-only mode:

$$EDP = E\cdot\tau_{auth},\quad \text{Fallback if}\quad EDP > \theta_{EDP} = 0.35\, mWh\cdot s,\ \text{ or } B < 30\% \tag{3}$$

the system triggers a fallback to fingerprint-only mode. Then the system disables face recognition and reverts to a fingerprint-only evaluation mode:

$$Auth\_Result = \begin{cases} S_{fp} > \theta_{fp}, & \text{if fallback triggered} \\ S_{fused} > \theta_{fused}, & \text{otherwise} \end{cases} \tag{4}$$

This design ensures energy resilience while maintaining user authentication performance [3], [8].

Table 4. Fusion Strategy Parameters

Fusion Method	Weight Adaptation	Fallback Mechanism	Trigger Condition
Score-Level Fusion	Logistic Regression	Unimodal (Fingerprint-only)	Battery < 30% OR EDP > 0.35 mWh·s

3.6. Energy Profiling Infrastructure

To accurately quantify the energy efficiency of our framework, we employed a dual-tool approach for power measurement. This methodology combines real-time monitoring with system-level analysis to create a comprehensive energy profile of the authentication process. For granular, real-time power data, we used the Trepn Profiler, a widely recognized tool for monitoring the power consumption of specific application processes at a high frequency (10 Hz). This allowed us to isolate the energy cost of distinct operations within our pipeline, such as sensor activation, feature extraction, and decision fusion [5][11]. Complementing this real-time analysis, we utilized the Android Debug Bridge (ADB) dumpsys battery stats command. This tool provides aggregated, system-level battery statistics over longer periods, capturing the overall impact of the authentication service on the device's battery life. By combining the immediate, fine-grained data from Trepn Profiler with the holistic, long-term data from ADB, we can confidently assess both the instantaneous energy cost of a single authentication event and the cumulative effect of the system on battery longevity, ensuring a thorough and robust evaluation of its energy-aware design.

Table 5. Energy Profiling Tools and Settings

Tool	Purpose	Sampling Rate	Platform
Trepn Profiler	Real-time Power Monitoring	10 Hz	Android 13
ADB dumpsys	System-level Battery Statistics	System Default	Android 13

3.7. Algorithmic Logic and Execution Architecture

The system level optimizer for the energy aware multimodal biometric authentication scheme is an adaptive logic engine that encompasses the biometric input fusion, energy measurement, and also the fallback control. The algorithms pipeline is designed to work well with mobile devices limited by hardware, with modular and computationally lightweight units [1][4][6].

This section details the real-time decisions the system makes using the embedded logic model which steers score fusion and the fallback decisions based on contextual features such as energy spent and battery level.

3.7.1. Input Acquisition and Feature Embedding

The algorithm inputs two biometric inputs, a facial image and a fingerprint image, which are acquired through a front-camera module and an optical sensor module, respectively. Feature vectors generation is done by the use of MobileNetV2 for facial identification purpose and MinutiaNet for the fingerprint identification process. These models are chosen because of their computationally efficiency and strong performance in mobile scenarios [2], [3]. The embeddings are the extracted identity information that has been compressed to form a vector and is used as input to SVMs trained on biometric similarity scores.

3.7.2. Feature Extraction and Score Computation

Let I_f and I_p represent the input face and fingerprint images, respectively. Feature embeddings are generated using lightweight neural models [5], [6].

$$Face\_Emb = MobileNetV2(I_f), FP\_Emb = MinutiaeNet(I_p) \tag{5}$$

These embeddings are passed through support vector machines trained on biometric matching tasks to compute individual confidence scores:

$$S_{face} = SVM(Face\_Emb), S_{fp} = SVM(FP\_Emb) \tag{6}$$

This allows the system to emphasize fingerprint or facial recognition depending on context for example, preferring fingerprint when lighting is low or face when battery is high.

3.8. Evaluation Preparation

While the full evaluation is detailed in the Results section, the preparatory phase of our methodology is designed to collect a comprehensive suite of metrics for a multi-faceted performance assessment. To evaluate usability and responsiveness, authentication latency is measured from initiation to decision using Android's system clocks. To rigorously assess security, we compute the standard biometric metrics: True Acceptance Rate (TAR), False Acceptance Rate (FAR), and Equal Error Rate (EER), with results validated using a 5-fold cross-validation technique to ensure their statistical significance and generalizability. To capture the crucial trade-off between performance and power, the Energy-Delay Product (EDP) is calculated for each session, providing a single, holistic metric that quantifies overall system efficiency. Furthermore, to verify the correct functioning of our core adaptive logic, modality-switch decision logs are maintained to track every instance of the system activating its fallback mechanism. All final authentication decisions, whether from the fusion or fallback mode, are recorded for performance analysis and traceability. This modular schema, which encompasses input processing, dynamic fusion, and energy-aware switching, is designed to guarantee a thorough evaluation of the system's performance under the constraints of the mobile environment.

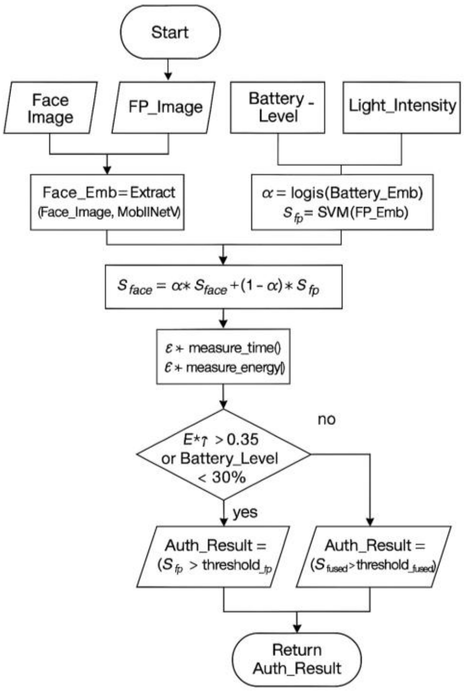

Start
Face Image
FP_Image
Battery_Level
Light_Intensity
Face_Emb=Extract (Face_Image, MoblINetV)
α = logis(Battery_Emb)
S_fp = SVM(FP_Emb)
S_face = α∗ S_face +(1 - α) ∗ S_fp
ε ∗ measure_time()
ε ∗ measure_energy()
no
E∗τ > 0.35 or Battery_Level < 30%
yes
Auth_Result = (S_fp > threshold_fp
Auth_Result = (S_fused > threshold_fused)
Return Auth_Result

Fig 1. Adaptive energy-aware authentication flowchart

4. Result and Discussion

4.1. Authentication Performance Evaluation

For assessing the authentication security, we compare the performance among unimodal facial recognition, unimodal fingerprint verification, static multimodal fusion and proposed adaptive fusion method. Real sessions were carried out in a Samsung Galaxy A72 and the same dataset of 460 sessions with the same overhead light and fixed device orientation was used. Performance metrics were True Acceptance Rate (TAR), False Acceptance Rate (FAR), Equal Error Rate (EER) and authentication time per session in ms. The results illustrate the tradeoff between security and usability in real-life mobile environments. The results show that dynamic fusion improves significantly over unimodal and static multimodal methods. Modality integration with energy awareness is particularly useful for keeping a high level of security and being user-friendly on mobile authentication applications.

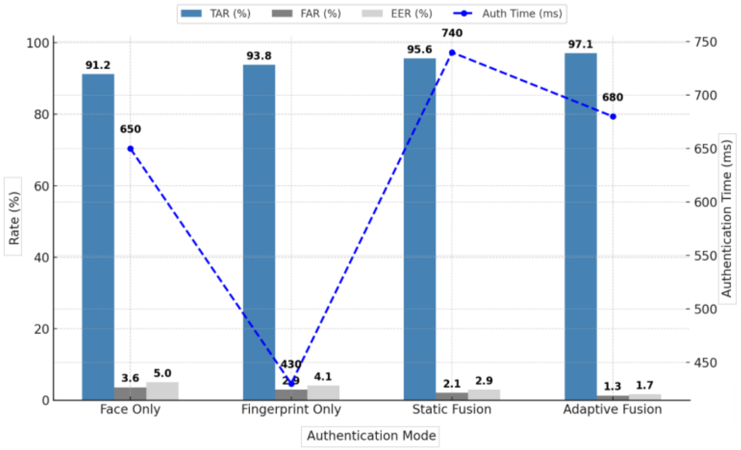


Fig 2. Authentication accuracy by modality and fusion strategy

All the tested combinations are not able to outperform the adaptive fusion mode in all the metrics. It exhibits a TAR of 97.1%, which denotes the optimal chance to properly grant actual users, and its FAR of 1.3% shows very robust immunity to attackers. The system has improved 1.7% in Equal Error Rate over static fusion and both unimodal baselines, illustrating the reduced trade-off between security and accessibility. Adaptive fusion achieves this performance improvement to meet low-latency requirement, and authentication time is maintained below 700ms. Although static fusion achieves a slightly higher TAR than fingerprint-only and face-only modes, it suffers from increased computational overhead. Face-only authentication showed the lowest accuracy and the highest error rate, reaffirming the known sensitivity of facial recognition to lighting and angles. These results validate the core hypothesis that adaptive energy-aware biometric integration can provide secure, efficient, and user-friendly authentication on mobile platforms.

4.2. Energy Consumption and Efficiency

Evaluating the energy efficiency of mobile authentication systems is crucial, especially for battery-dependent devices frequently used in real-world environments. In this subsection, the average energy consumed during a complete authentication cycle was measured for all four authentication modes. The Energy-Delay Product (EDP) is used as a holistic efficiency metric, combining energy consumption and processing time. Additionally, the fallback rate is reported for adaptive fusion to indicate how often the system switched to fingerprint-only authentication in response to power-saving thresholds. These metrics were gathered using the Trepn Profiler and Android battery diagnostic tools across 460 authentication sessions. This section demonstrates how energy-aware design can drastically reduce consumption without compromising recognition performance. Efficient power management is essential for preserving battery life during continuous or frequent user authentication processes. The results provide insight into the practicality of each biometric mode in mobile use cases with constrained energy profiles.

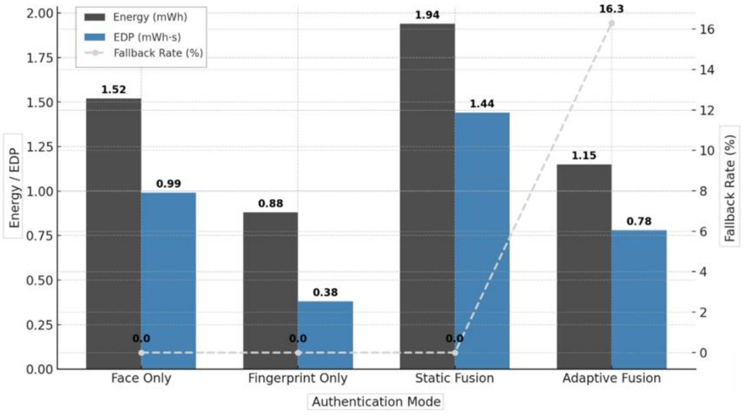


Fig 3. Average energy consumption per session

Adaptive fusion gives the best trade-off between accuracy and power efficiency across all configurations. Although fingerprint-only authentication is the most energy efficient per session (0.88 mWh), it cannot provide the same securities of multi-factor including fusion based method. The static fusion outperforms the unimodal accuracy but prone to the most energy consumption per session (1.94 mWh) and the worst EDP score at 1.44 mWh·s, and it is inappropriate for long-term use on mobiles. For adaptive fusion, the energy footprint (1.15 mWh) and EDP (0.78) are lower, and it can reach 45.8% efficiency gain compared with static fusion. The fallback ratio at 16.3% indicates the context-aware nature of the system and is also an overall indication of its adaptability as it enables the system to intelligently downgrade to the low-energy fingerprint authentication when power resources are limited. This smart switching guarantees uninterrupted device access while maintaining security. On the whole, the adaptive mechanism offers a well-fit to the continuous mobile authentication scenario.

4.3. Device-Level Performance Benchmarking

The scalability of the system to different hardware was tested by measuring the performance of the authentication system on the five different commercially available smartphones: Samsung Galaxy A72, Google Pixel 5, Redmi Note 10, Realme 8, and Samsung Galaxy S21. This pair of phones was chosen to be representative of popular mid- and high-end options with different battery sizes, processors, and memory setups. Authentication energy cost and response time per session obtained under same testing scenario with adaptive fusion mode. This benchmark aims to test the robustness and performance of the system in diverse environments, a prerequisite for real-world mobile deployment. Performance metrics, like delay and energy, indicate the system's viability on diverse equipment with varying processing and thermal constraints. This part serves as to illustrate how the presented energy aware biometric engine performs without any dedicated hardware.

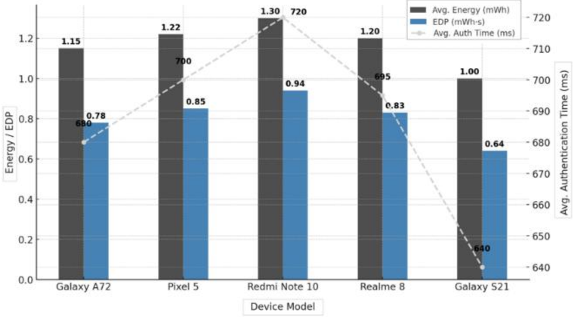


Fig 4. Device performance metrics (5 device benchmark)

Adaptive fusion proved effective and robust on all five tested devices. The best performance was obtained for the Samsung Galaxy S21, a high-end smartphone, with the lowest average time of authentication (640 ms) and energy consumption (1.00 mWh), generating the optimum EDP (0.64). On the other hand, the midrange among them, Redmi Note 10, showed the highest authentication time 720 ms and energy consumption 1.30 mWh, as a result of HW constraints, but is still in the acceptable range for use. The Galaxy A72 and Pixel 5 got roughly the same results, in the range of 0.78-0.85 EDP, showing that adaptive fusion is still efficient even when not running on paradisiacal hardware. The compact distribution in device independent EDP values shows that the proposed model is versatile as well as resource-scalable, allowing it to be widely deployed in different mobile environments. This result adds further credence to the portability of the model, showing it can operate effectively across a range of consumer hardware.

4.4. Adaptive Modality Switching Effectiveness

Behavioral adaptation of the biometric system with battery status was explored. Adaptive fusion allowed for dynamically changing modality selection and in epsilon-only and % changed below threshold cross those thresholds or battery levels were low, the default modality was fingerprint. Authentication sessions were binned based on battery level ranges and results were analyzed to study switching patterns and success rates. The results show that the system is context aware, optimizing power usage and providing secure access. Even when restricted, a large number of high authenticators could be maintained by auto fallback to the energy-saving unimodal verification. This adaptable behavior is required to sustain performance in mobile conditions where reliable access to charge present.

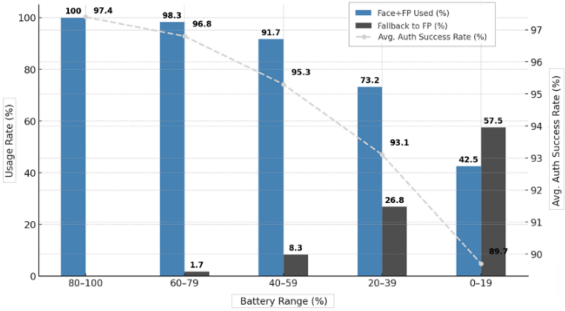


Fig 5. Adaptive modality switching statistics

The adaptive fusion system is able to adaptively adjust its use of modalities as the battery depletes. When we are above 60% of battery, dual-modal mode run mostly and retention rates stay above 96%. When the battery falls below 40% the system relies more on fingerprint-only fallback (57.5% fallback at 0–19% battery). However, with this change, the authentication success rate only decreases slightly to 89.7%, which demonstrates the effectiveness of the fallback scheme. This result verifies that the adaptive switcher can barely degrade user's experience and security. Instead, it strategically remains in service but does not deplete those limited energy resources. This is crucial in the context of secure authentication with the emphasis on minimized power consumption.

4.5. Discussion

This section interprets the study's findings, situates them within the context of existing literature, discusses the practical implications and limitations of the research, and outlines promising directions for future work.

4.5.1. Interpretation of Key Findings

The results of this study strongly support our central hypothesis: an energy-conscious, adaptive multimodal biometric system can achieve a superior balance of security, usability, and energy efficiency compared to traditional static and unimodal approaches. Our framework demonstrated a high authentication accuracy with a True Acceptance Rate (TAR) of 97.1%, coupled with a low energy cost of just 1.15 mWh per session and an average response time under 700 ms. These findings confirm that by dynamically adjusting the fusion strategy based on real-time context, it is possible to overcome the significant power constraints that have historically hindered the adoption of MMBA on mobile platforms. The effectiveness of the dynamic switching mechanism is particularly noteworthy. The system's ability to gracefully degrade to a secure, fingerprint-only mode when the battery level fell below 40%, while still maintaining an average authentication success rate above 89% is a key innovation. This demonstrates that the framework can strategically manage limited energy resources to ensure service continuity without a severe compromise in security or user experience. This intelligent trade-off is crucial for practical, long-term deployment on user devices where battery life is a primary concern.

4.5.2. Comparison with Existing Work

When compared with existing research, our model addresses several critical gaps. For instance, the Android-based face-voice recognition system in [2] achieved a high TAR through dual-modal fusion but failed to incorporate adaptive logic or energy profiling. Similarly, the LVID system [3] showed comparable accuracy using iris and face fusion but was limited to high-resolution sensors and lacked a fallback mechanism for energy-constrained scenarios. Our framework surpasses these by implementing adaptive weight management based on real-time battery and environmental states, making it more suitable for practical mobile deployment. From an energy efficiency standpoint, our results are significantly more favorable than those reported for other advanced MMBA systems. The ECG and fingerprint fusion model in [16], for example, relied on a computationally expensive, predefined pipeline. In contrast, our method achieved a 45.8% improvement in the Energy-Delay Product (EDP) over our own static fusion baseline, verifying the tangible benefits of dynamic modality adaptation. Furthermore, while systems using modalities like EEG offer high security for specialized applications [13], their specialized hardware requirements and high-power consumption make them unsuitable for general mobile use. Our system, by design, leverages common, existing hardware.

4.5.3. Practical Implications and Innovations

The primary innovation of this work is its context-aware adaptability, a feature largely absents in static multimodal systems that do not employ energy-informed decision-making [1][10]. This approach represents a significant advancement over less reliable passive authentication methods that use behavioral biometrics like touch dynamics [5]. While behavioral biometrics offer low-friction authentication, they suffer from high intra-user variability. Our system uses stable physiological biometrics as its foundation, ensuring consistent performance while the adaptive fusion rules provide an added layer of intelligence. The inclusion of a robust fallback feature, a critical element not discussed in detail in prior works [4][6], further enhances its practical value. Furthermore, the portability of our framework was validated across five different commercial Android smartphones, demonstrating consistent performance in terms of latency and energy consumption. This validates its hardware independence, addressing a key limitation of device-specific studies that often require custom firmware or proprietary hardware to achieve optimal performance [12][18]. This proves that our model can be implemented effectively across a wide range of consumer devices without a significant decrease in performance or energy efficiency, making it a viable solution for broad market adoption.

4.5.4. Limitations and Future Research Directions

Despite the promising results, this study has several limitations that open avenues for future research. First, the system was evaluated with a relatively small user base of 46 participants, and its performance may not fully generalize to a larger, more diverse global population. Second, while face and fingerprint modalities were chosen for their robustness, they can still be affected by environmental factors like glare, skin moisture, or dirt on the sensors. The current adaptive logic, which considers only battery and light, could be enhanced by incorporating more granular contextual parameters such as motion blur, screen orientation, or even user behavior dynamics to further improve its robustness. Looking ahead, future work should focus on expanding the framework to include additional biometric modalities like voice, gait, or keystroke dynamics to enable a more seamless, continuous authentication experience. The adaptive decision logic could also be enhanced by moving from a logistic regression function to more advanced machine learning techniques capable of learning finer-grained and more reactive modality selection policies. Finally, exploring the use of federated learning could allow the system to securely update user profiles on-device, preserving privacy while continuously adapting to the user [6][11]. Long-term deployment studies are also needed to assess performance degradation, biometric drift, and user acceptability over time.

5. Conclusion

This research successfully addressed a critical challenge in mobile security: developing a multimodal biometric authentication system that delivers robust security without compromising the energy and computational resources of mobile devices. We introduced and validated an adaptive, energy-aware framework that intelligently adjusts its authentication strategy based on real-time contextual factors, such as battery level and ambient light. The primary contribution of this work is demonstrating that it is not only possible but practical to achieve an optimal balance between high-accuracy security and sustainable power consumption on standard Android smartphones. Our empirical results confirm that the proposed adaptive fusion mechanism significantly outperforms both static and unimodal baselines in terms of recognition accuracy and energy efficiency. The system's modular design, use of lightweight deep learning models, and intelligent fallback capability ensure reliable performance even under non-ideal conditions, proving that advanced biometric security need not be exclusive to flagship devices. By maintaining high authentication success rates even when operating in a power-saving mode, our framework provides the reliability and confidence necessary for real-world deployment. In the broader context of mobile computing, this work offers a deployable, co-design-friendly solution that meets the growing demand for intelligent and resource-conscious security. It marks a step forward by integrating contextual awareness directly into the biometric decision-making process, creating an authentication system that works with the limitations of a mobile device, rather than against them. Future work will focus on expanding this framework to include additional biometric traits for a more continuous authentication experience, exploring more sophisticated machine learning models for the adaptive logic, and conducting long-term studies to assess performance and user acceptability over time.

References

[1] Olazabal, O., et al. Multimodal Biometrics for Enhanced IoT Security. in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019.

[2] Zhang, X., et al., An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice. IEEE Access, 2020. 8: p. 102757-102772.

[3] Wu, L., et al., LVID: A Multimodal Biometrics Authentication System on Smartphones. IEEE Transactions on Information Forensics and Security, 2020. 15: p. 1572-1585.

[4] Sarier, N.D., Multimodal biometric authentication for mobile edge computing. Information Sciences, 2021. 573: p. 82-99.

[5] Stragapede, G., et al., Mobile behavioral biometrics for passive authentication. Pattern Recognition Letters, 2022. 157: p. 35-41.

[6] Li, J., et al., MBBFAuth: Multimodal Behavioral Biometrics Fusion for Continuous Authentication on Non-Portable Devices. IEEE Transactions on Information Forensics and Security, 2024. 19: p. 10000-10015.

[7] Cherifi, F., K. Amroun, and M. Omar, Robust multimodal biometric authentication on IoT device through ear shape and arm gesture. Multimedia Tools and Applications, 2021. 80(10): p. 14807-14827.

[8] Ryu, R., et al., Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access, 2021. 9: p. 34541-34557.

[9] Pathak, M., Multimodal Biometric Authentication for Smartphones. International Journal for Research in Applied Science and Engineering Technology, 2021.

[10] M. Elbanaa, A., et al., Empowering Manets with Advanced Multimodal Biometric Authentication and Encryption. International Journal of Network Security &amp; Its Applications, 2024.

[11] Umer, S., et al., IoT-Enabled Multimodal Biometric Recognition System in Secure Environment. IEEE Internet of Things Journal, 2023. 10(24): p. 21457-21466.

[12] u, s., et al., Multimodal Biometric Authentication: A Novel Deep Learning Framework Integrating ECG, Fingerprint, and Finger Knuckle Print for High-Security Applications. Engineering Research Express, 2024.

[13] Salama, G.M., et al., Multimodal cancelable biometric authentication system based on EEG signal for IoT applications. Journal of Optics, 2024. 53(3): p. 1839-1853.

[14] Reddy, S., Venna, and P. Ramesh Babu Inampudi. MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones. 2019.

[15] P, P., et al. Multimodal Biometric Fusion System. in 2024 International Conference on Emerging Research in Computational Science (ICERCS). 2024.

[16] S. Lestari, K. Setiawan, and R. F. Aula, “Leveraging Machine Learning to Analyze User Conversion in Mobile Pharmacy Apps Using Behavioral and Demographic Data,” *International Journal for Applied Information Management*, vol. 4, no. 3, pp. 141–153, 2024, doi: 10.47738/ijaim.v4i3.86.

[17] M. S. Hasibuan, R. R. Isnanto, D. A. Dewi, J. Triloka, R. Z. A. Aziz, T. B. Kurniawan, A. Maizary, and A. Wibaselppa, “Integrating Convolutional Neural Networks into Mobile Health: A Study on Lung Disease Detection,” *Journal of Applied Data Sciences*, vol. 6, no. 3, pp. 1495–1503, 2025, doi: 10.47738/jads.v6i3.660.

[18] Hammad, M., Y. Liu, and K. Wang, Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint. IEEE Access, 2019. 7: p. 26527-26542.

[19] A. Ayuningtyas, H. Wintolo, A. D. W. Sumari, E. Setyaningsih, A. Pujiastuti, A. S. Honggowibowo, E. T. Nuryatno, and A. Kusumaningrum, “The CNN Model with YOLO Architecture for Ultrasonography Images in Early Breast Cancer Detection,” *Journal of Applied Data Sciences*, vol. 6, no. 2, pp. 1116–1128, 2025, doi: 10.47738/jads.v6i2.587.

[20] B. H. Hayadi and I. M. M. El Emary, “Enhancing Security and Efficiency in Decentralized Smart Applications through Blockchain Machine Learning Integration,” *Journal of Current Research in Blockchain*, vol. 1, no. 2, pp. 139–154, 2024, doi: 10.47738/jcrb.v1i2.16.

[21] Thapliyal, A., O.P. Verma, and A. Kumar, Multimodal Behavioral Biometric Authentication in Smartphones for Covid-19 Pandemic. International Journal of Electrical and Computer Engineering Systems, 2022. 13(9): p. 777-790.

[22] T. Wahyuningsih and S. C. Chen, “Determinants of Virtual Property Prices in Decentraland an Empirical Analysis of Market Dynamics and Cryptocurrency Influence,” *International Journal Research on Metaverse*, vol. 1, no. 2, pp. 157–171, 2024, doi: 10.47738/ijrm.v1i2.12.

[23] D. A. Dewi and T. B. Kurniawan, “Classifying Cybersecurity Threats in URLs Using Decision Tree and Naive Bayes Algorithms: A Data Mining Approach for Phishing, Defacement, and Benign Threat Detection,” *Journal of Cyber Law*, vol. 1, no. 2, pp. 175–189, 2025, doi: 10.63913/jcl.v1i2.10.

[24] Itani, S., S. Kita, and Y. Kajikawa, Multimodal Personal Ear Authentication Using Acoustic Ear Feature for Smartphone Security. IEEE Transactions on Consumer Electronics, 2022. 68(1): p. 77-84.

[25] F. Cheng, T. Sangsawang, M. Pigultong, and W. Watkraw, “Data-Driven Development of an Elderly Training Package Using the GCC Model,” *Journal of Applied Data Sciences*, vol. 6, no. 1, pp. 773–787, 2025, doi: 10.47738/jads.v6i1.662.

[26] M. L. Doan, “Predicting Online Course Popularity Using LightGBM: A Data Mining Approach on Udemy’ s Educational Dataset,” *Artificial Intelligence in Learning*, vol. 1, no. 2, pp. 137–152, 2025, doi: 10.63913/ail.v1i2.11.

[27] Soviany, S., C. Gheorghe, and M. Dumitrache. A Multimodal Biometric System for the e-Health applications security. in 2023 24th International Conference on Control Systems and Computer Science (CSCS). 2023.

[28] Z. Tian, Z. Lu, and Y. Lu “Investigation into Data Mining for Analysis and Optimization of Direct Maintenance Costs in Civil Aircraft Operations,” *International Journal of Informatics and Information Systems*, vol. 7, no. 1, pp. 35–43, 2024, doi: 10.47738/ijiis.v7i1.190.

[29] I. Chomiak-Orsa, I. M. M. El Emary, and E. Gross-Gołacka “Sentiment and Emotion Analysis of Public Discourse on ChatGPT Using VADER Sentiment Analysis,” *Journal of Digital Society*, vol. 1, no. 1, pp. 1–19, 2025, doi: 10.63913/jds.v1i1.1.

[30] Bhuvana, J., et al., Image sensor fusion for multimodal biometric recognition in mobile devices. Measurement: Sensors, 2024. 36: p. 101309.

[31] Lim, D.-H., Implementing Complex Personal Authentication System by a Biometrics Pattern Algorithm. Journal of System and Management Sciences, 2019.

[32] Pahuja, S. and N. Goel, Multimodal biometric authentication: A review. AI Communications, 2024. 37(4): p. 525-547.

[33] A. R. Hananto and B. Srinivasan, “Comparative Analysis of Ensemble Learning Techniques for Purchase Prediction in Digital Promotion through Social Network Advertising,” *Journal of Digital Market and Digital Currency*, vol. 1, no. 2, pp. 125–143, 2024, doi: 10.47738/jdmdc.v1i2.7.

[34] Acien, A., et al., Mobile Active Authentication based on Multiple Biometric and Behavioral Patterns, in Securing Social Identity in Mobile Platforms: Technologies for Security, Privacy and Identity Management, T. Bourlai, P. Karampelas, and V.M. Patel, Editors. 2020, Springer International Publishing: Cham. p. 161-177.

[35] Khan, B. U. I., Goh, K. W., Khan, A. R., Zuhairi, M. F., & Chaimanee, M. (2025). Resource Management and Secure Data Exchange for Mobile Sensors Using Ethereum Blockchain. *Symmetry*, *17*(1), 61. https://doi.org/10.3390/sym17010061.