A LIGHTWEIGHT FRAMEWORK FOR PRIVACY-PRESERVING BEHAVIORAL AUTHENTICATION: BALANCING RECOGNITION ACCURACY AND SYSTEM LATENCY

A PROJECT PROPOSAL SUBMITTED BY

W.M.T.R.S Weerakoon
(S20545)

to the

DEPARTMENT OF STATISTICS AND COMPUTER SCIENCE

in partial fulfillment of the requirements of the

Degree of Bachelor of Science (Honours) in Computer Science
of the

UNIVERSITY OF PERADENIYA, SRI LANKA

2 February, 2026

Preface

This is a proposal for the Project in Computer Science II (Research Project – CSC4996) for partial fulfillment of the requirements of the Degree of Bachelor of Science (Honours) in Computer Science at the Department of Statistics and Computer Science, University of Peradeniya, Sri Lanka.

This proposal provides the scope and context of the research project to be undertaken. It details the aims and research questions, background, methodology, and project design. This document also provides a schedule for the completion of the project, including a description of anticipated results and final products

The intended audience of this document is the academic staff of the Department of Statistics and Computer Science, University of Peradeniya, who will evaluate the project to determine whether it should be approved as proposed, approved with modifications, or not approved.

Table of Contents

List of Figures

List of Tables

List of Equations

List of Abbreviations

1.0 Introduction

Overview of the Research Domain In mechanisms such as Personal Identification Numbers (PINs) and passwords are increasingly becoming single points of failure [1]. They are susceptible to vulnerabilities like shoulder surfing, brute-force attacks, and social engineering [1], [2]. To address these vulnerabilities, Behavioral Biometrics—specifically Keystroke Dynamics and Mouse/Touch Dynamics—has emerged as a powerful alternative [3], [4]. Unlike static passwords, behavioral biometrics allow for continuous, passive authentication, verifying a user's identity based on *how* they interact with a device rather than *what* they know [5], [6].

1.1 Problem Statement

The primary problem addressed by this research is the critical trade-off between **user privacy** and **system latency** in behavioral authentication systems on resource-constrained mobile devices. While behavioral biometrics—such as keystroke dynamics and touch interactions—offer a robust solution for continuous authentication, the storage and processing of these behavioral patterns present significant security risks [3].

This issue affects millions of mobile banking and enterprise users who rely on smartphones for sensitive transactions. Unlike passwords, behavioral biometrics are immutable; a user cannot change their typing rhythm or hand geometry if the biometric template is compromised. Therefore, a breach of raw behavioral data constitutes a permanent loss of digital identity [1].

Current approaches fail to address this problem effectively due to a technical dichotomy between accuracy and efficiency:

- **Privacy Gaps in High-Accuracy Models:** State-of-the-art deep learning frameworks, such as those utilizing Recurrent Neural Networks (RNNs) or Image-based Encoding (e.g., KDPrint), achieve low Equal Error Rates (EER) but typically require the storage of **raw behavioral features** [2], [4]. This creates a single point of failure where the database becomes a high-value target for attackers.
- **Efficiency Gaps in Privacy-Preserving Methods:** Conversely, strong cryptographic solutions like Fully Homomorphic Encryption (FHE) allow for secure computation but suffer from prohibitive computational overhead. Research indicates that such heavy encryption schemes often introduce latencies ranging from seconds to minutes, rendering them impractical for **real-time, continuous authentication** where decisions must be made in milliseconds to maintain a seamless user experience [3].

There is currently no lightweight framework that effectively balances these conflicting requirements. This research seeks to bridge this gap by utilizing **Orthogonal Random Projections** to secure templates without degrading the speed or accuracy required for mobile devices.

1.2 Research Aim and Objectives

The primary aim of this research is to develop a lightweight, privacy-preserving framework for continuous behavioral authentication on mobile devices. This framework seeks to balance recognition accuracy and system latency by utilizing Orthogonal Random Projections for template security and Deep Support Vector Data Description (Deep SVDD) for efficient anomaly detection.

1. **To design a privacy-preserving feature transformation pipeline:** Develop a mechanism using **Orthogonal Random Projections (Johnson-Lindenstrauss Lemma)** [7] that secures behavioral biometric templates (making them mathematically irreversible) while preserving the Euclidean distances required for accurate pattern recognition.

2. **To optimize feature engineering for mobile efficiency:** Implement **KDPrint-style standardization** to transform raw time-series data into standardized image encodings, ensuring high recognition accuracy without the noise sensitivity of Min-Max scaling [4].

3. **To implement a lightweight anomaly detection model:** Develop a **Deep SVDD (Support Vector Data Description)** classifier [8] capable of running offline on mid-range mobile devices to distinguish between genuine users and imposters with minimal computational overhead.

4. **To evaluate the trade-off between privacy, accuracy, and latency:** Conduct a comparative analysis of the proposed framework against existing baselines (such as raw-data RNNs and Homomorphic Encryption), measuring performance metrics including **Equal Error Rate (EER)**, **System Latency (ms)**, and **Memory Usage** [2], [8].

1.3 Research Questions

To address the identified gaps in privacy and efficiency, this research aims to answer the following key questions:

1. **Primary Research Question:** To what extent can **Orthogonal Random Projections** (based on the Johnson-Lindenstrauss Lemma) balance

the conflicting requirements of template privacy, recognition accuracy, and system latency in behavioral authentication?

2. **Impact on Privacy and Irreversibility:** How effective is the proposed projection mechanism in rendering behavioral templates mathematically irreversible to attackers, compared to storing raw features or using standard Min-Max scaling?

3. **Feasibility for Mobile Environments:** Can a **Deep SVDD** (Support Vector Data Description) anomaly detection model achieve real-time authentication latency (e.g., < 100ms) on mid-range mobile devices without exceeding memory constraints?

2.0 Background

2.1 Technical and Theoretical Background

2.2 Literature Review

2.3 Research Gap

2.4 Assumptions and Constraints

- **Assumptions:** The system assumes users have a smartphone with standard accelerometer and gyroscope sensors.
- **Constraints:** The model must run offline on mid-range mobile devices without exceeding 50MB of memory usage.

3.0 Methodology and Project Design

3.1 Overview of the Proposed Methodology/Research Design

3.2 Data Collection

3.3 Ethical Considerations

3.4 Evaluation and Validation

- **False Acceptance Rate (FAR)**
- **False Rejection Rate (FRR)**
- **Equal Error Rate (EER)**
- **System Latency (ms)**

4.0 Anticipated Results/Final Products

4.1 Expected Outcomes

- A fully functional Android application capable of continuous authentication.
- A comparative analysis report on different RNN architectures (LSTM vs. GRU).
- A research paper submitted to an IEEE conference.

4.2 Project Deliverables

1. **Software Prototype:** Source code and executable APK.
2. **Final Thesis:** Comprehensive documentation of the research process.
3. **User Manual:** Guide for installing and testing the application.

4.3 Project Timeline

5.0 Project Schedule

5.1 Timeline and Gantt Chart

Phase	**Activity**	**Duration**
1	Literature Review	Months 1-2
2	Data Collection	Month 3
3	Model Implementation	Months 4-5
4	Testing and Validation	Month 6
5	Thesis Writing	Months 7-8

Table 1: Proposed Project Timeline

5.2 Milestones and Deliverables

- **Milestone 1:** Completion of Literature Review (Date)
- **Milestone 2:** Prototype Development (Date)
- **Final Submission:** Thesis and Defense (Date)

References

[1] S. S. Pirzado and et al., "Keystroke dynamics based technique to enhance the security in smart devices," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 1, pp. 123–133, 2021.

[2] A. T. Kiyani, A. Lasebae, K. Ali, M. U. Rehman, and B. Haq, "Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach," *IEEE Access*, vol. 8, pp. 156 177–156 189, 2020.

[3] M. Rahman and et al., "Scalable behavioral authentication for mobile devices," *Sensors*, vol. 21, no. 14, p. 4890, 2021.

[4] Y. Kim, D. Shin, and N. Kwon, "Kdprint: Passive authentication using keystroke dynamics-to-image encoding via standardization," *arXiv preprint arXiv:2405.01080*, 2024, Accessed via arXiv.

[5] S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics," in *European Convention on Security and Detection*, IET, 1995, pp. 111–114.

[6] F. Monrose and A. D. Rubin, "Password hardening based on keystroke dynamics," in *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS)*, ACM, 1999, pp. 73–82.

[7] W. B. Johnson and J. Lindenstrauss, "Extensions of lipschitz mappings into a hilbert space," in *Conference in modern analysis and probability*, Contemporary Mathematics, American Mathematical Society, 1984, pp. 189–206.

[8] L. Ruff et al., "Deep one-class classification," in *Proceedings of the 35th International Conference on Machine Learning (ICML)*, 2018, pp. 4393–4402.

Appendices

Appendix A: Survey Form

Appendix B: Code Snippets