PPG as a Bridge: Cross-Device Authentication for Smart Wearables with Photoplethysmography

JIACHENG LIU[†], Tsinghua University, China
JIANKAI TANG[†], Tsinghua University, China
GUANGYE ZHAO, Tsinghua University, China
RUICHEN GUI, University of Washington, United States
SONGQIN CHENG, Tsinghua University, China
TAITING LU, Pennsylvania State University, United States
JIAN LIU, Ant Group, China
WEIQIANG WANG, Ant Group, China
MAHANTH GOWDA, Pennsylvania State University, United States
YUANCHUN SHI, Tsinghua University, China
YUNTAO WANG[*], Tsinghua University, China

As smart wearable devices become increasingly powerful and pervasive, protecting user privacy on these devices has emerged as a critical challenge. While existing authentication mechanisms are available for interaction-rich devices such as smartwatches, enabling on-device authentication (ODA) on interaction-limited wearables, including rings, earphones, glasses, and wristbands, remains difficult. Moreover, as users increasingly own multiple smart devices, relying on device-specific authentication methods becomes redundant and burdensome. To address these challenges, we present PPGTransID, a ubiquitous and unobtrusive cross-device authentication (CDA) approach that leverages the real-time physiological consistency of photoplethysmography (PPG) signals across the human body. PPGTransID utilizes the widely available PPG sensors on wearable devices to capture users' physiological signals and compares them with remote PPG (rPPG) signals extracted from a smartphone camera, where robust face-based authentication is already established. In doing so, PPGTransID securely transfers the reliable authentication status of the smartphone to nearby wearable devices without requiring additional user interaction. An evaluation (N=33) shows that PPGTransID achieves a balanced accuracy of 95.5% and generalizes across multiple wearable form factors. Robustness experiments (N=10) demonstrate resilience to variations in lighting, camera placement, and user behavior, while a real-time usability study (N=14) confirms reliable performance with minimal interaction burden. Finally,

[†]Co-first authors.
[*]Corresponding author.

Authors' Contact Information: Jiacheng Liu, Tsinghua University, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Beijing, China, e-mail: jl4596@cornell.edu; Jiankai Tang, Tsinghua University, Department of Computer Science and Technology, Beijing, China, e-mail: tjk24@mails.tsinghua.edu.cn; Guangye Zhao, Tsinghua University, Beijing, China, e-mail: zhaogy23@mails.tsinghua.edu.cn; Ruichen Gui, University of Washington, Seattle, Washington, United States, e-mail: ruichg@uw.edu; Songqin Cheng, Tsinghua University, Beijing, China, e-mail: csq24@mails.tsinghua.edu.cn; Taiting Lu, Pennsylvania State University, University Park, Pennsylvania, United States, e-mail: txl5518@psu.edu; Jian Liu, Ant Group, Hangzhou, Zhejiang, China, e-mail: rex.lj@antgroup.com; Weiqiang Wang, Ant Group, Hangzhou, Zhejiang, China, e-mail: weiqiang.wwq@antgroup.com; Mahanth Gowda, Pennsylvania State University, Computer Science and Engineering, University Park, Pennsylvania, United States, e-mail: mahanth.gowda@psu.edu; Yuanchun Shi, Tsinghua University, Department of Computer Science and Technology, Beijing, China, e-mail: shiyc@tsinghua.edu.cn; Yuntao Wang (corresponding author), Tsinghua University, Department of Computer Science and Technology, Beijing, China, e-mail: yuntaowang@tsinghua.edu.cn.



This work is licensed under a Creative Commons Attribution 4.0 International License.
© 2026 Copyright held by the owner/author(s).
ACM 2474-9567/2026/9-ART129
https://doi.org/10.1145/3831968

a deployment on commercial hardware (N=10) confirms the practicability of PPGTransID in out-of-lab scenarios and its resistance to synchronized rPPG injection attacks.

CCS Concepts: • **Human-centered computing** → *Ubiquitous and mobile computing systems and tools.*

Additional Key Words and Phrases: Authentication, Wearable Device, Smart Sensing, Photoplethysmography

ACM Reference Format:
Jiacheng Liu, Jiankai Tang, Guangye Zhao, Ruichen Gui, Songqin Cheng, Taiting Lu, Jian Liu, Weiqiang Wang, Mahanth Gowda, Yuanchun Shi, and Yuntao Wang. 2026. PPG as a Bridge: Cross-Device Authentication for Smart Wearables with Photoplethysmography. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 10, 3, Article 129 (September 2026), 31 pages. https://doi.org/10.1145/3831968

1 INTRODUCTION

Identity authentication is a prerequisite for the growing role of smart wearables in healthcare, communication, and payment. Yet many wearables that can handle sensitive tasks are poorly equipped to authenticate users on their own. Interaction-limited wearables such as smart rings, earphones, glasses, and wristbands lack the screens, compute, and sensing that conventional On-device Authentication (ODA) presumes, which requires per-device template enrollment and on-device verification. Even where ODA is feasible, its enrolled templates degrade over time as users' physiological and behavioral characteristics drift [16], and repeating this enrollment on every device a user owns is redundant and burdensome. As users increasingly wear several such devices at once, authenticating each of them independently becomes impractical.

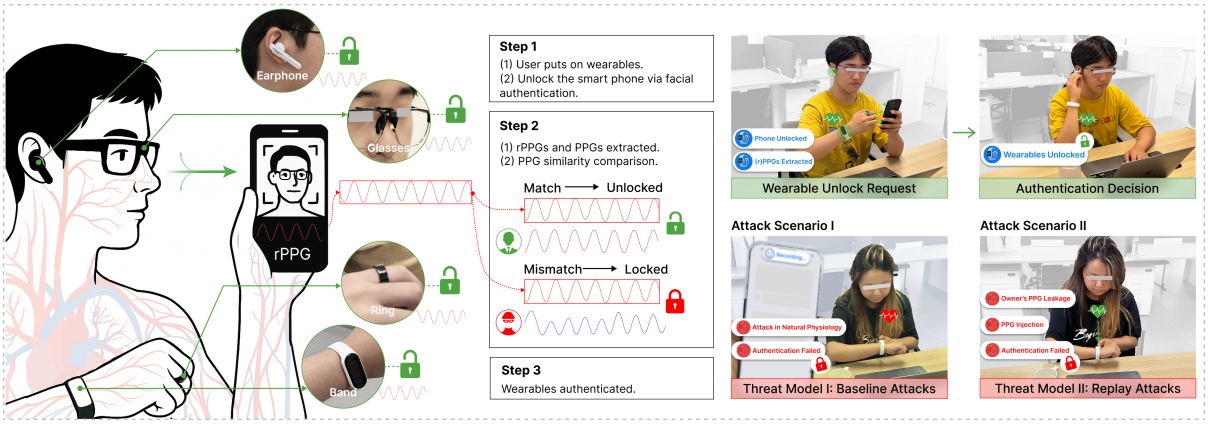


Fig. 1. **System Overview of PPGTransID.** PPGTransID is a cross-device authentication method that leverages the physiological consistency between rPPG signals captured by smartphones and PPG signals from smart wearables to transfer authentication status from the smartphone to co-worn devices. By doing so, it enables ubiquitous and unobtrusive authentication, allowing users to authenticate multiple wearables during everyday smartphone use with minimal disruption.

A promising alternative is **Cross-device Authentication (CDA) [17]**, where identity verified on a trusted token device [12] is transferred to co-worn devices. Since the token device has already authenticated the user through mature methods such as FaceID or fingerprint recognition, co-worn wearables need only confirm shared user presence rather than authenticate from scratch; the paired Apple Watch that unlocks when its owner unlocks an iPhone is a familiar example. By shifting the authentication burden to a capable token device, CDA sidesteps the per-device enrollment and template drift that limit ODA. Consequently, the key to CDA lies in reliably confirming co-presence: that the token device and the co-worn wearable are on the same person at the moment

of transfer. However, existing CDA confirms co-presence through synchronized human motion [12, 18, 35, 65] or vendor-specific proximity [43], each of which demands explicit user action, activity-dependent patterns, or brand-locked trust. What remains missing is a co-presence signal that is *unobtrusive, cross-vendor, and generalizable across heterogeneous wearables*.

Our key insight is that PPG provides exactly such a signal, not as an identity biometric, but as a real-time, cross-body consistency check. Blood volume pulses driven by the same heartbeat manifest at different body sites, so PPG measured at two locations on one person exhibits a consistency that PPG from two different people does not—precisely the co-presence property that CDA requires. With remote PPG (rPPG) extraction, capable token devices such as smartphones can be brought into the CDA system to serve as a reliable identity source: identity established on the smartphone effectively travels through the body, authenticating co-worn wearables via co-presence confirmation grounded in PPG consistency. Realizing this insight, however, is non-trivial: (1) the token device senses PPG remotely and contactlessly from a face video, whereas the wearable senses it through skin contact, and the two modalities must be aligned and matched despite differing noise, sampling rates, and waveform morphology; (2) differences in sensor vendor and sensing location further vary signal quality and PPG morphology across devices; and (3) non-ideal conditions such as lighting, camera position, and head movement introduce non-negligible artifacts that can degrade co-presence confirmation. Given these challenges, we frame our central research question as: ***Can the real-time consistency between smartphone-extracted rPPG and wearable-captured PPG serve as a practical, ubiquitous basis for cross-device authentication across heterogeneous smart wearables?***

Guided by this question, we present PPGTransID, a PPG-based CDA system that confirms co-presence between a smartphone and co-worn wearables without explicit user action. As shown in Figure 1, when a user unlocks their smartphone via facial authentication, the front camera captures a short face video in the background while the co-worn wearables simultaneously record PPG from their embedded optical sensors. PPGTransID extracts rPPG from the face video, aligns it with the wearable PPG, and computes a consistency score to decide whether the two signals originate from the same person; once confirmed, the smartphone's verified identity is transferred to the wearables, and the authenticated state is subsequently maintained through mechanisms such as wear detection [25] or continuous heart-rate monitoring [1]. To make this reliable in practice, PPGTransID addresses the three challenges above: a preprocessing and cross-modal alignment pipeline reconciles the differing noise, sampling, and morphology of contactless rPPG and contact PPG; its feature design remains robust to variation in sensor vendor and sensing location across heterogeneous wearables; and its performance is validated under non-ideal lighting, camera placement, and head movement.

We evaluate PPGTransID through four complementary user studies. A controlled offline benchmark (Study 1, N=33) across four wearable form factors—a custom band, ring, and glasses, and a commercial earphone—achieves a balanced accuracy (BAC) of 95.5% without per-user calibration, while remaining lightweight (0.46 M parameters) and low-latency (9.3 ms). A robustness study (Study 2, N=10) confirms that variations in lighting, camera-to-face distance, and head motion introduce no significant impact on accuracy. A real-time deployment on an iPhone 15 and a laptop (Study 3, N=14) attains a BAC of 97.7% under everyday screen use, with participants reporting favorable perceptions of usability. Finally, a fully off-the-shelf deployment on a Samsung Galaxy Watch 6 paired with iPhones, evaluated in two out-of-lab settings against a stronger attacker (Study 4, N=10), sustains BACs above 97.7% and remains robust to synchronized rPPG injection. Taken together, these results form the major contributions of this paper:

- We are the first to use the cross-modal consistency between smartphone rPPG and wearable contact PPG as a transferable authentication signal. By reframing PPG as a live co-presence cue rather than a stored per-device template, this enables cross-device authentication that is free of the template aging,

per-device enrollment interaction, and on-device compute and storage constraints inherent to on-device authentication.
- We design a device- and modality-agnostic pipeline that reconciles heterogeneous PPG signals into a unified 21-dimensional pairwise representation, enabling PPGTransID to generalize across unseen wearables and alternative token devices without per-user calibration.
- We conduct a comprehensive evaluation with 67 participants in total, covering resilience to three formalized threat models, generalizability across unseen wearables, alternative token devices, and commercial hardware, and robustness against transmission latency (WiFi and BLE), non-ideal lighting and user behavior, and out-of-lab settings.

2 RELATED WORK

2.1 Cross-device Authentication

CDA extends authentication beyond a single device by securely transferring identity from a trusted device to others. Early work showed that signals observable across devices can provide such a basis, including ambient RF noise [24], hand resonance [61], bodily electrical response [63], bone conduction [62], and heartbeat-based cross-modal keys [64]. These established the feasibility of shared physical or physiological features, but operated at the pairing or key-generation level rather than confirming co-presence for authentication transfer.

More explicit forms of CDA establish co-presence through synchronized human motion. ShakeUnlock [12] transfers an unlocked status by matching shaking patterns between devices; SAW [35] authenticates desktop computers from wristband motion; No-Need-to-Shake-It [65] correlates motion between a wristband and inertial-equipped objects; and Au-Id [18] identifies users from RFID-sensed activity. These demonstrate that body motion can act as a transferable cue, but they rely on explicit user movement or activity-dependent patterns, which add interaction overhead and are infeasible for head-worn wearables such as glasses and earphones that are not moved in concert with the token device. A second line relies on proprietary, proximity-based device trust, such as an iPhone unlocking a paired Apple Watch after FaceID; however, proximity does not guarantee that two devices are worn by the same person, and such trust is confined to a single vendor and exposed to relay or proximity attacks [43].

Across these paradigms, co-presence is established either through motion the user must produce or through vendor-specific proximity trust. Neither offers a co-presence channel that is unobtrusive, cross-vendor, and generalizable across heterogeneous wearables. Our work addresses this gap by confirming co-presence from the real-time, cross-body consistency of PPG, a modality already embedded in commodity phones and wearables, requiring no explicit gestures, no additional sensors, and no proximity assumptions.

2.2 Remote Photoplethysmography and Its Use for Authentication

rPPG extraction. rPPG recovers the blood volume pulse from facial video via subtle skin-color changes, offering a contactless alternative to contact PPG. Early methods relied on signal processing and color-space analysis [10, 55, 60], while deep models later learned spatio-temporal representations directly from video, from DeepPhys [7] and PhysNet [68] to transformer- and state-space-based architectures [33, 69, 73]. Most, however, are validated on high-quality, near-stationary video. Since our setting involves handheld phones and continuous use, we build on TN-rPPG [59] for reliable heart-rate extraction under motion and ME-rPPG [58] for real-time waveform estimation, which are designed for mobile deployment.

rPPG for authentication. A growing line of work leverages rPPG as a biometric for ODA. Li et al. [29] match per-user rPPG features from a headset camera against an enrolled template; Geng et al. [14] encode person-specific pulse-transit-time variability across facial ROIs for lightweight ViT classification; and Sun et al. [49] recover individual rPPG *waveform morphology* via rPPG–cPPG hybrid training. rPPG is also fused with face recognition

as a liveness cue [66]. These works establish rPPG as a viable authentication signal, but each operates within a single device under ODA and verifies identity by matching identity-discriminative rPPG features against a per-user template.

Such template matching depends on recovering stable, person-specific morphology, which is intrinsically hard. rPPG extractors are optimized for heart-rate accuracy, and faithful morphology reconstruction remains open [49], while enrolled templates also drift over time. Rather than requiring rPPG to carry a durable identity template, we use only the time-varying cardiac dynamics shared across body sites, confirming identity through the consistency between smartphone rPPG and wearable PPG. Because consistency needs neither faithful per-subject morphology nor a stored template, it offers a new, more robust path for rPPG-based authentication, letting a smartphone with mature facial authentication serve as a reliable identity source within a CDA system.

2.3 Authentication on Smart Wearables

Wearable authentication has been studied across multiple device form factors, ranging from wristbands to earbuds and smart glasses. PPG-based approaches have been proposed for on-wrist wearable authentication, where commercial devices such as Samsung Gear and Empatica E4 have demonstrated continuous implicit authentication in daily life [11]. Building on this, PPGPass [6] employed dual-channel PPG with adaptive filtering to improve robustness, while M-PPG [40] introduced motor-induced vibrations to enhance signal distinctiveness, though all remain tied to per-device enrollment. Moving from the wrist to the ear, EarPass [28] explored in-ear PPG with a quality assessment for motion artifacts, and EarID [19] advanced ear canal sensing, achieving 98.1% balanced accuracy but requiring specialized sensors. Extending further to head-mounted devices, SkullID [46] leveraged through-skull sound conduction for smartglasses, achieving error rates below 3% with robustness to donning variations, yet still confined to glasses-specific acoustic hardware.

These studies reveal the rich potential of physiological and anatomical signals for wearable authentication, but they share fundamental limitations: device-specific design, template-based registration, and limited generalizability across heterogeneous devices. In contrast, our work leverages PPG consistency between smartphones and wearables to transfer identity across devices, eliminating per-device enrollment while ensuring long-term reliability and low-burden user experience.

3 SYSTEM OVERVIEW

As illustrated in Figure 1, PPGTransID consists of three components: (1) smart wearables with embedded PPG sensors, (2) a mobile phone registered to the legitimate user via face-based authentication, and (3) a CDA process running on the phone that pairs the two signals and issues an authentication decision. In this work, we focus on four interaction-limited wearable form factors—smart earphones, glasses, rings, and bands—for which standalone on-device authentication is immature.

3.1 Theory of Operation

PPG, as a widely adopted and commercially mature sensing modality, exhibits three properties that make it a promising substrate for a unified, form-factor-agnostic CDA mechanism: (1) PPG signals from devices on the same user are correlated under proper preprocessing, despite morphological and noise differences, (2) it preserves sufficient inter-user distinctiveness for reliable authentication, and (3) it exhibits transient, moment-to-moment variations.

Cross-device consistency. PPG is an optical signal that reflects changes in light absorption and scattering induced by cardiac-driven pulsatile blood flow. Although differences in hardware characteristics and local tissue properties introduce morphological variations and small temporal offsets in PPG waveforms captured at different body locations, synchronized cross-device PPG signals still exhibit high correlation. Prior studies have shown that

these signals share common physiological features, such as heart rate and pulse rate variability, across devices worn by the same individual [3, 5, 38, 71].

Inter-user distinctiveness. PPG features exhibit substantial inter-user variability arising from physiological factors such as age, medical conditions, sex, and body mass index, which provides a natural basis for user discrimination [2, 37, 41]. Using the data collected in Study 1 (Section 5), we observe that synchronized cross-device PPG signals from the same user demonstrate significantly higher similarity than those from different users. Specifically, synchronized intra-user PPG pairs achieve a higher Pearson correlation (mean = 0.830, SD = 0.070) and coherence similarity (mean = 0.743, SD = 0.071). In contrast, inter-user PPG pairs exhibit substantially lower correlation (mean = 0.501, SD = 0.007) and coherence similarity (mean = 0.326, SD = 0.053).

Temporal variations. While prior work on PPG-based ODA has demonstrated that PPG signals contain stable morphological characteristics over time [6, 40, 52, 56, 72], these signals also exhibit natural temporal variations driven by dynamic cardiac activity. This variability allows PPG to support secure CDA without explicit template registration. We exploit it as the basis for pairwise feature extraction in Section 4.4 and empirically verify it in Section 5.6.

3.2 Threat Model

We consider an attacker A who has illegally obtained a wearable device W and aims to deceive the authentication system into believing that a legitimate user L is wearing and using W. We examine three threat models of increasing sophistication.

Threat Model I: Baseline attacks. A wears the stolen W and attempts to authenticate using their own physiological signals. Specifically, A wears W while L unlocks their mobile phone and initiates the CDA process. This model evaluates whether the system can be fooled by cross-device signals originating from different users.

Threat Model II: Time-shifted replay attacks. A obtains recorded PPG signals of L through unintended leakage or external monitoring, and injects them into the stolen W while L initiates the CDA process. Because acquiring, storing, and relaying PPG through realistic side channels inevitably introduces delay, the replayed signal is not synchronous with L's current physiological state. This model assesses whether the system can be deceived using a legitimate user's historical physiological data, a widely recognized risk in biometric authentication [47].

Threat Model III: Synchronized rPPG injection attacks. A covertly captures L's facial video in real time, extracts rPPG from the captured video using the same pipeline as the legitimate system, and streams the extracted signal into the stolen W at the moment L initiates authentication. Unlike Threat Model II, the injected signal reflects L's live physiological state, eliminating the time-shift defense.

Adversary capabilities and assumptions. Across all three threat models, we assume the attacker **(i)** has no privileged access to device internals or firmware on either the phone or the wearable; **(ii)** cannot bypass the authenticated, encrypted channel between the phone and paired wearables (e.g., the Bluetooth pairing layer); **(iii)** cannot exert fine-grained voluntary control over their own PPG waveform, since PPG reflects involuntary cardiac activity; **(iv)** cannot capture and replay the legitimate user's PPG with zero latency, as realistic side channels inevitably introduce delay (Threat Model II); and **(v)** for Threat Model III, captures the user's facial video covertly with a consumer-grade camera, rather than with specialized long-focal-length or high-SNR optics.

3.3 Hardware Implementation

We developed three custom wearable devices (a ring, a band, and glasses), along with a commercial TH2318 PPG earphone, to support the study objectives. Additional equipment included a commercial CMS50E+ pulse oximeter, an OPPO A52 smartphone (for earphone data recording), an OPPO Find X3 Pro (for fingertip video capture), an iPhone 15 (for facial video capture), and an ASUS ROG Strix G15 G513QM laptop (for recording PPG signals from the custom wearables).

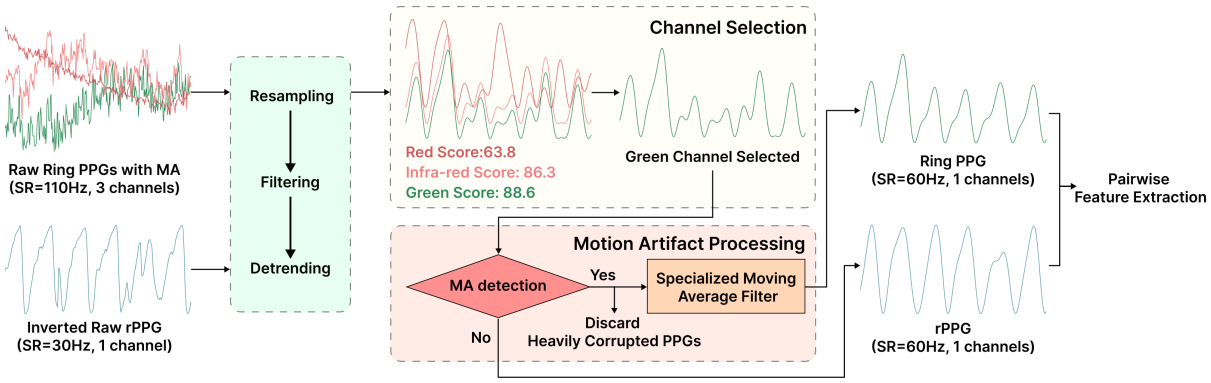


Fig. 2. **Preprocessing Pipeline.** To normalize PPG signals across devices and sensing modalities, signals are resampled, filtered, and detrended. For multi-channel devices, a quality score is computed for each channel, and the best channel is selected. MA processing classifies signals as clean, weakly corrupted, or heavily corrupted; heavily corrupted signals are discarded, while weakly corrupted signals are mitigated using a specialized moving average filter. Pairwise features are then extracted from the cleaned PPG pairs.

All custom devices shared the same electronic components but differed in mechanical design and configuration to optimize signal quality at their respective measurement sites. Each device employed an Analog Devices MAX30101 optical sensor, commonly used in prior work [21, 42]. To accommodate variations in skin and vascular properties across different body sites, LED drive currents were individually tuned to ensure sufficient signal amplitude. The sensors were driven by an nRF52832 microcontroller, which streamed PPG signals via USB to a laptop at 110 samples per second.

The custom devices were encased in 3D-printed, skin-safe thermoplastic polyurethane (TPU) enclosures designed to fit the anatomical contours of the measurement sites and maintain stable sensor–skin contact. As shown in Figure 4, the ring placed the sensor on the proximal phalanx of the index finger, the band positioned it on the dorsal forearm, and the glasses located it on the lateral side of the nasal bridge — the most commonly adopted site for PPG monitoring in glasses form factors [8, 45].

4 SYSTEM PIPELINE

In Section 1, we identified two core challenges for adapting PPG to CDA: (C1) PPG signals from different devices and sensing modalities (notably the contact-PPG vs. camera-rPPG split) vary substantially in SNR, waveform morphology, available channels, and sampling rates; and (C2) while PPG carries temporally stable features, CDA must instead exploit transient, moment-to-moment fluctuations as the basis for verifying co-presence across devices. To address both, we propose a unified preprocessing pipeline that reconciles cross-source discrepancies among PPG signals and yields consistent pairwise features for transient feature extraction.

4.1 rPPG Extraction

We employed two complementary approaches to extract rPPG signals from facial videos. The first is a temporal normalization–based rPPG method (TN-rPPG [59]), which processes 160 consecutive frames to generate a continuous waveform. By leveraging long temporal context, it is robust to subtle head motion and hand tremors, making it suitable for benchmarking authentication accuracy in controlled settings.

To support real-time interaction, we additionally used a memory-efficient single-frame inference method (ME-rPPG [58]), which estimates rPPG signals in a streaming, frame-by-frame manner. Although initially less stable, its state-space design adapts over time and enables responsive real-time use in usability experiments.

Both methods follow a shared pipeline consisting of facial video capture, region-of-interest detection and cropping, frame preprocessing (36×36), model inference, and waveform output. For clarity, we refer to TN-rPPG as Video-based rPPG and ME-rPPG as Frame-based rPPG throughout the paper.

4.2 Cross-Device Signal Normalization

To address challenge C1, we normalize the cross-source variance in PPG captured from different devices and modalities through a sequence of source-specific and shared preprocessing steps (as shown in Figure 2).

We first invert the rPPG signals before further processing, as both models are trained using an MSE loss to reconstruct transmission-mode PPG captured by a clip-based sensor, whose polarity is opposite to that of reflectance PPG from wearables [44]. We then apply a Butterworth bandpass filter (0.5–2 Hz) to all PPG signals, covering the typical resting heart rate range (48–100 bpm). All signals are subsequently resampled to 60 Hz, segmented into 12-second windows, and detrended using the DC-removal method of Hung et al. [20].

As different wearable devices provide different numbers and types of PPG channels, we perform channel selection to select the channel with the best signal quality and unify the number of channels across devices. Prior studies have shown that skewness (Sk) [72], kurtosis (Ku) [6, 27], relative spectral power (Rp) [9], and template matching score (Tm) [30, 39] are useful indicators for MA detection. However, we observe that the distributions of these metrics vary substantially across devices, making it difficult to define a single device-agnostic threshold. To address this challenge, we compute a unified channel quality score Q for each PPG channel as:

$$Q = \lambda_{\mathrm{Sk}}\, \mathbb{I}(-0.5 \le \mathrm{Sk} \le 0.8) + \lambda_{\mathrm{Ku}}\, \mathbb{I}(\mathrm{Ku} \le 0.7) + \lambda_{\mathrm{Rp}}\, \mathrm{Rp} + \lambda_{\mathrm{Tm}}\, \mathrm{Tm} \tag{1}$$

where $\mathbb{I}(\cdot)$ is an indicator function that equals 1 if the condition holds and 0 otherwise. Sk and Ku denote the skewness and kurtosis of the segment; $\mathrm{Rp} \in [0, 1]$ is the relative spectral power, defined as the fraction of spectral energy within the cardiac band (0.5–2 Hz); and $\mathrm{Tm} \in [0, 1]$ is the template matching score between each detected pulse and the segment-level average pulse template. We treat skewness and kurtosis as binary indicators, as long as they fall within empirically reasonable ranges, since their exact values do not reliably reflect signal quality across devices. We set $\lambda_{\mathrm{Sk}} = \lambda_{\mathrm{Ku}} = 0.1$ and $\lambda_{\mathrm{Rp}} = \lambda_{\mathrm{Tm}} = 0.4$, giving higher weight to the two continuous indicators whose values directly reflect signal quality and lower weight to the binary indicators that only provide coarse pass/fail evidence. The channel with the highest Q is selected for subsequent processing. See Appendix A.1 for details on this parameter choice.

4.3 Motion Artifact Processing

To manage motion artifacts (MA), we categorize signal segments into three classes: clean, weakly corrupted, and heavily corrupted. Segments with a relative spectral power score above 0.4 and a template-matching score above 0.95 are classified as clean. The remaining segments are further evaluated using three criteria: (1) at least two pulse cycles with template-matching scores exceeding the same 0.95 threshold; (2) temporal stability of inter-beat (RR) intervals, defined as a coefficient of variation $\sigma_{\mathrm{RR}}/\mu_{\mathrm{RR}} < 0.2$; and (3) physiological plausibility, with all RR intervals falling within $[0.6, 1.25]$ s, which is the same heart-rate range used in earlier filtering. A segment satisfying all three criteria is labeled as weakly corrupted; otherwise it is discarded as heavily corrupted. Weakly corrupted segments are retained for mitigation using a specialized moving-average filter [72].

Signals passing MA processing are segmented into fixed 6-second windows. Each segment is standardized and smoothed using a 3rd-order Savitzky–Golay filter. Using the dataset from Study 1 (5), we evaluate performance

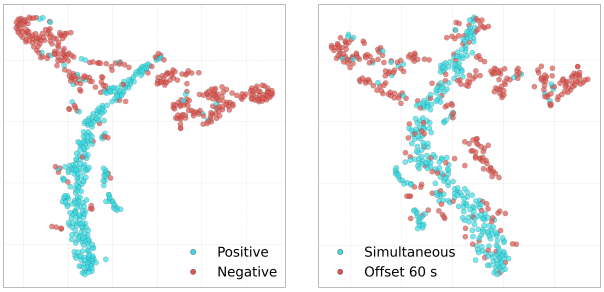


Fig. 3. **t-SNE Visualization of Features.** Features from 5 random subjects before classifier implementation. (a) Blue: signals synchronously collected on different devices from the same subject. Red: signals from different subjects on different devices. (b) Blue: same as (a). Red: pairs from the same subject but with a 60s temporal offset.

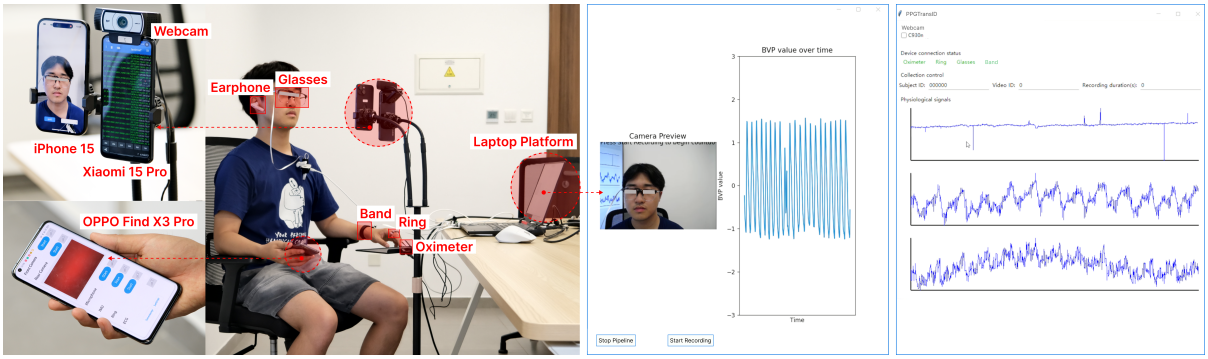


Fig. 4. **Devices and Experimental Setup in Study 1.** Illustration of the experimental setup in Study 1, showing the wearing placements, device arrangements, and the platforms used on the smartphones and laptop.

under shorter durations. While reducing the window length improves user experience, it leads to a gradual decline in accuracy. In the sitting condition, the system achieves 95.5% BAC with a 6-second window, which steadily drops to 90.8% at 3 seconds. To ensure sufficient reliability (BAC > 95%) while minimizing user burden, we adopt a 6-second duration in our system.

4.4 Pairwise Feature Extraction

To address challenge C2, we design a transient feature extraction method based on pairwise differences and similarities between simultaneous signals. From each pair, 21 features are derived: 14 absolute differences (8 time-domain, 6 frequency-domain) and 7 similarity measures (6 time-domain, 1 frequency-domain). Full details of the extracted features are provided in Table 6 in Appendix A.2. Feature selection followed a two-stage process: importance ranking (via XGBoost, Random Forest, and SVM) and ablation analysis. Removing any selected feature consistently degraded performance (e.g., BAC dropped from 95.5% to 95.3% in XGBoost when the least important feature is discarded), confirming their necessity.

Figure 3 visualizes the engineered features using t-SNE on 640 pairs from five randomly selected subjects. In (a), positive pairs (simultaneous signals on different devices from the same subject) and negative pairs (different subjects and devices) form well-separated clusters, demonstrating strong discriminability. In (b), red points denote

time-shifted pairs (60-second offset) from the same subject, which deviate from simultaneous pairs and align more closely with the negative class, confirming that the pairing captures transient, time-varying evidence rather than time-invariant physiological templates, which is the property C2 requires. Importantly, these plots only illustrate distribution trends of features before training; final performance is reported in Section 5.

4.5 Classification Algorithms

We compared six classification models: three traditional machine learning baselines (XGBoost, Random Forest, and SVM) and three deep learning models (Siamese-LSTM, Siamese-ResNet18, and Siamese-RAPID [52]).

4.5.1 Machine Learning Baselines. XGBoost was trained with 100 estimators, a maximum depth of 6, and a learning rate of 0.1. Random Forest used 100 estimators with unrestricted depth, and SVM employed an RBF kernel with default parameters.

4.5.2 Deep Learning Models. For the deep learning approach, we adopted a Siamese architecture [54], which is well suited for comparison tasks such as authentication [23, 26, 36, 65, 74], and is effective even with relatively small datasets. Each network processes paired inputs through shared backbones, and the absolute difference between representations is fed into a fully connected layer for binary classification. We explored three backbone variants: (1) a two-layer LSTM with a hidden size of 512, (2) a standard 1D ResNet18 producing a 64-dimensional representation, and (3) RAPID [52], a lightweight InceptionTime-style [22] architecture with attention mechanisms designed for PPG processing. The RAPID backbone in our implementation contains 18 RAPID blocks, while following the paper's recommended kernel-set size of 9 and output dimensionality of 128.

Prior to training, temporal difference and Welch transform were applied to generate three-channel inputs (original signal, temporal difference, and Welch spectrum). Models were optimized using binary cross-entropy with Adam (learning rate 1×10^{-4}), trained for up to 30 epochs with early stopping (patience = 5).

5 STUDY 1: SYSTEM BENCHMARKING ACROSS WEARABLES AND THREAT MODELS

Study 1 provides the core offline benchmark of PPGTransID under controlled conditions. With 33 participants and four wearable form factors (band, ring, glasses, earphone), we evaluate authentication accuracy across postures (sitting, standing) and rPPG extraction methods (video-based, frame-based), test resistance to baseline and time-shifted replay attacks (Threat Models I and II), and assess generalization to unseen devices, unseen postures, and shorter analysis windows.

5.1 Platform Setup

To support the evaluation study, we developed three data collection platforms: one for laptops and two for smartphones (iOS and Android), as shown in Figure 4.

The laptop platform was implemented in Python with a Tkinter-based interface. It automatically discovered and connected to the custom wearable devices (Section 3.3). The platform visualized incoming PPG signals in real time. PPG signals, IMU data, and Unix timestamps were continuously logged during data collection.

For smartphones, we implemented two dedicated video recording platforms. The iOS application recorded facial videos using the front-facing camera, while the Android application recorded fingertip videos using the back camera. We also experimented with Android phones for facial video recording (tested on Xiaomi 15 Pro and OPPO Find X3 Pro). However, the Android devices apply non-configurable video compression, which significantly degraded the rPPG signal quality compared to iPhones. For both platforms, each video frame was timestamped and synchronized.

Table 1. Different Models' Performance under Different Postures. Mean BAC of different methods under sitting (21,930 pairs) and standing (14,980 pairs) postures using LOSO validation on 33 subjects. XGBoost consistently achieved the highest accuracy across both conditions.

Method	**Size**	**Sitting**			**Standing**		
		EER(%) ↓	AUC(%) ↑	BAC(%) ↑	EER(%) ↓	AUC(%) ↑	BAC(%) ↑
Siamese-LSTM	12.1M	8.00 (5.61)	96.2 (4.48)	92.8 (5.46)	10.3 (4.17)	95.4 (2.53)	90.7 (3.74)
Siamese-ResNet18	14.8M	8.10 (2.19)	96.6 (1.37)	92.8 (2.03)	11.3 (3.74)	94.9 (2.70)	90.0 (3.40)
Siamese-RAPID	2.28M	5.77 (1.77)	98.0 (0.87)	95.1 (1.63)	8.85 (3.20)	96.0 (1.97)	92.3 (2.93)
SVM	16.0M	9.24 (3.54)	96.8 (1.63)	91.7 (2.78)	13.1 (5.22)	94.0 (3.79)	88.2 (4.28)
Random Forest	198M	5.10 (1.94)	98.6 (0.76)	95.4 (1.81)	7.93 (3.38)	97.2 (2.03)	92.8 (3.06)
XGBoost	**0.46M**	**5.09 (1.86)**	**98.7 (0.73)**	**95.5 (1.66)**	**7.80 (3.41)**	**97.3 (1.93)**	**92.9 (3.05)**

5.2 Methodology

Data were collected in two static postures: sitting and standing, each lasting 10 minutes. We focused on these two conditions, as they represent the most common scenarios in which users interact with smartphones, aligning with the envisioned use cases of PPGTransID . Temperature and illuminance near the participant's face were measured at the start of each experiment.

To synchronize timestamps across platforms (e.g., smartphones and the laptop), all devices were placed together in a box and subjected to three controlled drops prior to the experiment, allowing alignment via IMU peak detection. During data collection, an iPhone 15 and an external Logitech C930 webcam were positioned in front of participants for facial video capture. The ring, band, and oximeter were worn on the non-dominant hand, while the OPPO Find X3 Pro was held in the dominant hand, with its back camera covered by the participant's fingertip.

Each session lasted approximately 35 minutes. Participants received compensation equivalent to 8.5 USD in local currency. The study protocol was reviewed and approved by the university's Institutional Review Board (IRB).

5.3 Demographics

We recruited 33 participants (16 male, 17 female) with a mean age of 22.7 years (SD = 3.28, range = 18–30), 32 of whom were right-handed. The inclusion criterion was the absence of any diagnosed cardiac disease; no other physiological conditions were restricted.

5.4 Evaluation Setup

We adopted a leave-one-subject-out (LOSO) validation strategy, where models were trained on data from all but one participant and tested on the held-out participant.

rPPG signals were extracted from facial videos using both video-based and frame-based methods, and all PPG signals were then grouped into pairs for evaluation. Positive pairs consisted of signals from the same subject collected simultaneously on different devices, while negative pairs consisted of signals from different subjects and devices. Notably, non-simultaneous signals from the same subject were excluded from positive pairs (except in Section 5.6). In testing pairs, one PPG signal was always taken from a token device (e.g., smartphone, laptop, or band; smartphone with the video-based rPPG extraction by default), while the other was taken from a wearable. For training, a 2-second overlap was applied for data augmentation.

Table 2. Performance of video-based and frame-based rPPG extraction across four wearable devices in sitting and standing postures.

Type	Device	Sitting			Standing		
		EER(%) ↓	AUC(%) ↑	BAC(%) ↑	EER(%) ↓	AUC(%) ↑	BAC(%) ↑
Video-based rPPG	Band	4.67 (2.39)	98.7 (1,06)	96.2 (2.09)	9.01 (6.75)	95.8 (5.65)	92.5 (5.90)
	Ring	2.57 (2.01)	99.4 (0.69)	98.1 (1.53)	6.18 (4.24)	97.8 (2.10)	95.2 (3.28)
	Glasses	6.99 (4.49)	97.3 (2.84)	94.4 (3.72)	7.18 (7.13)	96.7 (5.82)	94.4 (4.83)
	Earphone	4.65 (2.91)	98.6 (1.25)	96.2 (2.34)	6.55 (4.67)	97.6 (3.12)	94.6 (3.39)
	Total	5.09 (1.86)	98.7 (0.73)	95.5 (1.66)	7.80 (3.41)	97.3 (1.93)	92.9 (3.05)
Frame-based rPPG	Band	5.86 (3.02)	98.2 (1.59)	95.2 (2.54)	11.5 (8.23)	94.4 (7.32)	90.8 (7.01)
	Ring	3.64 (2.45)	99.1 (3.31)	97.2 (1.02)	5.98 (3.37)	97.7 (2.00)	95.1 (2.65)
	Glasses	8.55 (5.39)	96.3 (3.57)	93.2 (4.28)	11.7 (8.90)	94.3 (7.60)	90.9 (6.71)
	Earphone	6.18 (3.56)	9.81 (2.45)	95.4 (3.09)	7.92 (4.34)	97.0 (3.93)	93.4 (4.00)
	Total	6.14 (2.82)	98.1 (1.26)	94.5 (2.60)	9.07 (3.78)	96.6 (2.17)	91.7 (3.32)

To balance the dataset, the number of negative pairs was matched to that of positive pairs. Approximately 22 k pairs were generated for testing in the sitting scenario and 15 k in the standing scenario. The exact counts varied depending on the specific evaluation setup.

We adopt balanced accuracy (BAC) as the primary evaluation metric, defined as the average of the true positive rate and true negative rate. For each evaluation, we select the decision threshold that maximizes BAC. We additionally report the Area Under the Receiver Operating Characteristic Curve (AUC) and the Equal Error Rate (EER). AUC captures the overall discriminative capability of the system across thresholds, while EER corresponds to the operating point where the false acceptance rate equals the false rejection rate. An ideal authentication system achieves BAC = 1.0, AUC = 1.0, and EER = 0. All metrics are computed as weighted averages across subjects, with weights proportional to the number of test pairs per subject.

5.5 Classifier Comparison and Resistance to Baseline Attacks

To compare the methods and assess PPGTransID 's resistance against baseline attacks, we used rPPG signals extracted from iPhone 15 facial videos as the token device signals. Detailed results are reported in Table 1. We further benchmarked inference latency and model size (parameters) on an Intel Xeon Gold 5218 CPU and an NVIDIA RTX 3090 GPU. The results are summarized in the bubble plot in Figure 5 (a). Notably, feature extraction time was included for traditional machine learning models (i.e., XGBoost, Random Forest, and SVM).

5.5.1 Classifier Selection. As shown in Table 1, XGBoost achieved the best overall trade-off, reaching the highest BAC in both postures (95.5% sitting, 92.9% standing) with only 0.46M parameters and a latency of 9.3 ms. Random Forest and Siamese-RAPID yielded comparable accuracy but required substantially higher complexity and slower inference. Siamese-LSTM and Siamese-ResNet18 delivered comparable BACs but required more memory and incurred longer latency. SVM lagged further behind with a ∼4% drop while having a larger model size.

We attribute the lower performance of deep learning models to two factors: the relatively small dataset size and the simplicity of the features required for this task, which traditional models can capture more effectively.

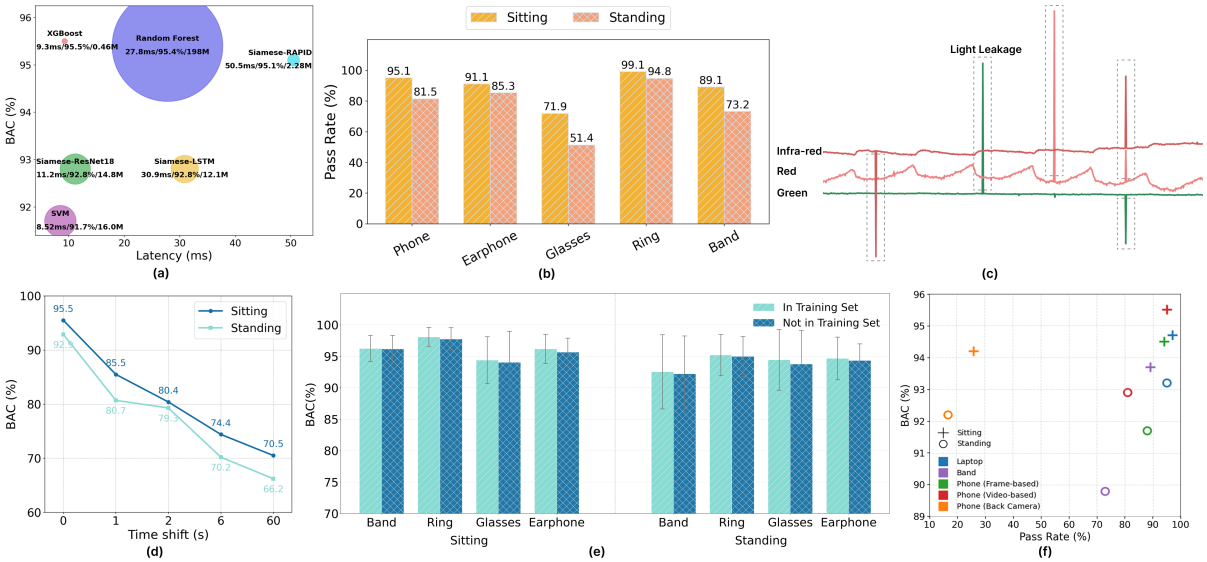


Fig. 5. **Study 1 Results.** (a) Trade-off among model performance, inference latency (x-axis), and parameter count (bubble size); XGBoost achieves the best overall balance. (b) Signal pass rates across the smartphone (video-based rPPG), earphone, glasses, ring, and band under sitting and standing postures. (c) Example of light leakage observed in the glasses prototype, partially explaining its lower pass rate in (b). (d) BAC decays steadily with increasing temporal offset between rPPG and wearable PPG, indicating that the system relies on instantaneous synchrony and is resistant to time-shifted replay attacks. (e) BAC when each wearable is excluded from the training set; performance changes by less than 1%, demonstrating generalization to unseen wearables. (f) BAC versus post-MA pass rate across alternative token devices (laptop, band, smartphone back camera, smartphone front camera); the smartphone front camera offers the best trade-off between accuracy and data utilization.

Given this balance of accuracy, memory efficiency, and speed, we adopt XGBoost as the default model in subsequent evaluations. Its performance demonstrates that PPGTransID can effectively resist baseline attacks without subject-specific calibration.

5.5.2 Per-device Evaluation. To evaluate the authentication performance of each device, we formed evaluation pairs between each wearable device and the smartphone, reporting both authentication performance (Table 2) and preprocessing pass rates (Figure 5 (b)).

All wearables achieve favorable accuracy, with performance differences primarily driven by two factors. (1) PPG signal quality varies by body site: fingertip measurements yield the highest SNR, wrist signals are weaker and less stable, and ear-canal and nasal-bridge signals fall in between [4, 15, 53]. (2) The band, ring, and glasses are self-developed prototypes, and design constraints—such as imperfect skin contact, limited LED intensity, and light leakage—further affect signal quality. As shown in Figure 5 (c), severe light leakage in the glasses prototype results in a lower pass rate than other devices, which exceed 90% accuracy in the sitting condition.

We also observe a consistent performance drop in the standing condition compared to sitting, where PPG amplitude and SNR decrease due to reduced perfusion under hydrostatic pressure [4, 31, 70]. The magnitude of degradation varies across devices, with the band (−3.7%) and ring (−2.9%) exhibiting the largest declines, consistent with their more distal vascular supply.

5.5.3 Robustness to rPPG Extraction Methods. Table 2 compares the performance under two rPPG extraction methods. PPGTransID achieves strong performance with both approaches, demonstrating its robustness to different rPPG generation pipelines. The video-based method consistently yields higher accuracy, which can be attributed to its ability to leverage temporal information across the entire window and thus produce higher-quality rPPG signals. Despite this gap, the results indicate that PPGTransID remains effective across both settings, enabling flexible deployment under different system constraints.

5.6 Time-Shifted Replay Analysis

Prior work has shown that PPG contains temporally stable features and can therefore support ODA across sessions; this raises the question of whether leaked historical PPG could threaten the proposed system. To evaluate this, we constructed positive pairs using rPPG and PPG signals from the same subject but recorded at different time intervals, simulating realistic delays in replay attacks. Results are summarized in Figure 5 (d).

We observe a steady decline in accuracy as temporal offsets increase. At a 60-second offset, performance drops sharply to 70.4% (sitting) and 66.2% (standing), indicating that time-shifted pairs are increasingly misclassified as negatives. This suggests that the system primarily relies on transient, temporally aligned features rather than invariant physiological patterns, which limits the effectiveness of replay attacks based on historical signals. However, we do not claim full immunity to replay attacks. Although accuracy declines sharply with increasing offset, it remains well above the chance-level BAC of ∼50% expected of a fully replay-resistant system, indicating that short-window replays still pose a meaningful threat. We discuss complementary mitigations in Section 9.2.

Furthermore, this sensitivity to temporal misalignment may raise concerns regarding usability in real-time deployments, where delays introduced by Bluetooth or WiFi transmission are unavoidable. We investigate this issue in Study 3 (6) and Study 4 (8).

5.7 Ubiquity across Token and Wearable Devices

PPGTransID 's practical utility depends on its ability to operate across heterogeneous devices, both as wearables and token devices. We evaluate this ubiquity by testing generalization to unseen wearables and extending token devices beyond smartphones.

5.7.1 Generalizability to Unseen Devices. To assess generalization to unseen wearables, we adopt a leave-one-device-out strategy, excluding each device from the training set in turn and retraining the model. As shown in Figure 5 (e), excluding any single device results in only marginal performance degradation across both postures. The largest decrease is observed for the earphone in the sitting condition, where BAC drops from 96.2% to 95.6%. This reduction is small in magnitude and suggests that the system maintains broadly stable performance.

5.7.2 Evaluation across Token Devices. While smartphones serve as the primary token device, we further evaluate alternative options. Following the pairing procedure in Section 5.4, we vary the token device at test time among a laptop, a band, the smartphone's back camera (OPPO Find X3 Pro), and the front camera (iPhone 15). For the laptop, rPPG is extracted in real time using a frame-based method; for the back camera, rPPG is derived from fingertip videos [32]. As token devices affect both classification accuracy and motion-artifact (MA) pass rate (Section 4.3), we report both metrics in Figure 5 (f).

Figure 5 (f) shows that the system achieved consistent performance across token devices in the sitting posture, ranging from 93.7% on the band to 95.5% on the smartphone's front camera. In the standing posture, performance remained acceptable on most devices, with the band again being the weakest (89.8%). Device-specific differences reflect both signal quality and stability. The back camera suffered from a low pass rate due to unstable fingertip

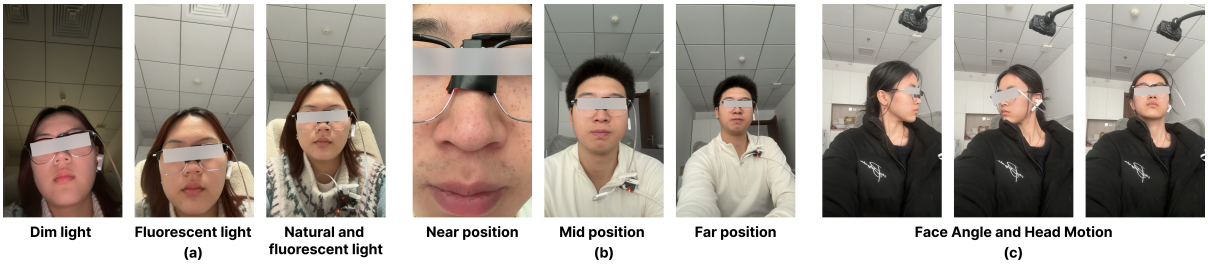


Fig. 6. **Examples of Different Lighting Conditions, Face Angles, and Camera Positionings.** (a) Front-camera frames under dim, fluorescent, and mixed natural–fluorescent lighting. (b) Frames captured at near, mid, and far camera distances. (c) Frames illustrating head motion at the far distance.

contact and light leakage. The front camera and the laptop showed stable performance, while the band was limited by lower signal quality.

6 STUDY 2: ROBUSTNESS UNDER ENVIRONMENTAL AND BEHAVIORAL VARIATIONS

While Study 1 validates the core concept of PPGTransID, Study 2 evaluates its robustness under non-ideal conditions beyond controlled static settings. With 10 participants, we vary environmental and usage factors, including lighting conditions, camera-to-face distance, and head motion, and directly test the pretrained Study 1 model without any fine-tuning.

6.1 Methodology

Using the same platform and hardware setup described in Section 5.1, each participant wore all wearables and held an iPhone 15 to complete three recording sessions, each under a different lighting condition: (1) **dim lighting** with neither natural nor in-door illumination, (2) **fluorescent lighting** only with natural light blocked, and (3) **mixed natural–fluorescent lighting**. Example front-camera frames in each lighting conditions are provided in Figure 6 (a).

As shown in Figure 6 (b), for each lighting condition, participants recorded data at three distances. In the **near position**, the face was placed partially outside the camera frame to simulate partial facial visibility. In the **mid position**, the phone was held at a typical viewing distance during normal use. In the **Far position**, participants fully extended their arm and moved their head (up, down, left, right) to introduce different angles of the face.

At the beginning of each session, we recorded the illuminance level near the participant's face.

Each session lasted approximately 30 minutes. Participants received compensation equivalent to 7 USD in local currency. The study protocol was reviewed and approved by the university's Institutional Review Board (IRB).

6.2 Demographics

We recruited 10 participants (4 male, 6 female) with a mean age of 21.1 years (SD = 2.28, ranging from 18 to 25). None of the participants had taken part in Study 1.

6.3 Influence of Lighting Conditions

To examine how lighting affects the system, we evaluated PPGTransID under diverse illumination levels, ranging from 18 lm to 36,800 lm. The average illuminance for the dim, fluorescent, and mixed natural–fluorescent lighting settings was 145 lm, 361 lm, and 5.68 klm, respectively.

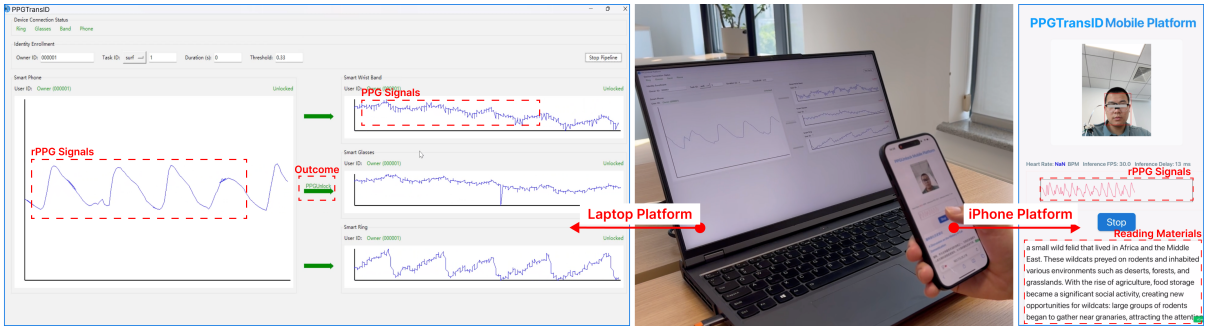


Fig. 7. **Platform Setup in Study 3.** Two platforms (a laptop and an iPhone) were used for system demonstration and real-time performance evaluation. The iPhone runs a web app that extracts and transmits facial rPPG signals in real time to the laptop, which displays PPG/rPPG signals from multiple wearables along with the system interfaces.

For each condition, authentication pairs were constructed using the same procedure as in Study 1 (Section 5.4) and evaluated using the pretrained XGBoost model from Study 1 without any fine-tuning. The resulting BACs were 96.6% (SD = 1.52%), 96.6% (SD = 1.69%), and 96.1% (SD = 2.74%), with rPPG pass rates of 77.8% (SD = 13.2%), 83.8% (SD = 11.7%), and 70.8% (SD = 25.4%) for dim, fluorescent, and mixed lighting conditions, respectively. Although fluorescent light yielded a slightly higher pass rate, Kruskal–Wallis tests found no significant differences in either BAC ($H(2)=2.93$, $p=0.231$) or rPPG pass rate ($H(2)=1.83$, $p=0.400$) across conditions.

6.4 Influence of Camera Positioning and Head Movement

rPPG extraction can be affected by partial facial visibility, extreme face–camera distances, and head movement, potentially impacting authentication reliability. To systematically assess these factors, we grouped them into three representative usage scenarios: (1) **Near position:** the user holds a smartphone at an unusually short distance, causing partial facial occlusion; (2) **Mid position:** typical smartphone usage distance; (3) **Far position:** video-call–like scenarios with long face–camera distance and continuous head movement.

Using the same evaluation procedure as in the previous section, the resulting BACs were 97.5% (SD = 2.05%), 96.9% (SD = 1.83%), and 96.2% (SD = 1.60%) for the near, mid, and far conditions, respectively. Corresponding rPPG signal pass rates were 79.6% (SD = 17.5%), 85.8% (SD = 15.4%), and 66.8% (SD = 21.8%). Kruskal–Wallis tests indicate no significant differences across conditions for either BAC ($H(2)=1.05$, $p=0.591$) or pass rate ($H(2)=4.25$, $p=0.120$).

The evaluations demonstrate that PPGTransID maintains stable authentication performance across diverse lighting conditions, camera positions, and user behaviors—even in extreme scenarios. While certain conditions may reduce rPPG signal pass rates, they do not compromise authentication accuracy. These results indicate that **PPGTransID is robust to real-world variability and holds strong potential for deployment in practical wearable authentication applications**.

7 STUDY 3: REAL-TIME DEPLOYMENT AND USABILITY

Study 3 moves from offline evaluation to live interaction. We implemented PPGTransID as a real-time system running over a LAN (iPhone front camera + laptop classifier) and recruited 14 participants to perform authentication sessions under three live tasks: standard unlock, unlock while scrolling an article, and acting as a baseline attacker. This study evaluates the system's behavior under transmission latency, one-handed smartphone use, and reports usability feedback.

7.1 Platform Setup

To support the study, two platforms are designed, one on a laptop and one on an iPhone 15, as shown in Figure 7.

The iPhone platform was implemented as a web-based application capable of capturing facial videos, extracting rPPG signals, and transmitting them to the laptop in real time. Signal transfer was handled through a self-hosted LAN server. To enhance user experience and improve system interpretability, the frame-based rPPG extraction method was adopted. The web interface included a live camera preview, a pipeline control button, and an AI-generated short article presented in both English and the local language.

The laptop platform was implemented in Python with a Tkinter interface, supporting rPPG reception, PPG collection, signal visualization, and system demonstration. Once the rPPG data were received from the smartphone, the system initiated a 6-second countdown for data collection. Synchronization was not performed in order to evaluate the system's robustness to WiFi transmission latency. Specifically, the laptop-side PPG signal was directly paired with the smartphone rPPG signal received at the same time, without any temporal alignment. After each collection session, the platform automatically executed the proposed system and displayed the results: authenticated wearables were highlighted in green, failed authentications in red, and channels rejected by MA processing turned from light grey to dark grey. The system resets automatically after each evaluation.

7.2 Methodology

The study consisted of three sessions, each including three randomized tasks: (A) self-device authentication, (B) self-device authentication while scrolling, and (C) baseline attacks. Each task was repeated five times per session. The study included the three custom wearables (ring, band, and glasses). The earphone was excluded from the demo because the TH2318 PPG earphone does not provide an open interface for real-time PPG streaming.

In Task A, participants wore the devices (ring and band on the non-dominant hand, iPhone 15 in the dominant hand) and initialized the pipeline by pressing the start button. They then recorded video and signals by looking at the phone in a natural and comfortable posture. Once the laptop displayed the authentication outcome, participants reviewed the result, after which the system reset automatically. Task B followed the same protocol, except participants read and scrolled through an article in a natural position at a normal pace during data collection. In Task C, participants acted as attackers, attempting to unlock the experimenter's wearables. The procedure mirrored Task A, except the smartphone was controlled by the experimenter who acted as the owner.

To account for potential variability, wearables were remounted after each session. After all three sessions, participants completed a post-study questionnaire on usability and perceptions. Each study lasted about 60 minutes, and participants received compensation equivalent to USD 14. The protocol was approved by the university's IRB.

7.3 Demographics

We recruited 14 participants (9 male, 5 female) with a mean age of 24.1 years (SD = 3.48, range : 19–30), 13 of whom were right-handed. None of the participants had taken part in Studies 1 and 2.

7.4 Evaluation Setup

To assess system performance, we recorded the confidence scores of positive predictions generated by the XGBoost model trained in Study 1 without any fine-tuning. We then grouped task pairs (A+C and B+C) to calculate the average BAC across all 14 participants. The results are summarized in Figure 8.

7.5 Real-time Resistance against Baseline Attacks

To evaluate the system's resistance against baseline attacks (Treat Model I) in a real-time demonstration, tasks A and C were grouped to calculate the metrics.

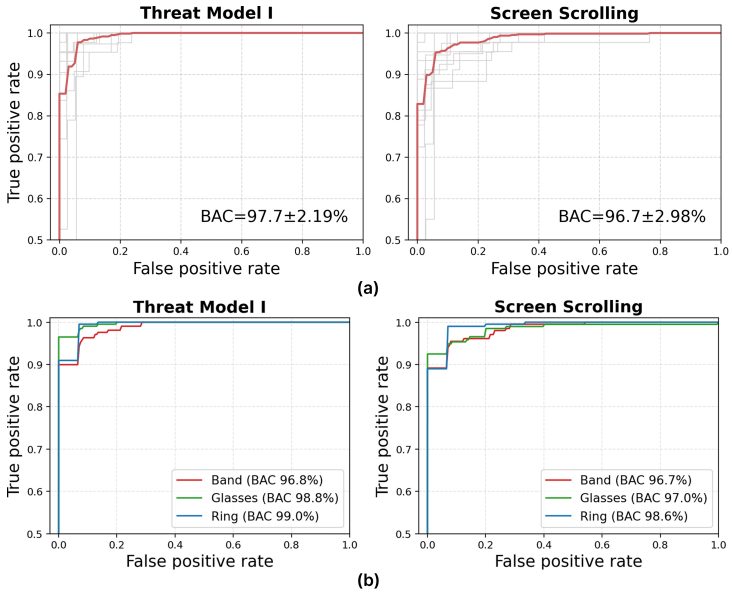


Fig. 8. **Study 3 Real-Time ROC Analysis.** (a) ROC curves aggregated across all three wearables, split by evaluation scenario: Threat Model I (tasks A+C) and CDA during screen scrolling (tasks B+C). Gray lines show per-participant ROCs; red lines show the across-participant average. (b) ROC curves aggregated per wearable device (Band, Glasses, Ring), shown separately for the two scenarios. Some curves appear less smooth due to the limited number of positive–negative pairs per subject-device cell (30 pairs). Together, the two views show that the system maintains high authentication accuracy both across scenarios and across individual wearable form factors.

Figure 8 (a) shows that the system achieved a BAC of 97.7%, outperforming the 95.5% observed in Study 1. This increase was expected, as only two subjects were involved in forming negative pairs and the total number of tested pairs (15, $(repetitions) \times 3$, $(devices) \times 14$, $(subjects) \times 2$, $(tasks) = 1260$ pairs) was much smaller than in Study 1 (21,930 pairs), making the grouping problem relatively easier. Importantly, the system maintained stable performance under LAN-based data transmission latency, typically ranging from 5 to 20 ms [48], suggesting that such network delay does not hinder its functionality.

7.6 Generalizability on Screen Scrolling

We envisioned that PPGTransID could capture facial videos from users in the background, without interrupting ongoing smartphone use. To evaluate its feasibility, tasks B and C were grouped to test the system's reliability under text-reading scenarios.

As shown in Figure 8 (a), the system achieves a BAC of 96.7%. Figure 8 (b) further shows that different devices obtain comparable performance. Among all devices, smart glasses exhibit the largest performance drop of 1.8% compared to the sitting-still condition, indicating that the motion introduced by screen scrolling results in only a minor and acceptable degradation in performance. In practice, smartphone use frequently involves one-handed interaction [67], indicating that our system already covers a large portion of everyday use cases.

Taken together, these results demonstrate the practicality of PPGTransID during one-handed smartphone use. They show that rPPG signals can be reliably extracted from facial videos captured during natural interactions,

enabling authentication with minimal interruption. This highlights the potential to unobtrusively integrate PPGTransID into mobile devices without disrupting user experience.

7.7 Usability Results

Table 3. **Questionnaire dimensions and average scores.** Higher scores indicate more positive evaluation.

ID	Dimension	Average Score
Q1	Smart wearable usage	6.21
Q2	Privacy protection need	6.43
Q3	Understandable	6.35
Q4	Ease of use	6.00
Q5	Authentication time acceptability	5.29
Q6	Low cognitive load	5.14
Q7	Memorability	6.14
Q8	Low physical demand	6.14
Q9	Low effort expended	5.79
Q10	Low frustration	5.64
Q11	Authentication accuracy	5.79
Q12	Attack resistance	6.14
Q13	Reliability	5.93
Q14	Privacy acceptance	5.86
Q15	Social acceptance	5.86
Q16	Tendency to use	5.79
Q17	Potential scalability	6.00
Q18	Potential applications (open question)	N/A
Q19	Open comments	N/A

We administered a 7-point Likert questionnaire covering usage context, perceived efficiency, cognitive and physical demands, reliability, acceptance, and scalability. All 17 items are listed in Table 3, with the full wording in Appendix A.3.

Overall reception. Participants rated PPGTransID positively across dimension (all means $\geq 5.14/7$), with the strongest ratings for explainability (Q3, 6.35), privacy-protection need (Q2, 6.43), and memorability (Q7, 6.14), and the weakest—though still above neutral—for cognitive load (Q6, 5.14) and authentication time (Q5, 5.29). The high Q1 and Q2 scores confirm that the use context and concerns motivating our design are shared by actual wearable users.

Recurring concerns. Open-ended feedback clustered around two themes. First, several participants found the laptop-based interaction slow or effortful (P2, P7, P13, P14), while attributing their cognitive-load ratings to the prototype UI rather than to the authentication pipeline itself—e.g., P6: "results should be displayed on the smartphone instead of the laptop." We note that the laptop in Study 3 was used solely to validate the real-time pipeline end-to-end; a production deployment of PPGTransID is intended to run entirely on the phone, which we demonstrate in Study 4 (8.1). Second, two participants raised concerns about generalization: P7 questioned scalability to larger populations, and P12 worried about robustness after exercise. We acknowledge that the 33-participant Study 1 cohort, while sufficient to establish feasibility, remains limited and may not capture the full variability of users with cardiac conditions or sub-clinical physiological abnormalities; we discuss this bias



Fig. 9. Real-time demonstration of PPGTransID.

explicitly in Section 9.4. Regarding post-exercise use, although heart rate may remain elevated after exercise, such changes are not expected to invalidate PPGTransID.

Envisioned applications. All participants agreed that PPGTransID has broader applicability (Q17, 6.00), spontaneously suggesting use cases in three categories: security and access control (smart-home, vehicle, door, and workplace access; banking MFA), healthcare (patient–record matching, health-data personalization), and privacy-preserving personalization (adaptive car seats, continuous implicit authentication). These scenarios extend beyond wearable CDA and point to a broader design space for physiological identity.

8 STUDY 4: IN-THE-WILD DEPLOYMENT AND SYNCHRONIZED INJECTION ATTACK

To evaluate PPGTransID beyond custom hardware and the time-shifted replay model of Section 5.6, we deployed the system on a Samsung Galaxy Watch and an iPhone, and tested its feasibility in real-world indoor and outdoor settings and its resilience to synchronized rPPG injection attacks on 10 participants.

8.1 Real-Time Deployment on Commercial Devices

To assess the practicability of PPGTransID on off-the-shelf hardware, we implemented the full pipeline on a Samsung Galaxy Watch 6 (Wear OS) and two iPhones (iPhone 15 and iPhone 14 Pro). Signal acquisition, preprocessing, feature extraction, and classification all run natively on-device, with no reliance on external servers or cloud infrastructure.

As shown in Figure 9, the smartwatch streams raw PPG via Samsung's Privileged Health SDK, sampling the green channel at approximately 25 Hz. Each sample is locally detrended with a first-order IIR high-pass filter ($f_c = 0.5$ Hz) and transmitted to the phone through a custom BLE GATT service. Each 8-byte packet carries the sample value and its local timestamp; BLE operates in low-latency mode, yielding an end-to-end delay of 20–50 ms.

The iPhone captures facial video via AVFoundation at 30 fps. Face regions are detected every 10 frames using Vision, and rPPG is extracted from the mean RGB trace of the detected region by the frame-based method. The incoming PPG stream and the extracted rPPG are both resampled to 60 Hz and segmented into 6-second windows. Each segment is detrended, smoothed with a Savitzky–Golay filter, z-score normalized, and bandpass filtered (0.5–2 Hz). A 21-dimensional pairwise feature vector is then fed into an XGBoost classifier, deployed as a JSON model and executed by a lightweight native tree-walker in Swift. We do not perform explicit cross-device

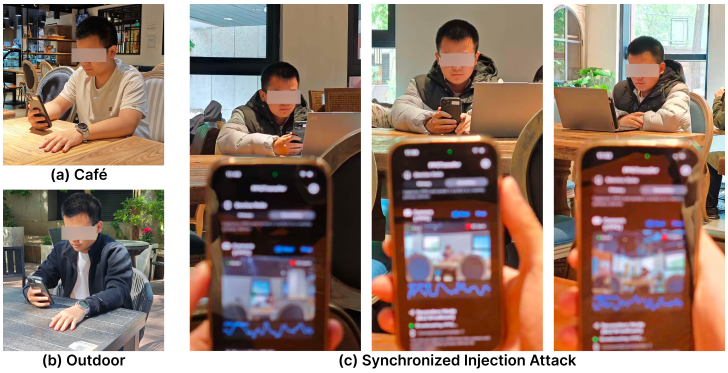


Fig. 10. Study 4 settings. (a) Café and (b) outdoor self-authentication. (c) Synchronized rPPG injection attack: the experimenter covertly films the participant from 1–2 m at three angles (front-left, straight-on, front-right).

synchronization; PPGTransID instead relies on its inherent robustness to the moderate temporal misalignment introduced by BLE transmission.

To support the synchronized rPPG injection attack, the smartphone application supports two roles. As a *token device*, it auto-connects to nearby wearables over BLE, displays the local rPPG and incoming PPG in real time, and runs a 6-second countdown once the user presses Start. After the countdown, it reports the similarity decision (Figure 9, right). As an *adversary device*, it captures rPPG from the back camera and forwards the locally extracted waveform to the victim's token phone, simulating an attacker who covertly records the legitimate user's facial video and injects the resulting rPPG into a stolen wearable.

8.2 Methodology

8.2.1 Participants and Setup. We recruited 10 participants (all male, right-handed; mean age = 19.8 years, SD = 1.40), none of whom had taken part in any of the previous studies. After introduction and consent, each participant wore the Samsung Galaxy Watch 6 on their non-dominant hand and completed the protocol in two out-of-lab settings: a public café and an outdoor bench (Figure 10 (a) (b)).

8.2.2 Commercial-Device Evaluation. In each setting, the participant held an iPhone in token-device mode and triggered self-authentication 15 times. The experimenter then wore the same smartwatch and performed 15 baseline attacks (Threat Model I) against the participant's phone.

8.2.3 Synchronized rPPG Injection Attack. To evaluate Threat Model III in the wild, the participant remained seated in the café while holding the legitimate token phone, and the experimenter held a second iPhone 15 in adversary mode and covertly recorded the participant's face from a distance of 1–2 m. As illustrated in Figure 10 (c), each participant triggered 15 authentication attempts while the adversary phone filmed from three angles—front-left, straight-on, and front-right—for 5 attempts each. The similarity score returned by the on-device classifier was logged for every trial.

The study lasted approximately 30 minutes. Participants received compensation equivalent to 7 USD in local currency. The study protocol was reviewed and approved by the university's Institutional Review Board (IRB).

Table 4. Per-stage latency of PPGTransID on the iPhone 14 Pro (mean (SD) over 15 trials).

Stage	Time (ms)
Preprocessing	6.19 (0.42)
Feature extraction	58.3 (2.57)
XGBoost inference	0.0694 (0.0330)
Total	64.6 (2.90)

8.3 Results

8.3.1 In-the-wild Deployment on Commercial Devices. Pairing the 15 self-authentication trials with the 15 baseline attacks in each setting, PPGTransID achieved a BAC of 98.3% (SD = 1.67%) in the café and 97.7% (SD = 3.35%) on the outdoor bench. These results are on par with Study 3 (Section 7) and indicate that PPGTransID remains effective on commercial wearables that expose standard PPG APIs, without hardware customization or per-user calibration. Failures were more frequent outdoors, where dappled shade from trees and intermittent hair occlusion driven by wind degraded rPPG quality. A limitation of this evaluation is that it covers only the smartwatch form factor, since raw PPG access on commercial earphones, rings, and smart glasses is not currently exposed by mainstream SDKs; assessing those form factors awaits broader vendor support.

8.3.2 Resistance to Synchronized rPPG Injection. Pairing the 15 self-authentication trials with the 15 injection trials yields a BAC of 99.3% (SD = 1.33%), indicating that PPGTransID is robust to synchronized rPPG injection under our covert-capture protocol. We observed that rPPG quality extracted from the adversary phone degraded sharply beyond approximately 1 m, leading to unstable injected signals. Filming at shorter distances would likely raise the attack success rate but is unlikely to remain covert in practice. We do not claim resistance against adversaries equipped with long-focal-length or otherwise specialized optics, which we treat as out of scope.

8.4 On-Device Latency

We profiled the on-device pipeline on the iPhone 14 Pro and report per-stage latency in Table 4. A complete CDA decision incurs 64.6 ms (SD = 2.90 ms) of compute, which is negligible relative to the 6-second acquisition window. Feature extraction dominates the budget at roughly 90% of total compute, leaving substantial room for engineering-level optimization (e.g., vectorization or operator fusion).

9 DISCUSSION

This section discusses what our results imply for deploying, securing, and governing a PPG-based CDA system in practice, together with the limitations of our current evaluation.

9.1 Application Considerations

Beyond unlocking wearables, PPGTransID's underlying primitive—instantaneous cross-modality PPG consistency as evidence of co-presence—suggests three broader classes of application.

Identity hand-off to non-wearable smart devices. PPG sensors and cameras are increasingly embedded in non-wearable platforms such as smart mirrors [34] and automotive seats [57]. By using PPGTransID to pass

verified identity from an already-authenticated phone to such devices, the device can personalize its behavior (seat position, display layout, account switching) and synchronize user-specific data without requiring a separate login.

Unobtrusive continuous authentication. Study 3 showed that PPGTransID operates reliably during typical one-handed phone use such as scrolling and reading (BAC 96.7%). This opens the possibility of treating PPGTransID as a *continuous* rather than one-shot authenticator: re-verifying co-presence periodically during natural phone use rather than only at the moment of unlock. Such continuous operation would reduce the window in which a lost or stolen wearable remains valid, and amortize the 6-second evaluation window across background activity, reducing the interaction cost of explicit re-authentication. However, realizing this would require platform-level support for periodic sanctioned background camera access, raising potential privacy concerns.

Clinical identity–data binding. In clinical settings, PPG is routinely acquired for cardiovascular monitoring, and rPPG is increasingly used during remote consultations. PPGTransID could bind physiological recordings to a verified patient identity at the moment of capture, reducing manual record-matching errors in hospitals and enabling reliable identity tagging in telemedicine. We note, however, that deployment in clinical populations would require further validation beyond our current cohort (Section 9.4).

9.2 Security Boundaries and Mitigations

We characterize PPGTransID under three threat models (Section 3.2) and report evidence of resistance to baseline impersonation, time-shifted replay, and synchronized rPPG injection (Studies 1, 3, and 4). In this section, we discuss the security boundary of PPGTransID and potential mitigation.

Mitigating short-window replay. Section 5.6 shows that PPGTransID's reliance on transient features limits replay effectiveness but does not fully eliminate short-window replay. Two complementary directions can strengthen this defense. (1) reducing the chance of historical-signal leakage: encrypting the wearable-phone PPG link via the standard BLE pairing layer, and performing all computation on the phone without persisting raw signals on either device, jointly raise the bar for an attacker to ever obtain a usable recording of recent PPG. (2) tightening the temporal margin at the model level: contrastive training that treats only sub-second-aligned pairs as positives and same-subject pairs with second-scale offsets as negatives can sharpen the model's sensitivity to small temporal misalignments, narrowing the window in which a replayed signal would remain accepted.

Mimicry Attacks. A threat model widely discussed in prior CDA and PPG-biometric work is physiological mimicry, in which an attacker actively manipulates their own physiological state to resemble the legitimate user [12, 47, 65]. We exclude precise mimicry from our primary threat models (assumption (iii) in Section 3.2) on the grounds that voluntary control of PPG morphology is not currently practical, and validate this assumption with a pilot study. In a session conducted alongside Study 3 (14 participants), attackers (participants) measured the legitimate owner's (experimenter) heart rate with an oximeter and attempted to align their own rate via deep breathing or light physical activity for one minute, before mounting a baseline-style attack. The system's BAC against these mimicry-augmented attacks (97.6%, SD = 2.34%) was statistically indistinguishable from that under Threat Model I (97.7%); participants further reported difficulty in deliberate heart-rate control (P7 and P8 noted feeling disoriented when attempting to slow down heart rate, while P2 and P5 found their post-exercise rates often overshooting the target). We exclude this threat model from the main evaluation because our pilot indicates that voluntary heart-rate control is not practical. We are also not aware of other practical techniques for voluntarily controlling PPG. Mimicry therefore remains an explicit assumption in our threat model rather than a primary evaluation, pending advances in physiologically faithful PPG synthesis.

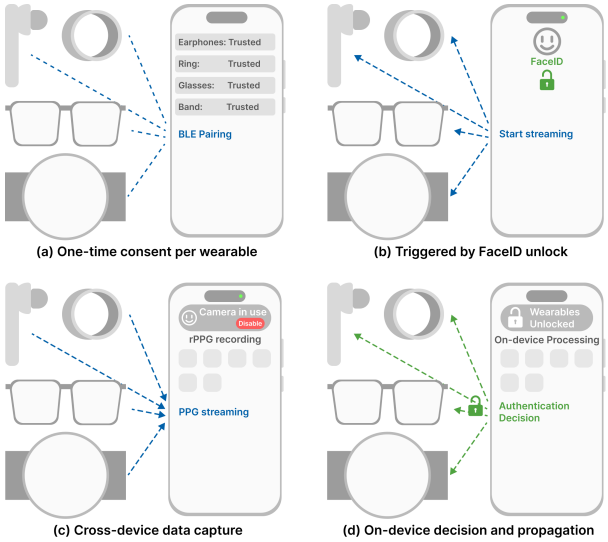


Fig. 11. Deployment pipeline of PPGTransID. (a) During onboarding, the user pairs each wearable with the phone via BLE, establishing a trusted device set. (b) The phone triggers a session at FaceID unlock, signaling the paired wearable to start streaming. (c) The phone simultaneously records rPPG from the front camera and receives PPG from the wearable. (d) Pairwise CDA runs on-device, and the resulting decision is propagated to the wearable.

9.3 Deployment, Consent, and Privacy Model

PPGTransID relies on cameras for rPPG extraction and on wearable PPG sensors that reveal cardiovascular state, which are both sensitive. Figure 11 illustrates our intended deployment lifecycle and consent flow.

One-time consent per wearable. Users enable CDA once for each wearable during initial pairing, consistent with the onboarding flows of existing commercial wearables. After consent is granted, PPGTransID operates passively during normal phone use; per-session prompts would be burdensome given that participants already rated explicit authentication time and cognitive load lower than other usability dimensions (Q5, Q6 in Table 3).

On-device processing only. As described in Section 8.1, all signal processing and classification are performed locally on the phone. No video, PPG or rPPG waveforms are transmitted to external servers, and physiological data need only be retained within the 6-second analysis window. This minimizes the attack surface associated with Threat Models II and III, while also reducing privacy risks arising from camera and physiological data usage.

User control and transparency. Users can disable PPGTransID globally or per wearable at any time, which terminates camera and sensor access. We further recommend visible capture indicators, analogous to the camera-in-use indicators already present on iOS and Android, so that users are aware when facial video is being processed, even though the processing itself is brief and local.

Platform and pairing trust. Two concerns underpin this consent model: background front-camera use and cross-device data trust. We acknowledge that frequent or unconstrained background camera use may not be permitted by mobile operating systems and could raise user concerns. PPGTransID therefore anchors its primary trigger to FaceID-initiated unlocks, extending the legitimately invoked camera session by a few additional seconds for rPPG extraction before releasing the camera, keeping camera use bounded and OS-permitted. For cross-device trust, PPGTransID accepts PPG only from wearables that have completed the BLE pairing and consent flow above, reusing the trust relationship the OS already maintains for paired devices.

9.4 Bias, Population Coverage, and Use-Context Limitations

Our studies collectively recruited 67 participants (mean age 22.3 years, no diagnosed cardiac disease). While sufficient to establish feasibility, this cohort is not fully representative of the population that would ultimately use wearable CDA, and several sources of bias and scope limitation warrant discussion.

Non-stationary use. A pilot evaluation with 5 participants under the Study 4 deployment setting showed substantially reduced performance during walking (BAC 75.3%, SD = 5.42%), with failures dominated by degraded rPPG caused by severe facial motion and rapidly changing illumination; wearable-side motion artifacts were partially mitigated by steadier hand posture and the MA-processing stage. We therefore scope PPGTransID to stationary or near-stationary smartphone use, such as scrolling, reading, video calls, payment confirmation, which covers the majority of contexts in which FaceID is currently triggered. We further envision PPGTransID as complementary to IMU-based CDA methods such as MoMatch [65]: PPGTransID handles near-stationary interactions, while MoMatch can take over when wearables and the smartphone share consistent motion patterns. Moreover, improving PPGTransID's robustness to motion through IMU-assisted compensation, multimodal fusion, or generative reconstruction of corrupted PPG [50] remains an important direction for future work.

Scope of the technical contribution. PPGTransID reuses established rPPG extraction and PPG sensing components rather than proposing new ones; its contribution is the co-presence reframing and the system that realizes it. A consequence is that PPGTransID's ceiling is bounded by the quality of the underlying rPPG extractor: improvements in mobile rPPG would directly translate into better co-presence confirmation, and conversely, scenarios where rPPG fails (e.g., walking, as discussed above) bound our applicability.

Form factor of commercial deployment. Our in-the-wild deployment was conducted exclusively on a Samsung Galaxy Watch 6, and we did not extend it to commercial earphones, smart glasses, or rings. While our custom prototypes show that the underlying primitive generalizes across body sites (Section 5), performance on other commercial form factors and vendors may differ, and broader validation across commercial wearables is left to future work.

Cardiovascular conditions. All participants were free of diagnosed cardiac disease. Arrhythmia, severely reduced heart-rate variability, or pacemaker-regulated rhythms may alter the pairwise features on which PPG-TransID depends. We do not claim effectiveness for these populations without further validation.

Age distribution. The cohort skewed young (mean 22.3 years). Older adults have different PPG morphology (e.g., reduced dicrotic notch prominence due to arterial stiffness) and different smartphone-use patterns, both of which could affect performance.

Skin tone. rPPG relies on subtle colour changes induced by the blood volume pulse, and prior work has documented reduced extraction quality on darker skin tones [51]. Our cohort did not span the full range of Fitzpatrick skin types; we expect the first-order effect to be lower pass rates at the MA-processing stage rather than degraded BAC among passing segments, but this should be verified on more diverse cohorts.

Duration floor. PPGTransID requires approximately 6 seconds of synchronized signal. This prevents use in ultra-short verification scenarios (sub-second unlocks) where gesture-based CDA [12] would be more appropriate. Reducing this floor—via higher sampling rates, modeling of partial waveforms, or predictive signal reconstruction—would broaden applicability but is beyond the present work.

10 CONCLUSION

This paper presented PPGTransID, the first cross-device authentication system that leverages real-time consistency between rPPG from smartphones and contact PPG from wearables. PPGTransID enables a ubiquitous and unobtrusive authentication approach, allowing users to unlock wearables during routine smartphone use without additional sensors or explicit gestures. Our evaluation demonstrated consistent performance across rings, bands, glasses, and earphones, achieving 95.5% balanced accuracy in an offline benchmark (N=33), 97.7% in real-time

use (N=14), and 97.7–98.3% in an in-the-wild deployment on commercial devices (N=10). Under three threat models, PPGTransID rejected baseline impersonation, limited the effectiveness of historical-leak replay, and resisted synchronized rPPG injection from covert cameras at moderate range, while running at 64.6 ms per decision on-device. Participants further evaluated the system positively across usability, reliability, and privacy dimensions. Together, these findings establish PPG as a practical bridge for CDA in wearable ecosystems, opening new directions for secure and unobtrusive authentication.

Acknowledgments

This work is supported by the National Key R&D Program of China under Grant No. 2024YFB4505500 & 2024YFB4505502 and Ant Group Research Fund.

References

[1] Pablo Armañac-Julián, Spyridon Kontaxis, Andrius Rapalis, Vaidotas Marozas, Pablo Laguna, Raquel Bailón, Eduardo Gil, and Jesús Lázaro. 2022. Reliability of pulse photoplethysmography sensors: Coverage using different setups and body locations. *Frontiers in Electronics* 3 (2022), 906324.

[2] Robert Avram, Geoffrey H Tison, Kirstin Aschbacher, Peter Kuhar, Eric Vittinghoff, Michael Butzner, Ryan Runge, Nancy Wu, Mark J Pletcher, Gregory M Marcus, et al. 2019. Real-world heart rate norms in the Health eHeart study. *NPJ digital medicine* 2, 1 (2019), 58.

[3] Robert C Block, Mohammad Yavarimanesh, Keerthana Natarajan, Andrew Carek, Azin Mousavi, Anand Chandrasekhar, Chang-Sei Kim, Junxi Zhu, Giovanni Schifitto, Lalit K Mestha, et al. 2020. Conventional pulse transit times as markers of blood pressure changes in humans. *Scientific Reports* 10, 1 (2020), 16373.

[4] Karthik Budidha and Panayiotis A Kyriacou. 2013. Devepopment of an optical probe to investigate the suitability of measuring photoplethysmographs and blood oxygen saturation from the human auditory canal. In *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 1736–1739.

[5] Joel S Burma, James K Griffiths, Andrew P Lapointe, Ibukunoluwa K Oni, Ateyeh Soroush, Joseph Carere, Jonathan D Smirl, and Jeff F Dunn. 2024. Heart rate variability and pulse rate variability: do anatomical location and sampling rate matter? *Sensors* 24, 7 (2024), 2048.

[6] Yetong Cao, Qian Zhang, Fan Li, Song Yang, and Yu Wang. 2020. PPGPass: Nonintrusive and secure mobile two-factor authentication via wearables. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 1917–1926.

[7] Weixuan Chen and Daniel McDuff. 2018. Deepphys: Video-based physiological measurement using convolutional attention networks. In *Proceedings of the european conference on computer vision (ECCV)*. 349–365.

[8] Nicholas Constant, Orrett Douglas-Prawl, Samuel Johnson, and Kunal Mankodiya. 2015. Pulse-Glasses: An unobtrusive, wearable HR monitor with Internet-of-Things functionality. In *2015 IEEE 12th international conference on wearable and implantable body sensor networks (BSN)*. IEEE, 1–5.

[9] Duy Dao, S. M. A. Salehizadeh, Yeonsik Noh, Jo Woon Chong, Chae Ho Cho, Dave McManus, Chad E. Darling, Yitzhak Mendelson, and Ki H. Chon. 2017. A Robust Motion Artifact Detection Algorithm for Accurate Detection of Heart Rates From Photoplethysmographic Signals Using Time–Frequency Spectral Features. *IEEE Journal of Biomedical and Health Informatics* 21, 5 (2017), 1242–1253. doi:10.1109/JBHI.2016.2612059

[10] Gerard De Haan and Vincent Jeanne. 2013. Robust pulse rate from chrominance-based rPPG. *IEEE Transactions on Biomedical Engineering* 60, 10 (2013), 2878–2886.

[11] Deniz Ekiz, Yekta Said Can, Yagmur Ceren Dardagan, and Cem Ersoy. 2020. Can a smartband be used for continuous implicit authentication in real life. *IEEE Access* 8 (2020), 59402–59411.

[12] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2016. Shakeunlock: Securely transfer authentication states between mobile devices. *IEEE Transactions on Mobile Computing* 16, 4 (2016), 1163–1175.

[13] Jesse Fine, Michael J McShane, Gerard L Coté, and Christopher G Scully. 2022. A computational modeling and simulation workflow to investigate the impact of patient-specific and device factors on hemodynamic measurements from non-invasive photoplethysmography. *Biosensors* 12, 8 (2022), 598.

[14] Mingxi Geng, Gongda Hu, Gang Wang, and Yiyu Wang. 2024. Efficient rPPG-Based Biometric Authentication Using Lightweight Vision Transformer. In *2024 4th International Conference on Electronic Information Engineering and Computer Communication (EIECC)*. IEEE, 488–491.

[15] Vera Hartmann, Haipeng Liu, Fei Chen, Qian Qiu, Stephen Hughes, and Dingchang Zheng. 2019. Quantitative comparison of photoplethysmographic waveform characteristics: Effect of measurement site. *Frontiers in physiology* 10 (2019), 198.

[16] Daniel Hintze, Rainhard D Findling, Muhammad Muaaz, Eckhard Koch, and René Mayrhofer. 2015. Cormorant: towards continuous risk-aware multi-modal cross-device authentication. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive*

and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers. 169–172.

[17] Christian Holz and Frank R Bentley. 2016. On-demand biometrics: Fast cross-device authentication. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 3761–3766.

[18] Anna Huang, Dong Wang, Run Zhao, and Qian Zhang. 2019. Au-id: Automatic user identification and authentication through the motions captured from sequential human activities using rfid. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2 (2019), 1–26.

[19] Chenpei Huang, Hui Zhong, Zhen Chen, Xiaoqi Qin, Lan Zhang, Xiaoyong (Biran) Yuan, and Miao Pan. 2025. Leveraging Binary Ear Canal Scanning Code for User Authentication in Earbuds. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. doi:10.1145/3706599.3719788

[20] Manh Pham Hung, Matthew Yiwen Ho, Yiming Zhang, Dimitris Spathis, Aaqib Saeed, and Dong Ma. 2025. Reliable Physiological Monitoring on the Wrist Using Generative Deep Learning to Address Poor Skin-Sensor Contact. *arXiv preprint arXiv:2504.02735* (2025).

[21] Sheikh Muhammad Asher Iqbal, Mary Ann Leavitt, Imadeldin Mahgoub, and Waseem Asghar. 2024. A wearable Internet of Things device for noninvasive remote monitoring of vital signs related to heart failure. *IoT* 5, 1 (2024), 155–167.

[22] Hassan Ismail Fawaz, Benjamin Lucas, Germain Forestier, Charlotte Pelletier, Daniel F Schmidt, Jonathan Weber, Geoffrey I Webb, Lhassane Idoumghar, Pierre-Alain Muller, and François Petitjean. 2020. Inceptiontime: Finding alexnet for time series classification. *Data Mining and Knowledge Discovery* 34, 6 (2020), 1936–1962.

[23] Liliana Ivanciu, Iustin-Alexandru Ivanciu, Paul Farago, Marius Roman, and Sorin Hintea. 2021. An ECG-based authentication system using Siamese neural networks. *Journal of Medical and Biological Engineering* 41, 4 (2021), 558–570.

[24] Wenqiang Jin, Ming Li, Srinivasan Murali, and Linke Guo. 2020. Harnessing the Ambient Radio Frequency Noise for Wearable Device Pairing. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (2020). https://dl.acm.org/doi/10.1145/3372297.3417288

[25] Matin Kheirkhahan, Hiranava Das, Manoj Battula, Anis Davoudi, Parisa Rashidi, Todd M Manini, and Sanjay Ranka. 2017. Power-efficient real-time approach to non-wear time detection for smartwatches. In *2017 IEEE EMBS international conference on biomedical & health informatics (BHI)*. IEEE, 217–220.

[26] Youngsam Kim, Jong-hyuk Roh, and Soohyung Kim. 2025. Siamese network-based user-independent model for surface electromyogram biometric authentication. *ETRI Journal* (2025).

[27] Joan Lambert Cause, Ángel Solé Morillo, Juan C García-Naranjo, Johan Stiens, and Bruno da Silva. 2024. The Impact of Contact Force on Signal Quality Indices in Photoplethysmography Measurements. *Applied Sciences* 14, 13 (2024), 5704.

[28] Jiao Li, Yang Liu, Zhenjiang Li, and Jin Zhang. 2023. EarPass: Continuous user authentication with in-ear PPG. In *Adjunct Proceedings of the 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing & the 2023 ACM International Symposium on Wearable Computing*. 327–332.

[29] Lin Li, Chao Chen, Lei Pan, Leo Yu Zhang, Jun Zhang, and Yang Xiang. 2023. SigA: rPPG-based authentication for virtual reality head-mounted display. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*. 686–699.

[30] Pooi Khoon Lim, Siew-Cheok Ng, Nigel H Lovell, Yong Poh Yu, Maw Pin Tan, Devin McCombie, Einly Lim, and Stephen J Redmond. 2018. Adaptive template matching of photoplethysmogram pulses to detect motion artefact. *Physiological measurement* 39, 10 (2018), 105005.

[31] Stephen P Linder, Suzanne M Wendelken, Edward Wei, and Susan P McGrath. 2006. Using the morphology of photoplethysmogram peaks to detect changes in posture. *Journal of clinical monitoring and computing* 20, 3 (2006), 151–158.

[32] Giulio Lovisotto, Henry Turner, Simon Eberz, and Ivan Martinovic. 2020. Seeing Red: PPG Biometrics Using Smartphone Cameras. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*.

[33] Chaoqi Luo, Yiping Xie, and Zitong Yu. 2024. PhysMamba: Efficient Remote Physiological Measurement with SlowFast Temporal Difference Mamba. In *Chinese Conference on Biometric Recognition*. Springer, 248–259.

[34] Xulin Ma, Jiankai Tang, Zhang Jiang, Songqin Cheng, Yuanchun Shi, Dong Li, Xin Liu, Daniel McDuff, Xiaojing Liu, and Yuntao Wang. 2025. Non-Contact Health Monitoring During Daily Personal Care Routines. In *IEEE BSN*.

[35] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. 2018. SAW: Wristband-based authentication for desktop computers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018), 1–29.

[36] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2021. Using siamese neural networks to perform cross-system behavioral authentication in virtual reality. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*. IEEE, 140–149.

[37] Aravind Natarajan, Alexandros Pantelopoulos, Hulya Emir-Farinas, and Pradeep Natarajan. 2020. Heart rate variability with photoplethysmography in 8 million individuals: a cross-sectional study. *The Lancet Digital Health* 2, 12 (2020), e650–e657.

[38] Meir Nitzan, B Khanokh, and Y Slovik. 2001. The difference in pulse transit time to the toe and finger measured by photoplethysmography. *Physiological measurement* 23, 1 (2001), 85.

[39] Christina Orphanidou, Timothy Bonnici, Peter Charlton, David Clifton, David Vallance, and Lionel Tarassenko. 2015. Signal-Quality Indices for the Electrocardiogram and Photoplethysmogram: Derivation and Applications to Wireless Monitoring. *IEEE Journal of Biomedical and Health Informatics* 19, 3 (2015), 832–838. doi:10.1109/JBHI.2014.2338351

[40] Jiaqi Pan, Xinyan Zhou, Yue Hou, Xiaoyu Ji, and Haiming Chen. 2024. M-PPG: A Non-intrusive Authentication for Wearable Devices via PPG Sensors with Motor Excitations. *IEEE Sensors Journal* (2024).
[41] Junyung Park, Hyeon Seok Seok, Sang-Su Kim, and Hangsik Shin. 2022. Photoplethysmogram analysis and applications: an integrative review. *Frontiers in physiology* 12 (2022), 808451.
[42] Ghessette Mae Punay, Reynaldo Guieb, Carl Timothy Tolentino, Marc Rosales, Paul Jason Co, and John Richard Hizon. 2024. Extraction of Heart Rate from Photoplethysmography Signals on Multiple Sites for Wearable Heart Monitoring Systems. In *TENCON 2024-2024 IEEE Region 10 Conference (TENCON)*. IEEE, 1202–1206.
[43] Aanjhan Ranganathan and Srdjan Capkun. 2017. Are We Really Close? Verifying Proximity in Wireless Systems. *IEEE Security & Privacy* 15 (2017), 52–58. https://ieeexplore.ieee.org/document/7945214/
[44] Scott Ryals, Ambrose Chiang, Sharon Schutte-Rodin, Arvind Chandrakantan, Nitun Verma, Steven Holfinger, Fariha Abbasi-Feinberg, Anuja Bandyopadhyay, Kelly Baron, Sumit Bhargava, et al. 2023. Photoplethysmography—new applications for an old technology: a sleep technology review. *Journal of Clinical Sleep Medicine* 19, 1 (2023), 189–195.
[45] Alice Scandelli, Ilaria Crupi, Pietro Bartoli, Andrea Giudici, Arianna De Vecchi, and Federica Villa. 2024. Study of PPG Sensor Positioning on Smart Eyewear for Biosensing. In *2024 IEEE Sensors Applications Symposium (SAS)*. IEEE, 1–6.
[46] Hyejin Shin, Jun Ho Huh, Bum Jun Kwon, Iljoo Kim, Eunyong Cheon, HongMin Kim, Choong-Hoon Lee, and Ian Oakley. 2024. SkullID: Through-Skull Sound Conduction based Authentication for Smartglasses. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. doi:10.1145/3613904.3642506
[47] Hyejin Shin, Jun Ho Huh, Bum Jun Kwon, Iljoo Kim, Eunyong Cheon, HongMin Kim, Choong-Hoon Lee, and Ian Oakley. 2024. SkullID: Through-skull sound conduction based authentication for smartglasses. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–19.
[48] Kaixin Sui, Mengyu Zhou, Dapeng Liu, Minghua Ma, Dan Pei, Youjian Zhao, Zimu Li, and Thomas Moscibroda. 2016. Characterizing and improving wifi latency in large-scale operational networks. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. 347–360.
[49] Zhaodong Sun, Xiaobai Li, Jukka Komulainen, and Guoying Zhao. 2024. Biometric authentication based on enhanced remote photoplethysmography signal morphology. In *2024 ieee international joint conference on biometrics (ijcb)*. IEEE, 1–10.
[50] Jiankai Tang, Kequan Chen, Yuntao Wang, Yuanchun Shi, Shwetak Patel, Daniel McDuff, and Xin Liu. 2023. Mmpd: multi-domain mobile video physiology dataset. In *2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. IEEE, 1–5.
[51] Jiankai Tang, Xinyi Li, Jiacheng Liu, Xiyuxing Zhang, Zeyu Wang, and Yuntao Wang. 2024. Camera-Based Remote Physiology Sensing for Hundreds of Subjects Across Skin Tones. arXiv:2404.05003 [cs.CV]
[52] Jiankai Tang, Jiacheng Liu, Renling Tong, Kai Zhu, Zhe Li, Xin Yi, Junliang Xing, Yuanchun Shi, and Yuntao Wang. 2025. Exploring Reliable PPG Authentication on Smartwatches in Daily Scenarios. *arXiv preprint arXiv:2503.23930* (2025).
[53] Pei-Yun Tsai, Chiu-Hua Huang, Jia-Wei Guo, Yu-Chuan Li, An-Yeu Andy Wu, Hung-Ju Lin, and Tzung-Dau Wang. 2021. Coherence between decomposed components of wrist and finger PPG signals by imputing missing features and resolving ambiguous features. *Sensors* 21, 13 (2021), 4315.
[54] Rahul Rama Varior, Mrinal Haloi, and Gang Wang. 2016. Gated siamese convolutional neural network architecture for human re-identification. In *European conference on computer vision*. Springer, 791–808.
[55] Wim Verkruysse, Lars O Svaasand, and J Stuart Nelson. 2008. Remote plethysmographic imaging using ambient light. *Optics express* 16, 26 (2008), 21434–21445.
[56] Li Wan, Kechen Liu, Hanan Abdullah Mengash, Nuha Alruwais, Mesfer Al Duhayyim, and K Venkatachalam. 2024. Deep learning-based photoplethysmography biometric authentication for continuous user verification. *Applied Soft Computing* 156 (2024), 111461.
[57] Jiyao Wang, Xiao Yang, Qingyong Hu, Jiankai Tang, Can Liu, Dengbo He, Yuntao Wang, Yingcong Chen, and Kaishun Wu. 2025. PhysDrive: A Multimodal Remote Physiological Measurement Dataset for In-vehicle Driver Monitoring. *arXiv preprint arXiv:2507.19172* (2025).
[58] Kegang Wang, Jiankai Tang, Yuxuan Fan, Jiatong Ji, Yuanchun Shi, and Yuntao Wang. 2025. Memory-efficient Low-latency Remote Photoplethysmography through Temporal-Spatial State Space Duality. *arXiv preprint arXiv:2504.01774* (2025).
[59] Kegang Wang, Jiankai Tang, Yantao Wei, Mingxuan Liu, Xin Liu, and Yuntao Wang. 2024. A Plug-and-Play Temporal Normalization Module for Robust Remote Photoplethysmography. *arXiv preprint arXiv:2411.15283* (2024).
[60] Wenjin Wang, Albertus C den Brinker, Sander Stuijk, and Gerard de Haan. 2016. Algorithmic principles of remote PPG. *IEEE Transactions on Biomedical Engineering* 64, 7 (2016), 1479–1491.
[61] Wei Wang, L. Yang, and Qian Zhang. 2016. Touch-and-guard: secure pairing through hand resonance. *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2016). https://dl.acm.org/doi/10.1145/2971648.2971688
[62] Yao Wang, Yufei Chen, Haibin Zhang, Minjie Lyu, and Tao Gu. 2025. S2Pair: Secure and Simple Device Pairing Using Human Bone as a Key Generator. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 9 (2025), 1 – 29. https://dl.acm.org/doi/10.1145/3729466

[63] Yao Wang, Tao Gu, Yu Zhang, Minjie Lyu, Tom Hao Luan, and Hui Li. 2022. Enabling secure touch-to-access device pairing based on human body's electrical response. *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking* (2022). https://dl.acm.org/doi/10.1145/3495243.3564146
[64] Bo Wei, Weitao Xu, Chengwen Luo, and Jin Zhang. 2024. FaceFinger: Embracing Variance for Heartbeat Based Symmetric Key Generation System. *IEEE Transactions on Mobile Computing* 23 (2024), 14218–14232. https://ieeexplore.ieee.org/document/10631295
[65] Chuxiong Wu, Xiaopeng Li, Fei Zuo, Lannan Luo, Xiaojiang Du, Jia Di, and Qiang Zeng. 2022. Use It-No Need to Shake It! accurate implicit authentication for everyday objects with smart sensing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 3 (2022), 1–25.
[66] Maoying Wu, Wu Zeng, Ruochen Tan, Yin Ni, and Lan Yang. 2023. Authentication that Combines rPPG Information with Face Detection on the Blockchain. In *International Artificial Intelligence Conference*. Springer, 80–94.
[67] Hui-Shyong Yeo. 2018. Enabling Single-Handed Interaction in Mobile and Wearable Computing. In *Adjunct Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology* (Berlin, Germany) *(UIST '18 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 236–239. doi:10.1145/3266037.3266129
[68] Zitong Yu, Xiaobai Li, and Guoying Zhao. 2019. Remote photoplethysmograph signal measurement from facial videos using spatio-temporal networks. *arXiv preprint arXiv:1905.02419* (2019).
[69] Zitong Yu, Yuming Shen, Jingang Shi, Hengshuang Zhao, Philip Torr, and Guoying Zhao. 2022. PhysFormer: Facial Video-based Physiological Measurement with Temporal Difference Transformer. In *CVPR*.
[70] Hongwei Yuan, Sven Poeggel, Thomas Newe, Elfed Lewis, Charusluk Viphavakit, and Gabriel Leen. 2017. An experimental study of the effects of external physiological parameters on the photoplethysmography signals in the context of local blood pressure (hydrostatic pressure changes). *Sensors* 17, 3 (2017), 556.
[71] Emi Yuda, Kento Yamamoto, Yutaka Yoshida, and Junichiro Hayano. 2020. Differences in pulse rate variability with measurement site. *Journal of Physiological Anthropology* 39, 1 (2020), 4.
[72] Tianming Zhao, Yan Wang, Jian Liu, Jerry Cheng, Yingying Chen, and Jiadi Yu. 2022. Robust Continuous Authentication Using Cardiac Biometrics From Wrist-Worn Wearables. *IEEE Internet of Things Journal* 9, 12 (June 2022), 9542–9556. doi:10.1109/JIOT.2021.3128290
[73] Bochao Zou, Zizheng Guo, Jiansheng Chen, Junbao Zhuo, Weiran Huang, and Huimin Ma. 2025. RhythmFormer: Extracting patterned rPPG signals based on periodic sparse attention. *Pattern Recognition* 164 (2025), 111511.
[74] Fei Zuo, Xiaopeng Li, Patrick Young, Lannan Luo, Qiang Zeng, and Zhexin Zhang. 2018. Neural machine translation inspired binary code similarity comparison beyond function pairs. *arXiv preprint arXiv:1808.04706* (2018).

A APPENDIX

A.1 Sensitivity Analysis of Channel Quality Weights

To select the values of λ_{Sk}, λ_{Ku}, λ_{Rp}, and λ_{Tm} in Eq. (1), we conducted an analysis on the Study 1 sitting condition. Because the four weights are constrained by $\sum \lambda = 1$ with $\lambda_{\mathrm{Sk}} = \lambda_{\mathrm{Ku}}$ and $\lambda_{\mathrm{Rp}} = \lambda_{\mathrm{Tm}}$, we swept $\lambda_{\mathrm{Sk}} = \lambda_{\mathrm{Ku}}$ from 0.05 to 0.40 with $\lambda_{\mathrm{Rp}} = \lambda_{\mathrm{Tm}}$ adjusted accordingly, holding all other components of the pipeline fixed. For each configuration, we re-ran channel selection and the LOSO evaluation using the same XGBoost classifier as in the main paper. Results are reported in Table 5.

Table 5. Sensitivity of BAC to the weighting in Eq. (1) on Study 1 (sitting).

λ_{Sk}	λ_{Ku}	λ_{Rp}	λ_{Tm}	BAC (%)
0.05	0.05	0.45	0.45	95.5 (1.79)
0.10	**0.10**	**0.40**	**0.40**	**95.5 (1.66)**
0.20	0.20	0.30	0.30	95.3 (1.77)
0.30	0.30	0.20	0.20	95.3 (1.77)
0.40	0.40	0.10	0.10	95.3 (1.77)

We find that different configurations have little impact on the final BAC, and therefore adopt ($\lambda_{\mathrm{Sk}} = \lambda_{\mathrm{Ku}} = 0.10$, $\lambda_{\mathrm{Rp}} = \lambda_{\mathrm{Tm}} = 0.40$) as our final choice.

A.2 Extracted Features

Table 6 lists the 21 features extracted from each PPG pair, together with their full names and explanations. As shown in the table, we extract two categories of pairwise features:

Difference features: For each characteristic f_k, we compute the absolute difference between the two signals

$$D_k = \left| f_k^{(1)} - f_k^{(2)} \right| \tag{2}$$

where $f_k^{(1)}$ and $f_k^{(2)}$ are the values of the k-th feature extracted from two PPGs from a PPG pair, respectively.

Similarity features: These directly measure how closely the signals co-vary, such as

$$S_k = \mathrm{sim_k}(x^{(1)}, x^{(2)}) \tag{3}$$

where $x^{(1)}$ and $x^{(2)}$ denote the two PPGs from a pair and sim_k is the k-th similariy feature.

Table 6. **Selected Features.** The 21 features extracted from each PPG-pair.

Category	Name	Explanation
Time-domain difference	Heart rate	Mean heart rates
	$PPI_{systolic}$ std.	Std. of systolic peak's pulse-to-pulse interval (PPI) [41]
	Mean pulse rise time (PRT)	Mean of the time from pulse onset to systolic peak [13]
	PRT std.	Standard deviation of PRT
	PRT ratio	Mean PRT per cardiac cycle
	PRT ratio std.	Std. of PRT ratio
	Skewness	Distribution asymmetry of waveform
	Kurtosis	Sharpness/peakedness of waveform distribution
Frequency-domain difference	Main frequency	Dominant spectral peak frequency
	Second frequency	Secondary spectral peak frequency
	High-frequency energy ratio	Energy ratio in band >1Hz
	Low-frequency energy ratio	Energy ratio in band 0.5–1Hz
	LF/HF ratio	Ratio of low- to high-frequency energy
	Spectral entropy	Entropy of normalized power spectrum
Time-domain similarity	Coherence	Average coherence in 0.5–2Hz band
	Maximum cross-correlation	Highest correlation coefficient
	Maximum lag	Lag at which correlation peaks
	DTW distance	Dynamic Time Warping distance
	Pearson correlation	Linear correlation coefficient
	Cosine similarity	Vector cosine similarity of signals
Frequency-domain similarity	Cosine similarity	Cosine similarity of power spectral densities

A.3 User Study Questionaire

Table 7 presents the exact questions that appeared on the questionnaire provided to the participants in Study 3.

A.4 LLM Usage Clarification

We used ChatGPT 5.0 to perform grammar check and correction.

Table 7. **Full Questionnaire Items.** Higher scores indicate more positive evaluation.

ID	Question
Q1	I often use smart wearable devices such as smartwatches, bracelets, headphones, rings, glasses, etc.
Q2	I think smart wearable devices need privacy protection.
Q3	I think this system is easy to understand.
Q4	I think this system is easy to use.
Q5	I think the unlocking time required for this system is acceptable.
Q6	I think using this system requires very little thought, attention, or cognitive processing.
Q7	I think this system has a very low memory burden.
Q8	I think using this system requires very little physical effort.
Q9	I think using this system requires very little effort.
Q10	I think using this system involves little frustration.
Q11	I think this system can reliably unlock personal (wearable) devices.
Q12	I think this system is very difficult to be effectively attacked.
Q13	I believe this system can provide secure unlocking for smart wearable devices.
Q14	I can accept the use of privacy in this system.
Q15	I am willing to use this device in public places.
Q16	I think I will use this system frequently.
Q17	I think there are more potential application scenarios for this system.
Q18	Possible potential application scenarios. (Open question)
Q19	Suggestions for the system. (Open comments)