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 The more conventional knowledge-based authentication techniques, such passwords and Personal Identification Numbers (PINs), are quickly turning into single points of failure in the constantly changing cybersecurity landscape of today. Well-known assaults like shoulder surfing, brute-force attacks, and social engineering can affect these static authentication systems. Behavioral Biometrics, more especially Keystroke Dynamics and Mouse Dynamics, has become a strong alternative authentication technique for confirming digital identification in response to the drawbacks and weaknesses of static authentication approaches. Behavioral biometrics enable continuous and passive user authentication based on a user's unique typing patterns or mouse movement trajectories, as opposed to static passwords, which authenticate what a user knows.

Motivation and Significance The use of behavioral biometrics creates a significant privacy conundrum even if they provide strong defense against unwanted access. In contrast to passwords, biometric characteristics are inherent and unchangeable; if the biometric template is compromised, a user cannot alter their hand geometry or typing rhythm. The storing of raw templates in a central database is therefore a high-risk liability since a breach of raw behavioral data results in a permanent loss of digital identity.

The state-of-the-art solutions to this privacy issue involve the use of heavy cryptographic techniques, including Homomorphic Encryption (HE), which enables computations to be performed on the encrypted data. Nevertheless, these approaches involve unaffordable computational costs and high system latency, making them unsuitable for real-time, continuous monitoring in resource-constrained edge devices. This gives rise to a substantial trade-off, whereby the current solutions are either fast and privacy-invasive (using raw data) or private but slow (using heavy encryption).

Existence of a Research Gap Unified frameworks that successfully strike a compromise between robust template privacy and high-speed anomaly detection are currently lacking. Current "lightweight" methods frequently ignore the requirement for biometric revocability—the capacity to cancel and replace a compromised biometric template—in favor of concentrating only on recognition accuracy. In order to fill this gap, this study suggests a brand-new, lightweight framework that combines Deep Support Vector Data Description (Deep SVDD) with Keyed Johnson-Lindenstrauss (JL) Projections. This method seeks to ensure a safe

and smooth user experience by offering mathematically guaranteed privacy and template revocability without the latency costs of conventional encryption.

1.1 Problem Statement

The crucial trade-off between user privacy, system latency, and template revocability in continuous behavioral authentication systems is the main issue this study attempts to solve. Although behavioral biometrics, like Keystroke Dynamics and Mouse Trajectories, provide a reliable way to continuously confirm a user's identification, there are serious security vulnerabilities associated with the processing and storage of these behavioral patterns. Behavioral biometrics are inherent and unchangeable, unlike passwords or tokens; if the biometric template is hacked, a person cannot alter their hand shape or biomechanical typing rhythm. Therefore, centralized biometric databases are a high-value target for attackers as a breach of raw behavioral data results in a permanent loss of digital identity.

Current approaches fail to address this problem effectively due to a technical dichotomy between security and performance:

1.2 Research Aim and Objectives

1.3 Research Questions

2.0 Background

2.1 Theoretical and Technical Background

2.2 Literature Review

2.3 Research Gap

2.4 Assumptions and Constraints

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

4.0 ANTICIPATED RESULTS/FINAL PRODUCTS

5.0 Project Schedule

A Appendices