REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Polytechnique

Département Électronique

Laboratoire des Dispositifs de Communication et de Conversion Photovoltaïque

Doctoral Thesis
in: Electronics Engineering

Option: **Instrumentation**

Entitled

Behavioral Biometrics for Continuous Authentication of Smartphone Users

Presented by:
Ouadjer Youcef

Publicly defended on January 19, 2026, before a Jury composed of:

President	Prof. Adel Belouchrani	Ecole Nationale Polytechnique.
Examiner	Prof. Jean-Luc Dugelay	EURECOM - Sophia Antipolis - France.
Examiner	Prof. Youcef Chibani	University of Science and Technology Houari Boumediene.
Examiner	Prof. Cherif Larbes	Ecole Nationale Polytechnique.
Invited Examiner	Dr. Nesrine Bouadjenek	Ecole Nationale Polytechnique.
Supervisor	Prof. Mourad Adnane	National School of Autonomous Systems Technology.
Co-Supervisor	Prof. Sid-Ahmed Berrani	National School of Artificial Intelligence.

ENP 2026

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Polytechnique

Département Électronique

Laboratoire des Dispositifs de Communication et de Conversion Photovoltaïque

Doctoral Thesis
in: Electronics Engineering

Option: **Instrumentation**

Entitled

Behavioral Biometrics for Continuous Authentication of Smartphone Users

Presented by:
Ouadjer Youcef

Publicly defended on January 19, 2026, before a Jury composed of:

President	Prof. Adel Belouchrani	Ecole Nationale Polytechnique.
Examiner	Prof. Jean-Luc Dugelay	EURECOM - Sophia Antipolis - France.
Examiner	Prof. Youcef Chibani	University of Science and Technology Houari Boumediene.
Examiner	Prof. Cherif Larbes	Ecole Nationale Polytechnique.
Invited Examiner	Dr. Nesrine Bouadjenek	Ecole Nationale Polytechnique.
Supervisor	Prof. Mourad Adnane	National School of Autonomous Systems Technology.
Co-Supervisor	Prof. Sid-Ahmed Berrani	National School of Artificial Intelligence.

ENP 2026

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Polytechnique

Département Électronique

Laboratoire des Dispositifs de Communication et de Conversion Photovoltaïque

Thèse de Doctorat
en : Électronique

Option : **Instrumentation**

Intitulée

Exploitation des caractéristiques comportementales biométriques pour l'authentification d'un utilisateur de smartphone

Présentée par :

Ouadjer Youcef

Soutenue publiquement le 19 janvier 2026, devant le jury composé de :

Président	Prof. Adel Belouchrani	Ecole Nationale Polytechnique.
Examinateur	Prof. Jean-Luc Dugelay	EURECOM - Sophia Antipolis - France.
Examinateur	Prof. Youcef Chibani	USTHB.
Examinateur	Prof. Cherif Larbes	Ecole Nationale Polytechnique.
Invitée	Dr. Nesrine Bouadjenek	Ecole Nationale Polytechnique.
Directeur de thèse	Prof. Mourad Adnane	ENS de Technologie des Systèmes Autonomes.
Co-Directeur	Prof. Sid-Ahmed Berrani	ENS d'Intelligence Artificielle.

ENP 2026

الملخص

أصبحت الهواتف الذكية ضرورية لإدارة العمليات الحساسة مثل الخدمات المصرفية عبر الإنترنت، والوصول إلى السجلات الطبية، وإجراء المدفوعات الرقمية، واستخدام الخدمات الحكومية. ونتيجة لذلك، ازداد طلب المستخدمين على أنظمة مصادقة قوية وسهلة الاستخدام. ومع ذلك، تعاني أساليب المصادقة التقليدية على الهواتف الذكية، مثل الأساليب المعتمدة على المعرفة (كأرقام التعريف الشخصية وكلمات المرور) والأنظمة البيومترية الثابتة (مثل بصمة الإصبع والتعرّف على الوجه)، من قيود كبيرة. إذ تُعد هذه الأساليب عرضة لهجمات التتبع والتزوير، كما أنها تفشل في توفير أمان مستمر بعد فتح قفل الجهاز. ولمواجهة هذه التحديات، نقترح تصميم وتقييم أنظمة مصادقة مستمرة فعّالة ومتعددة الوسائط تعتمد على القياسات الحيوية السلوكية.

في البداية، تستعرض هذه الدراسة مراجعة شاملة لأحدث الأساليب في مجال المصادقة المستمرة، مع تسليط الضوء على التقدم الأخير في طرائق القياسات الحيوية السلوكية مثل حركات اليد وإيماءات اللمس، إضافة إلى تحديد أوجه القصور في مجموعات البيانات الحالية، ولا سيما غياب الطرائق السلوكية البيومترية المتزامنة ومتعددة الوسائط، إلى جانب الخصائص البيومترية الثابتة مثل ملامح الوجه.

بعد ذلك، يتم تصميم نظام مصادقة مستمرة فعّال من خلال دراسة تقنيات متقدمة لاختيار السمات بهدف تحديد السمات الأكثر أهمية، مما يُظهر تحسناً ثابتاً في الأداء عند استخدام مجموعة السمات المختارة.

علاوة على ذلك، يتم تقديم نظام جديد للمصادقة المستمرة يعتمد على التعلم التباينى ذاتي الإشراف. ويستخدم هذا النظام بنية شبكة عصبية التفافية خفيفة الوزن قائمة على الالتفافات القابلة للفصل عمقياً، مما يحقق دقة عالية في مهام التحقق من هوية المستخدمين والتعرف عليهم، مع الحفاظ على الكفاءة الحسابية.

ومن خلال توسيع إطار التعلم التباينى ذاتي الإشراف الذي تم تقديمه في المساهمة السابقة، يتم تصميم إطار دمج متعدد الوسائط يجمع بين بيانات حركات اليد وإيماءات اللمس. ويتم تنفيذ الدمج على مستوى السمات، حيث يُظهر النظام أداءً قوياً حتى عند استخدام مجموعات بيانات صغيرة ومُعنونة، في الحالات التي تكون فيها البيانات البيومترية المُعلَّمة نادرة.

لمعالجة النقص في مجموعات البيانات «MM-BioSync» وأخيراً، يتم تقديم مجموعة بيانات جديدة متعددة الوسائط تُسمى العامة المتزامنة للقياسات الحيوية السلوكية. وتدمج هذه المجموعة بيانات من الكاميرات الأمامية، ومستشعرات الحركة، وتفاعلات شاشة اللمس. وتُظهر التجارب المُجراة على هذه المجموعة أن دمج جميع الوسائط التي تم التقاطها أثناء مهام القراءة والكتابة يحقق أفضل أداء في التحقق من هوية المستخدمين، مما يؤكد أهمية الأساليب متعددة الوسائط في المصادقة المستمرة.

تُبرز نتائج هذه الأطروحة الإمكانات الكبيرة للقياسات الحيوية السلوكية ودمج الوسائط المتعددة في تمكين المصادقة المستمرة للمستخدمين. ومن خلال معالجة التحديات الرئيسية المتعلقة بأداء النماذج، والكفاءة الحسابية، وتوفر مجموعات البيانات، يُسهم هذا العمل في تطوير أحدث ما توصل إليه البحث العلمي، ويوفر أساساً لتطوير حلول مصادقة آمنة وسهلة الاستخدام على الهواتف الذكية.

الكلمات المفتاحية:

التعلم ذاتي الإشراف؛ القياسات الحيوية السلوكية؛ المصادقة المستمرة؛ مجموعة بيانات متعددة الوسائط.

Résumé

Les smartphones sont devenus essentiels pour la gestion d'opérations sensibles telles que les services bancaires en ligne, l'accès aux dossiers médicaux, les paiements numériques ou l'utilisation des services administratifs. En conséquence, les utilisateurs exigent des systèmes d'authentification robustes. Toutefois, les méthodes d'authentification traditionnelles, basées sur la connaissance (par exemple, les codes PIN ou mots de passe) ou sur des données biométriques statiques (empreintes digitales, reconnaissance faciale), présentent des limitations majeures. Elles sont vulnérables aux attaques par traces ou usurpation, et ne garantissent aucune sécurité continue une fois l'appareil déverrouillé. Pour répondre à ces défis, nous proposons la conception et l'évaluation de systèmes d'authentification continue, efficaces et multi-modaux, exploitant la biométrie comportementale.

En premier lieu, le travail présente une revue complète des méthodes d'authentification continue les plus récentes, mettant en lumière les avancées dans les modalités biométriques comportementales telles que les mouvements de la main et les gestes tactiles, tout en identifiant les limitations des jeux de données existants, notamment l'absence de modalités biométriques comportementales multi-modales et synchronisées, ainsi que le manque d'intégration avec des caractéristiques biométriques statiques comme le visage.

Ensuite, un système d'authentification continue efficace est conçu en explorant des méthodes avancées de sélection de caractéristiques, permettant d'identifier les traits les plus pertinents et d'améliorer les performances grâce à un sous-ensemble optimisé.

Par la suite, un nouveau système d'authentification continue est proposé, basé sur un apprentissage auto-supervisé. Ce système s'appuie sur une architecture légère de réseau de neurones convolutifs, assurant une haute précision dans les tâches de vérification et d'identification tout en maintenant une efficacité computationnelle.

En prolongeant ce cadre d'apprentissage auto-supervisé, nous concevons un modèle de fusion multi-modale, combinant les données issues des mouvements de la main et des gestes tactiles. La fusion est réalisée au niveau des caractéristiques, démontrant une performance robuste même sur des jeux de données annotés de petite taille.

Enfin, un nouveau jeu de données multi-modal, MM-BioSync, est introduit pour pallier le manque de jeux de données publics synchronisés en biométrie comportementale. Ce jeu intègre des données issues de caméras frontales, de capteurs de mouvement et d'interactions avec l'écran tactile. Les expériences menées montrent que l'intégration de toutes les modalités capturées lors des tâches de lecture et d'écriture fournit les meilleures performances en vérification d'utilisateur, confirmant ainsi la pertinence des approches multi-modales pour l'authentification continue.

Les résultats de cette thèse mettent en évidence le potentiel des biométries comportementales et de la fusion multi-modale dans l'établissement de systèmes d'authentification continue. En répondant aux défis liés aux performances des modèles, à l'efficacité computationnelle et à la disponibilité des données, ce travail fait progresser l'état de l'art et ouvre la voie à des solutions d'authentification sécurisées et adaptées aux smartphones.

Mots-clés: Apprentissage auto-supervisé ; Authentification continue.

Abstract

Smartphone devices have become essential for managing sensitive operations such as online banking, accessing medical records, making digital payments, and using government services. As a result, consumers have raised the demand for robust and user-friendly authentication systems. However, traditional smartphone authentication methods such as knowledge-based (e.g., PIN codes, passwords) and static biometric systems (e.g., fingerprint, facial recognition) suffer from significant limitations. These methods are vulnerable to smudge and spoofing attacks, and fail to provide ongoing security once a device is unlocked. To address these challenges, we propose the design and evaluation of efficient, multi-modal continuous authentication systems leveraging behavioral biometrics.

As a starting point, the research presents a comprehensive review of state-of-the-art methods for continuous authentication, highlighting recent progress in behavioral biometric modalities such as hand movement and touch gestures, and identifying limitations in existing datasets. Particularly the lack of synchronized multi-modal behavioral biometric modalities, combined with static biometric characteristics such as facial features.

Following, an efficient continuous authentication system is designed, by investigating advanced feature selection to identify most relevant features, showing consistent improvement with the subset of selected features.

Further a new continuous authentication system is introduced using self-supervised contrastive learning. The system employs a lightweight convolutional neural network architecture based on depthwise separable convolutions, achieving high accuracy in user verification and identification tasks while maintaining computational efficiency.

By extending the original self-supervised contrastive learning framework introduced in the previous contribution, a multi-modal fusion framework is designed, by combining hand movement and touch gesture data. Fusion is performed at the feature-level, demonstrating robust performance even on small annotated datasets where labeled biometric data is scarce.

Lastly, a novel multi-modal dataset, MM-BioSync, is introduced to address the lack of synchronized behavioral biometric public datasets. The dataset integrates data from front-facing cameras, motion sensors, and touchscreen interactions. Experiments conducted on the dataset reveal that integrating all modalities captured during reading and writing tasks yields the best performance in user verification, underscoring the value of multi-modal approaches for continuous authentication.

The findings of this thesis highlight the potential of behavioral biometrics and multimodal fusion in enabling continuous user authentication. By addressing key challenges related to model performance, computational efficiency, and dataset availability, this work advances the state-of-the-art and provides a foundation for developing secure and user-friendly authentication solutions on smartphones.

Keywords: Behavioral biometrics; Continuous authentication; Multi-modal dataset; Self-supervised learning.

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Professor Adnane Mourad, for his unwavering guidance, mentorship, and support throughout this journey. His profound knowledge and insightful feedback have been invaluable in shaping my growth as a researcher. Every meeting with him during the course of this thesis was an opportunity to refine my work and share impactful ideas.

I would like to extend my heartfelt gratitude to my co-supervisor, Professor Berrani Sid-Ahmed, for being an exceptional mentor and source of inspiration. I am deeply fortunate to have learned so many facets of research under his guidance, which have significantly enriched my academic and professional journey. His unwavering belief in my potential encouraged me to tackle challenging projects that I once thought were beyond my capabilities.

I would also like to express my sincere gratitude to Professor Bouadjenek Nesrine for her valuable advice and support. I had the privilege of collaborating with her in organizing the 9-th edition of International School on Signal Processing and its Applications in June 2024. An enriching experience that greatly contributed to expand my knowledge.

There are other remarkable people to whom I am grateful. I would like to specially thank Professor Jean-Luc Dugelay from Eurecom. Professor Dugelay hosted me as a visiting Ph.D student, and made the experience very enriching. I would also like to express my gratitude to Professor Chiara Galdi from Eurecom. Together with Professor Jean-Luc Dugelay and my supervisors, we started a research collaboration that I am willing to strengthen in the near future.

I would like to express my sincere gratitude to Professor Adel Belouchrani, President of the jury, for kindly accepting to review and evaluate this thesis. His expertise and insightful feedback are deeply appreciated. I also extend my thanks to Professor Youcef Chibani for generously agreeing to serve as a member of the jury and for his valuable time and consideration.

I am equally grateful to Professor Cherif Larbes, Director of the LDCCP Laboratory, for his participation as a jury member and for creating an exceptional research environment within the lab. His efforts to promote academic excellence and support young researchers have significantly contributed to my doctoral journey. I consider myself fortunate to have conducted my research within the LDCCP laboratory.

I am thankful to all members of École Nationale Polytechnique with whom I interacted, and made the PhD journey as pleasant as possible. Thanks to all my colleagues and friends.

Finally I am thankful to my family members who supported me during the past years, they believed in me more than I did, and encouraged me to give my best. There are no enough words to describe my gratitude for them.

Contents

List of Tables

List of Figures

I General context . . . 17
II Role of behavioral biometrics in continuous authentication . . . 18
III Structure of the thesis . . . 19
IV Scope and contributions of the thesis . . . 21

Chapter 1 Background: Continuous Authentication and Behavioral Biometrics 24

1.1 Introduction . . . 25
1.2 Continuous authentication as a biometric system . . . 25
1.2.1 Operational modes of biometric systems . . . 25
1.2.2 Biometric system architecture . . . 26
1.2.3 Evaluation of biometric systems . . . 28
1.3 Behavioral biometric modalities . . . 30
1.3.1 Walking gait . . . 30
1.3.2 Touch gestures . . . 30
1.3.3 Keystroke dynamics . . . 31
1.3.4 Behavior profiling . . . 31
1.3.5 Hand movement . . . 31
1.4 Sensors used for continuous authentication . . . 31
1.4.1 Accelerometer . . . 31
1.4.2 Gyroscope . . . 31
1.4.3 Magnetometer . . . 32
1.4.4 Touch sensor . . . 33
1.5 Conclusion . . . 34

Chapter 2 Related Works 35

2.1 Introduction . . . 36
2.2 Behavioral biometrics-based continuous authentication methods . . . 36
2.2.1 Walking gait . . . 36
2.2.2 Touch gestures . . . 39
2.2.3 Keystroke dynamics . . . 41
2.2.4 Behavior profiling . . . 43

2.2.5 Hand movement . . . 45
2.2.6 Multi-modal continuous authentication . . . 47
2.2.6.1 Sensor-level fusion . . . 48
2.2.6.2 Feature-level fusion . . . 48
2.2.6.3 Score-level fusion . . . 49
2.2.6.4 Decision-level fusion . . . 49
2.2.6.5 Rank-level fusion . . . 50
2.3 Multi-modal datasets . . . 52
2.4 Conclusion . . . 55

Chapter 3 Feature selection for touch-based behavioral biometric authentication 56
3.1 Introduction . . . 57
3.2 Feature selection methods: an overview . . . 57
3.3 Feature Selection Using Gradient-Tree Boosting . . . 57
3.3.1 Obtained results . . . 60
3.3.2 Discussion . . . 61
3.4 Conclusion . . . 61

Chapter 4 Continuous Authentication on Smartphones based on Self-supervised Learning 62
4.1 Introduction . . . 63
4.2 Self-Supervised Contrastive Learning and Gesture Patterns . . . 63
4.2.1 Contrastive learning framework . . . 64
4.2.1.1 Data augmentation . . . 64
4.2.1.2 CNN Base Encoder . . . 65
4.2.1.3 Neural Network projection Head . . . 66
4.2.1.4 Contrastive loss . . . 66
4.2.2 Downstream evaluation . . . 67
4.2.2.1 Datasets description and implementation . . . 67
4.2.2.2 Obtained results . . . 67
4.2.2.2.1 User verification accuracy . . . 68
4.2.2.2.2 User Identification and Computational Cost . . . 68
4.2.2.2.3 Effect of varying standard deviation during data augmentation . . . 70
4.2.2.2.4 User verification on small annotated datasets . . . 70
4.2.3 Discussion . . . 72
4.3 Self-Supervised Based Multi-Modal Fusion for Continuous Biometric Authentication on Mobile Devices . . . 73
4.3.1 Multimodal fusion . . . 73
4.3.2 Multi-modal data . . . 73
4.3.3 Encoder module . . . 74
4.3.4 Multi-modal fusion module . . . 75
4.3.5 Contrastive task . . . 75

4.3.6 Experimental evaluation 75
4.3.6.1 Datasets and Implementation details 76
4.3.6.2 User verification 76
4.3.6.3 Evaluation on small annotated datasets 77
4.3.7 Discussion 77
4.4 Conclusion 79

Chapter 5 Multi-Modal Synchronized Sensing Dataset for Implicit Biometric Verification 80
5.1 Introduction 81
5.2 The MM-BioSync Dataset 81
5.2.1 Acquisition process 81
5.2.2 Dataset organization 83
5.2.3 Description of Modalities 83
5.2.3.1 Hand movement 83
5.2.3.2 Touch gestures 87
5.2.3.3 Keystroke patterns 87
5.2.3.4 Front-facing images 87
5.3 Experiments and evaluation 88
5.3.1 Training dataset 89
5.3.2 Baseline models 90
5.3.3 Results and discussion 91
5.4 Conclusion 92

Bibliography 97

Confidentielle