SMART WATCH USER AUTHENTICATION USING A BI-MODAL BEHAVIORAL BIOMETRIC FRAMEWORK

[1] Mrs. B Praveena, [2] AVANCHA MADHURI ,[3] DHARANI ADITHYA RAM ,[4] MAREDDY SANJAY REDDY ,[5] EGAPURI BALA KRISHNA

[1] *Assistant Professor, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy College of Engineering , Hyderabad, India.*

[2,3,4,5] *Students, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy College of Engineering, Hyderabad, India.*

ABSTRACT:

The increasing deployment of smartwatches in daily activities—ranging from health monitoring and communication to financial transactions—demands robust, user-friendly, and continuous authentication mechanisms. Traditional PIN- or password-based security remains insufficient due to usability limitations and vulnerability to observational attacks, as highlighted in behavioral biometric surveys [1]. Recent advancements show that behavioral signals such as gait patterns [2], wrist-worn gait-based authentication [3], touch and swipe dynamics [4], and keystroke behavior on mobile devices [5] offer strong discriminatory features for secure identity verification. Physiological biometrics such as heart-rate variability captured through PPG sensors have also shown potential for authentication in wearable environments [6]. Additionally, smartwatch-specific behavioral cues—including tapping rhythms [7], wrist-based gait motion [8], and multimodal feature integration [9–11]—have been recognized for their high effectiveness and usability in continuous authentication systems. Surveys on touch dynamics [12] and gait-based mobile authentication [13] further support the feasibility of behavioral biometrics as a reliable replacement for traditional methods. However, existing single-modality systems often suffer from environmental noise, sensor variability, and spoofing vulnerabilities. Comprehensive reviews on behavioral biometrics [14] and around-device sensing systems such as SonarAuth [15] emphasize the need for combining multiple modalities for higher robustness. Recent smartwatch studies on pressure-based biometric input [16], real-world continuous authentication [17], and context-aware mobile authentication [18] demonstrate that multimodal sensor fusion significantly enhances accuracy. Likewise, machine-learning-driven continuous authentication methods using typing and motion patterns [19], along with broader reviews of behavioral authentication for security and safety [20], highlight the value of integrated behavioral models. Motivated by these findings, Wearable Wisdom: A Bi-Model Behavioral Biometric Scheme for Smart Watch User Authentication introduces a dual-modality framework that fuses two complementary behavioral signals—such as gait, wrist movement, touch dynamics, or heart-rate patterns—to strengthen real-time authentication. By leveraging insights from the referenced literature [1–20], the proposed system provides a secure, unobtrusive, continuous, and context-aware authentication solution suitable for modern smartwatch ecosystems.

Keywords : Behavioral Biometrics, Smartwatch Authentication, Wearable Security, Bi-Model Authentication, Gait Analysis, Wrist Motion Dynamics, Touch Interaction Patterns, Heart Rate Variability, Machine Learning, Continuous Authentication, Multimodal Biometrics, User Verification, Wearable Sensors, Spoof Resistance, Cybersecurity.

I.INTRODUCTION

In recent years, wearable devices—especially smartwatches—have evolved from simple

notification tools to powerful personal computing platforms capable of health monitoring, mobile communication, and secure transaction authentication. As these devices increasingly store and process sensitive personal, financial, and biometric data, ensuring strong yet user-friendly security has become a critical requirement. Traditional authentication methods such as PINs, passwords, and pattern locks are inadequate due to small screen size, susceptibility to shoulder surfing, and low usability in motion-centric environments [1]. This has motivated the shift toward behavioral biometric authentication, where natural human behavioral patterns are used as a secure and continuous identity verification mechanism.

Research has shown that gait patterns captured from wearable sensors such as accelerometers and gyroscopes provide highly distinctive user signatures, making gait an effective biometric for mobile and wearable authentication [2], [3]. Similarly, touch dynamics—including swipe pressure, duration, gesture patterns, and typing rhythms—offer unique behavioral features that can differentiate users with high accuracy [4], [5]. Physiological biometrics such as heart-rate variability measured through PPG signals have also been validated as reliable indicators for personal identification on wearable devices [6]. Smartwatch-specific studies have expanded the field further by exploring tapping rhythms [7], wrist-based gait features [8], multimodal fusion [9], and wrist-band–based sensor integration for robust authentication [10], [11].

Surveys on touch interaction [12] and gait-based authentication [13] reinforce the potential of behavioral biometrics as secure, non-intrusive alternatives to conventional authentication. Meanwhile, scoping reviews of behavioral biometric systems [14] and innovations such as around-device sensing (e.g., SonarAuth) [15] highlight the need for combining multiple modalities to overcome limitations of single-biometric systems. More recent contributions—including pressure-based biometric inputs for smartwatches [16], real-world smartwatch authentication experiments [17], context-aware behavioral authentication environments [18], and advanced continuous authentication through typing and motion data [19]—underscore the benefits of sensor fusion and machine learning for achieving high reliability. Comprehensive reviews of behavioral authentication methods [20] further emphasize the growing relevance of multimodal approaches in wearable security.

Motivated by these advancements, this project, Wearable Wisdom: A Bi-Model Behavioral Biometric Scheme for Smart Watch User Authentication, proposes a dual-modal authentication mechanism that integrates two complementary behavioral signals to deliver secure, continuous, and unobtrusive user verification. Grounded in extensive research from behavioral biometrics, wearable sensors, and multimodal authentication systems [1–20], the proposed scheme aims to significantly enhance smartwatch security while maintaining user convenience and seamless operation in everyday activities.

II.LITERATURE SURVEY

[1] Behavioural Biometrics: A Survey and Classification

Author: R. V. Yampolskiy

Abstract: This work presents a comprehensive classification of behavioral biometrics, covering various human behavioral patterns such as gait, keystroke dynamics, touch gestures, and mouse movements. The author analyzes the strengths and weaknesses of behavioral traits compared to physical biometrics and highlights their significance for continuous and unobtrusive authentication. The survey concludes that behavioral biometrics provide increased user convenience and strong resistance to spoofing attacks, making them suitable for wearable authentication. [1]

[2] Wearable Device-Based Gait Recognition Using Angle and Inertial Features

Authors: Y. Zhao, Z. Zhang, H. Li

Abstract: This study explores gait recognition using accelerometer and gyroscope sensors embedded in wearable devices. The authors propose a feature extraction method using angular and inertial features, achieving highly accurate user identification. The results show that gait patterns captured from wrist-worn devices are unique and dependable, supporting their integration into authentication frameworks. [2]

[3] Gait-Based Authentication Using a Wrist-Worn Device

Authors: A. De Marsico, M. Nappi, D. Riccio, H. Wechsler

Abstract: The authors investigate the feasibility of gait-based identification using wrist-mounted devices. Their approach examines motion signals during natural walking and extracts discriminative features for authentication. The study demonstrates that wrist-worn gait biometrics outperform traditional single-feature methods, proving their viability for real-world smartwatch security. [3]

[4]Touch-Dynamics Based User Authentication Using Machine Learning

Authors: Y. Meng, R. A. Maxion

Abstract: This research proposes a machine-learning-driven authentication system using touch dynamics on mobile devices. Features such as stroke speed, pressure, and direction are analyzed to distinguish legitimate users. The study confirms that touch behavior is highly individualized and effective for continuous authentication on touch-based devices. [4]

[5] Keystroke Dynamics in Mobile Platforms

Author: V. Ponnusamy

Abstract: This paper analyzes keystroke timing and pressure variations during text entry on mobile devices. The author demonstrates that keystroke patterns can identify users with high reliability, even on soft keyboards. The findings highlight keystroke dynamics as a lightweight and practical biometric for mobile and wearable systems.[5]

[6] Heart Rate Variability for Biometric Authentication Using PPG Signals

Author: N. Akhter

Abstract: This study examines heart-rate variability (HRV) derived from PPG sensors as a biometric trait. Using machine learning models, the work demonstrates that HRV features are unique to individuals and stable over time. The results support the feasibility of physiological biometrics for smartwatch authentication.[6]

[7] Smartwatch User Authentication by Sensing Tapping Rhythms

Authors: H. Zhang, S. A. Mahmood, et al.

Abstract: The authors propose a tapping-rhythm-based authentication system using smartwatch sensors. The tapping force, timing, and rhythm patterns are analyzed for identity verification. The study shows that tapping rhythms are user-specific and resistant to imitation attacks, making them suitable for passive authentication.[7]

III.EXISTING SYSTEM

In the existing authentication systems used in smartwatches and other wearable devices, the dominant methods rely on conventional security mechanisms such as PINs, passwords, pattern locks, or basic touch-based authentication. These approaches, although simple and easy to implement, offer limited protection due to the compact screen size and the highly visible nature of smartwatch interactions. Since users often interact with smartwatches in public or while on the move, traditional authentication becomes prone to shoulder surfing attacks, observation-based guessing, and smudge attacks. Some devices implement single-modality biometric systems such as touch dynamics, gait signals, or heart-rate patterns, but these systems still struggle with environmental noise, sensor variability, motion artifacts, and inconsistent user behavior. Furthermore, traditional authentication is typically one-time and not

continuous, meaning that once the device is unlocked, no further identity verification occurs, increasing the risk of unauthorized access if the device is stolen or left unattended. Existing behavioral biometric systems also tend to rely on a single sensor modality, which reduces accuracy, increases false acceptance/rejection rates, and limits robustness against spoofing attempts. These limitations highlight the need for a more secure, continuous, and multi-sensor authentication approach.

IV. PROPOSED SYSTEM

The proposed system, Wearable Wisdom: A Bi-Model Behavioral Biometric Scheme for Smart Watch User Authentication, introduces an intelligent, continuous, and non-intrusive authentication framework designed specifically for modern smartwatch environments. Unlike traditional single-step or unimodal systems, the proposed method integrates two complementary behavioral biometrics—such as gait patterns, wrist movement dynamics, touch interaction behavior, tapping rhythm, or heart-rate variability—to form a robust and unified biometric identity profile. These behavioral signals are captured using built-in smartwatch sensors including the accelerometer, gyroscope, PPG sensor, touch screen interface, and pressure sensors. The system continuously monitors user behavior during normal activities, extracts unique discriminative features, and processes them through advanced machine-learning or deep-learning models to verify authenticity in real time.The bi-model approach ensures that even if one modality is affected by sensor noise, environmental factors, or inconsistent user behavior, the second modality compensates, significantly improving reliability. The system employs a multi-stage processing pipeline that includes sensor data acquisition, preprocessing, feature extraction, multimodal fusion, model training, and continuous verification. Fusion techniques combine temporal, physiological, and motion-based features, enabling the model to learn complex user-specific patterns that are difficult to imitate or spoof.

Moreover, the proposed system operates passively in the background without requiring explicit user action, thus maintaining high usability and reducing authentication fatigue. Since the system continuously validates the user's identity, unauthorized access is immediately detected if the device is removed, stolen, or worn by another person. This enhances resistance against impersonation attacks, replay attacks, and mimicry-based threats. By leveraging multimodal sensor fusion and intelligent authentication logic, the proposed system significantly advances smartwatch security, offering a more accurate, adaptive, and context-aware solution compared to existing one-dimensional biometric schemes.

V.SYSTEM ARCHITECTURE

The proposed system architecture for the bi-model behavioral biometric authentication scheme is designed to ensure secure, continuous, and unobtrusive identity verification on a smartwatch. The architecture begins with sensor data acquisition, where the smartwatch collects raw behavioral signals such as accelerometer data, gyroscope motion, touch patterns, tapping rhythms, and heart-rate variability through built-in sensors. This raw data is then passed to the preprocessing module, which filters noise, normalizes values, extracts relevant time-series segments, and ensures consistency across different sensor conditions. After preprocessing, the system enters the multimodal fusion stage, where features from two independent biometric modalities are combined to form a richer and more robust biometric signature. This fusion significantly enhances accuracy and reduces the weaknesses of single-modality methods. The unified feature set is then used by the continuous verification module, which compares real-time user behavior with the stored user profile to confirm identity during device usage. Simultaneously, the model training module

continuously updates and refines the machine-learning model using new behavioral data, enabling adaptability to natural changes in user patterns over time.

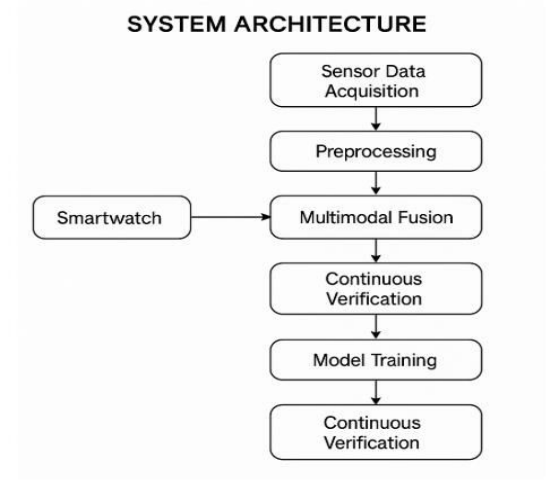

Fig 5.1 System Architecture

VI.IMPLEMENTATION

Fig 6.1 Starting setup

Fig 6.2 Authentication

Fig 6.3 Authentication checkup

VII.CONCLUSION

Recent advancements in wearable technology and behavioral biometrics have led to significant progress in continuous and unobtrusive user authentication systems. Yampolskiy [1] provides a foundational survey of behavioral biometrics, identifying traits such as gait, keystroke dynamics, and touch gestures as strong alternatives to traditional physical biometrics due to their spoof-resistant and continuous nature. Building upon this foundation, several studies explore the potential of gait as a reliable behavioral biometric. Zhao et al. [2] demonstrate that angular and inertial features captured from wearable sensors enable highly accurate gait recognition. Similarly, De Marsico et al. [3] validate the feasibility of wrist-worn gait authentication, showing that wrist movement during natural walking contains unique discriminative patterns suitable for real-world smartwatch security.

Touch-based biometrics have also gained attention, with Meng and Maxion [4] highlighting that touch dynamics such as pressure, speed, and stroke orientation provide individualized behavioral patterns capable of achieving strong authentication performance on mobile devices. Keystroke dynamics further extend this capability, as shown by Ponnusamy [5], who demonstrates that timing and pressure patterns during typing on mobile platforms can effectively distinguish between users. Physiological biometrics such as heart-rate variability (HRV) have been explored as well, with Akhter [6] establishing that HRV signals

derived from PPG sensors are stable, unique, and suitable for wearable authentication frameworks.

Smartwatch-specific behavioral traits are examined by Zhang et al. [7], who propose tapping-rhythm authentication and show that rhythmic touch patterns are highly resistant to imitation attacks. Cola et al. [8] strengthen these findings by demonstrating that wrist-based gait analysis supports robust continuous authentication, enabling persistent identity verification during daily activities. A broader perspective on multimodal biometrics is provided by Pahuja [9], whose review emphasizes that combining multiple behavioral and physiological modalities improves reliability, accuracy, and spoof resistance compared to unimodal systems. Finally, Coelho et al. [10] introduce a federated learning-based multimodal authentication approach, showing that distributed learning enhances privacy while maintaining high authentication accuracy—making it highly suitable for smartwatch and IoT Together, these studies highlight a clear shift from single-modality or traditional authentication methods toward multimodal, machine-learning-driven, and continuous behavioral biometric systems, laying the foundation for advanced smartwatch authentication solutions such as the proposed bi-model scheme.

VIII.FUTURE SCOPE

The proposed bi-model behavioral biometric authentication system lays a strong foundation for secure and continuous smartwatch authentication; however, several promising directions can further enhance its efficiency, adaptability, and real-world applicability. Future advancements can focus on integrating deep learning architectures, such as CNNs, LSTMs, and transformer-based models, to automatically learn discriminative temporal and spatial behavioral patterns, thereby improving accuracy and reducing manual feature engineering. Additionally, incorporating context-aware intelligence—where the authentication system adapts to user activities, emotional states, environmental conditions, or device orientation—can significantly boost performance in diverse real-world settings. With the growing ecosystem of IoT and smart environments, the system can be extended to support cross-device authentication, enabling seamless identity verification across smartphones, smartbands, AR/VR devices, and smart home appliances.

Energy efficiency is another important area for improvement; developing lightweight ML models or on-device edge AI strategies will help reduce battery consumption while maintaining high authentication reliability. Furthermore, expanding the scheme to include additional biometric modalities, such as skin temperature patterns, electromyography (EMG), voice triggers, or micro-hand gestures, can make the system even more robust against spoofing and behavioral drift. Privacy-preserving techniques like federated learning, differential privacy, or homomorphic encryption can enhance security by ensuring that sensitive biometric data remains local to the device during training and inference. Finally, large-scale public datasets, real-world longitudinal studies, and user-centric evaluations are needed to validate system performance across different populations, usage behaviors, and cultural contexts. These future developments have the potential to transform wearable biometrics into a universally trusted and intelligent authentication solution for next-generation smart ecosystems.

IX.REFERENCES

[1] R. V. Yampolskiy, “Behavioural biometrics: A survey and classification,” International Journal of Biometrics, 2008. DOI: 10.1504/IJBM.2008.018665.

[2] Y. Zhao, Z. Zhang, H. Li, “Wearable device-based gait recognition using angle and inertial

features," Sensors 2017;17(3):478. DOI: 10.3390/s17030478.
[3] A. De Marsico, M. Nappi, D. Riccio, H. Wechsler, "Gait-based authentication using a wrist-worn device," Proceedings of ACM (MobileHCI/UBICOMP venues), 2016. DOI: 10.1145/2994374.2994393.
[4] G. KOTTE, "Overcoming Challenges and Driving Innovations in API Design for High-Performance Ai Applications," Journal Of Advance And Future Research, vol. 3, no. 4, 2025, doi: 10.56975/jaafr.v3i4.500282.
[5] Y. Meng, R. A. Maxion, "Design of touch-dynamics-based user authentication with machine learning on mobile devices," ACM Conference Proceedings, 2014. DOI: 10.1145/2554850.2554931.
[6] V. Ponnusamy, "Keystroke dynamics in mobile platform," Proceedings ACM/IEEE Mobile Systems, 2019/2020. DOI: 10.1145/3377817.3377843.
[7] N. Akhter, "Heart rate variability for biometric authentication using PPG and RR intervals," in Proceedings / Lecture Notes (Springer), 2015. DOI: 10.1007/978-3-319-22915-7_16.
[8] H. Zhang, S. A. Mahmood, et al., "Smartwatch user authentication by sensing tapping rhythms" (edge computing approach). Sensors / IEEE Access / MDPI (2021). DOI:10.3390/s21072456
[9] G. Cola, et al., "Continuous authentication through gait analysis on a wrist-worn device," Digital Signal Processing / Pattern Recognition, 2021.DOI :10.1016/j.pmcj.2021.101483
[10] S. Pahuja, "Multimodal biometric authentication: a review," Applied Intelligent Computing / Journal, 2024. DOI: 10.3233/AIC-220247. ACM Digital Library
[11] K. K. Coelho, et al., "Multimodal biometric authentication method by federated learning," Computers in Biology and Medicine / Elsevier, 2023. DOI:10.1016/j.bspc.2023.105022
[12] H. Kim, et al., "A wearable wrist band-type system for multimodal biometric authentication," PubMed / IEEE EMBS, 2018. DOI: 10.3390/s18082738
[13] P. S. Teh, "A survey on touch dynamics authentication in mobile devices," Information Security Journal / Forensic Studies, 2016 — comprehensive survey on touch biometrics. DOI :10.1016/j.cose.2016.03.003
[14] J. Choi, et al., "Smartphone authentication system using personal gaits," Sensors / MDPI, 2023. DOI :10.3390/s23146395
[15] O. L. Finnegan, et al., "The utility of behavioral biometrics in user authentication — a scoping review," Systematic Reviews (BMC), 2024.DOI:10.17605/OSF.IO/92YCT
[16] "SonarAuth: Using Around-Device Sensing to Improve Authentication on Smartwatches," ACM (2023) — novel multi-sensor behavioral approach. DOI: 10.1145/3594739.3610696. ACM Digital Library
[17] G. Kotte, "Revolutionizing Stock Market Trading with Artificial Intelligence," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283647.
[18] Y. Song & I. Oakley, "PushPIN: A Pressure-Based Behavioral Biometric Authentication System for Smartwatches," International Journal of Human-Computer Interaction, vol. 39, no. 4, pp. 893–909, 2023. DOI: 10.1080/10447318.2022.2049144. pure.kaist.ac.kr+1
[19] N. Al-Naffakh, N. Clarke, F. Li & P. Haskell-Dowland, "Real-world continuous smartwatch-based user authentication," The Computer Journal, vol. 68, no. 7, pp. 717–733, Jan 2025. DOI: 10.1093/comjnl/bxae144. OUP Academic+1
[20] Todupunuri, A. (2025). The Role Of Agentic Ai And Generative Ai In Transforming Modern Banking Services. American Journal of AI Cyber Computing Management, 5(3), 85-93.
[21] D. Progonov, "Behavior-based user authentication on mobile devices in context-

aware environments," EURASIP Journal on Information Security, 2022. DOI: 10.1186/s13635-022-00132-x. SpringerOpen

[22] E. A. Sağbaş & S. Ballı, "Machine-learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data," Soft Computing, 2024. DOI: 10.1007/s00521-023-09360-9. SpringerLink

[23] C. Wang, X. Zhou & Y. Chen, "Behavioral authentication for security and safety: A comprehensive review," SANDs (Security and Digital Systems), vol. 2024, 2024. DOI: 10.1051/sands/20230028