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

PINs Personal Identification Numbers

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

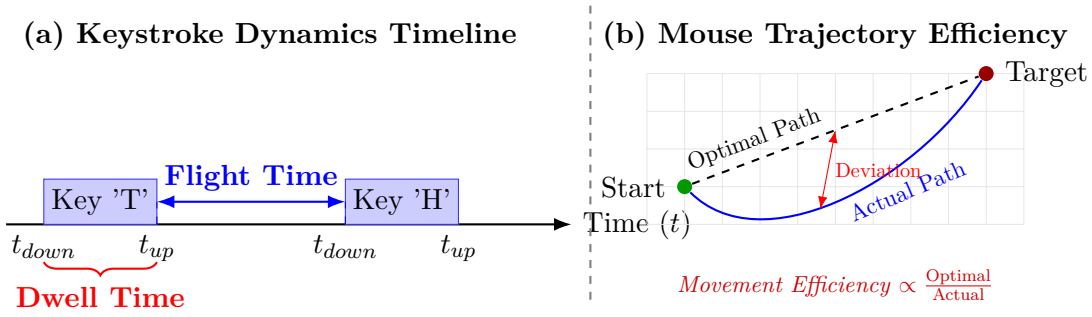

Figure 1: Visual Representation of Biometric Features. **(a)** Keystroke Dynamics: Dwell Time represents the key press duration, while Flight Time measures the latency between distinct keystrokes. **(b)** Mouse Dynamics: Comparison between the optimal straight-line path and the actual user trajectory, used to calculate movement efficiency and curvature.

2.1.1 Keystroke Dynamics

This is the measurement of biomechanical typing patterns. The fundamental features include Dwell Time (duration a key is pressed) and Flight Time (latency between releasing one key and pressing the next). These features form a unique "digital signature" for each user.

2.1.2 Mouse Dynamics

This involves analyzing the unique behavioral patterns of a user's mouse interactions. Unlike simple click-tracking, this research focuses on complex motor-skill features:

- **Movement Efficiency:** The ratio of the straight-line distance to the actual path taken (analyzing hand jitter and curvature).
- **Velocity & Acceleration Profiles:** The rate of speed change as the cursor approaches a target (e.g., users often decelerate differently when clicking a button).
- **Click-to-Click Latency:** The timing between releasing a button and moving to the next location.

- **Drag-and-Drop characteristics::** The pressure and speed consistency during sustained click events.

2.1.3 Recurrent Neural Networks (RNNs) & LSTMs

Since keystroke data is inherently sequential (a time-series of events), standard feed-forward networks often fail to capture temporal dependencies. RNNs, and specifically Long Short-Term Memory (LSTM) networks, are theoretically suited for this task as they maintain a "memory" of previous inputs, allowing them to model complex, non-linear typing rhythms over time.

2.1.4 Johnson-Lindenstrauss (JL) Lemma

To address the "curse of dimensionality" and system latency, this research utilizes the JL Lemma. This mathematical theorem states that points in a high-dimensional space can be projected into a lower-dimensional space using Orthogonal Random Projections while approximately preserving the Euclidean distances between them. This allows for lightweight processing without significant loss of accuracy.

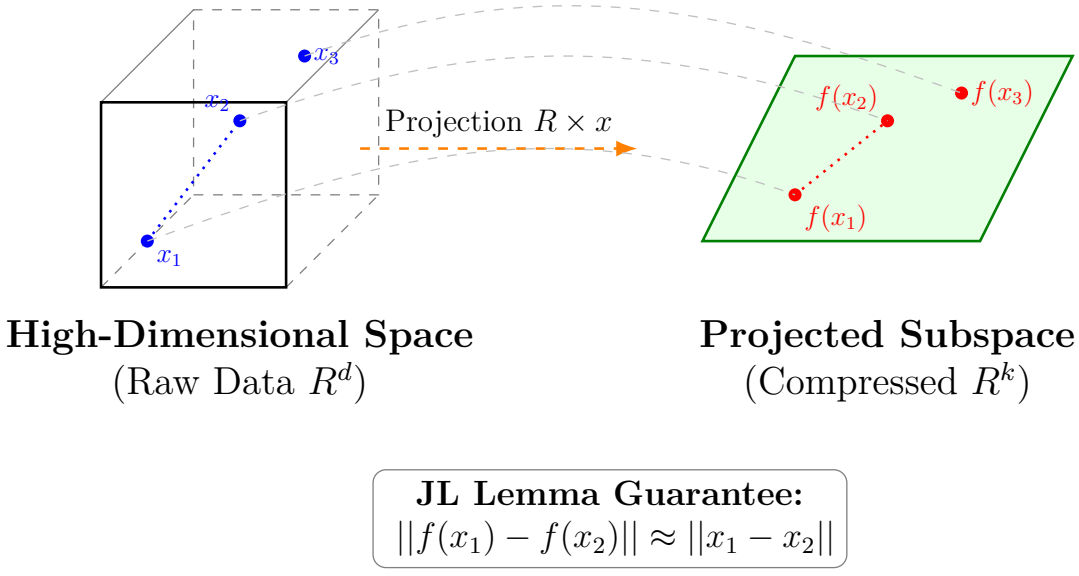

Figure 2: Conceptual Visualization of the Johnson-Lindenstrauss (JL) Lemma. Points from a high-dimensional feature space (Left) are projected onto a lower-dimensional subspace (Right). The blue and red dotted lines illustrate that the relative Euclidean distances between points are approximately preserved despite the massive reduction in dimensions.

2.1.5 Homomorphic Encryption (HE)

To ensure privacy, the system employs Homomorphic Encryption, a cryptographic form that allows computations to be performed on encrypted data without first decrypting it. This ensures that the user's raw biometric template is never exposed in plaintext during the authentication process.

2.2 Literature Review

2.2.1 Overview of Reviewed Literature

To establish a theoretical framework for this research, a comprehensive review of existing literature was conducted, focusing on Keystroke Dynamics, Mouse Dynamics, and Privacy-Preserving Machine Learning. The following table summarizes the key research papers referenced, highlighting their specific contributions to this project ("Key Takeaway") and the limitations ("Research Gap") that this proposal aims to address.

Table 1: Summary of Key Related Studies

Reference & Study	**Key Contribution to This Project**	**Identified Gap / Limitation**
Gaines et al. (1980) & Joyce et al. (1990)	**Foundational Theory:** Established that typing rhythms (dwell/flight time) are unique and stable enough for identity verification.	Relied on static, fixed-text passwords, which are insufficient for continuous authentication.
Mondal & Bours (2017)	**Multimodal Fusion:** Proved that combining Keystroke and Mouse dynamics significantly reduces Equal Error Rate (EER) compared to single modalities.	Fusion was achieved by simply concatenating features, creating a high-dimensional vector that slows down real-time processing.
Kim et al. (2018)	**Feature Engineering:** Introduced "user-adaptive" features, showing that personalized feature selection improves accuracy.	Focused entirely on accuracy; lacked any "template protection" or encryption to secure the stored data.
Kim et al. (2025)	**Deep SVDD Validation:** Demonstrated that Deep SVDD outperforms traditional models (6.7% EER) by encoding time-series data into images.	Restricted to *mobile PINs* (touch interactions) and lacked cryptographic encryption (HE) or multimodal fusion (Mouse).
Kiyani et al. (2020)	**Continuous Authentication:** Validated the use of Recurrent Neural Networks (RNNs) for verifying users continuously, not just at login.	Did not address the high latency introduced when trying to add encryption to these continuous streams.
Islam et al. (2021)	**Scalability Metrics:** Provided a framework for measuring how error rates grow as the user database size increases.	Addressed scalability of accuracy but not the scalability of privacy (how to store millions of secure templates).

2.2.2 Foundational Studies (Static Authentication)

Early research laid the groundwork for typing pattern analysis. Gaines et al. (1980) demonstrated that typing rhythms are unique to individuals, identifying that even simple digraph latencies could distinguish users with high confidence. Building on this, Joyce and Gupta (1990) formalized the use of "latency signatures" for identity verification, showing that comparing a test signature against a mean reference signature could achieve low impostor pass rates. Monrose et al. (1999) extended this concept to "password hardening," combining typing rhythms with passwords to increase entropy against offline attacks.

2.2.3 Feature Engineering and Adaptive Systems

As research matured, the focus shifted to handling the variability in human behavior. Kim et al. (2018) highlighted the limitations of fixed-text authentication and proposed "user-adaptive feature extraction." Their work demonstrated that by dynamically selecting features based on a user's specific typing speed ranks (rather than a fixed keyboard layout), the Equal Error Rate (EER) could be significantly reduced. This underscored the need for personalized models in behavioral authentication.

2.2.4 Mouse Dynamics and Multimodal Fusion

Research into mouse dynamics has evolved from simple statistics to complex trajectory analysis. Ahmed and Traore (2007) pioneered the use of movement speed and direction histograms, achieving reasonable accuracy but noting high false-positive rates in unconstrained environments. Later, Zheng et al. (2011) improved this by analyzing "point-by-point" angle-based metrics, proving that fine-grained motor skills are harder to forge than simple click statistics.

Recent studies have shifted toward Multimodal Authentication, combining keystroke and mouse data to overcome the weaknesses of single-modality systems. Mondal and Bours (2017) demonstrated that fusing these two biometrics significantly reduces the Equal Error Rate (EER) because an imposter is unlikely to mimic both a user's typing rhythm and their mouse hand-eye coordination simultaneously. However, existing multimodal frameworks often simply concatenate feature vectors, leading to massive dimensionality that slows down real-time processing—a problem this research aims to solve using the JL Lemma.

2.2.5 Deep Learning and Continuous Authentication

Recent approaches have adopted Deep Learning (DL) to improve accuracy. Zareen et al. (2018) utilized Bayesian Regularized Neural Networks, achieving an EER of 0.9%, which outperformed many standard statistical methods. Kiyani et al. (2020) proposed a "Robust Recurrent Confidence Model" (R-RCM) using ensemble learning for continuous monitoring.

Most recently, **Kim et al. (2025)** proposed "KDPrint," a method that transforms keystroke dynamics into images and utilizes **Deep Support Vector Data Description (Deep SVDD)** for anomaly detection. Their work achieved a notable EER of 6.7% on mobile devices, validating Deep SVDD as a superior classifier for one-class authentication tasks. However, their approach focused exclusively on mobile PINs (touch interaction) and utilized image encoding for feature representation rather than cryptographic privacy. This leaves a significant gap for applying Deep SVDD to *encrypted, multimodal* desktop environments, which this research aims to fulfill.

2.2.6 Scalability and System Performance

While accuracy has improved, scalability remains a challenge. Islam et al. (2021) introduced the notion of "Scalable Behavioral Authentication," analyzing how verification error rates increase as the user database grows. They proposed a "doppelganger-based" personalized verification algorithm to mitigate error growth, highlighting that system performance must be evaluated not just on accuracy, but on its ability to handle large-scale deployments.

2.3 Research Gap

Despite the extensive literature on improving the accuracy of behavioral biometrics (Kiyani et al., 2020; Zareen et al., 2018) and recent advancements in Deep Learning anomaly detection (Kim et al., 2025), a critical trilemma remains unsolved: balancing **Accuracy**, **Efficiency**, and **Privacy**.

1. **Computation vs. Latency in Multimodal Systems:** Integrating Mouse Dynamics with Keystroke Dynamics doubles the feature space complexity. While recent studies like Kim et al. (2025) successfully utilized Deep SVDD for mobile PINs, they focused on single-modality touch data. Processing a high-dimensional, multimodal stream (typing + mouse trajectories) creates a computational bottleneck that current frameworks fail to address efficiently without dimensionality reduction.

2. **Privacy Vulnerability (Lack of Encryption):** Most existing frameworks focus on verifying raw feature vectors or transformed representations. For instance, while Kim et al. (2025) introduced "image encoding" to obscure raw keystrokes, this is a feature transformation technique, not a cryptographic privacy guarantee. It lacks the mathematical irreversibility of **Homomorphic Encryption (HE)**. If the central database is compromised, these behavioral templates (images or vectors) are susceptible to reverse-engineering or replay attacks, leading to a permanent loss of digital identity.

3. **Lack of Integrated Privacy-Preserving Architectures:** While cryptographic solutions exist, standard encryption prevents the system from performing the distance calculations needed for authentication (like Euclidean distance). There is currently no implementation that combines the anomaly detection power of **Deep SVDD** (validated by Kim et al., 2025) with **Homomorphic Encryption** for secure, privacy-preserving inference.

2.3.1 Summary of Novel Contributions

This study makes the following original contributions to the field of behavioral authentication:

1. **Dual-Mode Privacy Architecture**

   This research proposes a novel dual-mode behavioral authentication framework that separates high-security encrypted inference (CKKS-based) from lightweight projected privacy mode (Johnson–Lindenstrauss-based), enabling adaptive deployment based on transaction risk level. The architecture allows the system to dynamically balance security guarantees and computational efficiency.

2. **Dimensionality-Constrained Encrypted Inference**

   Unlike prior work that applies Deep SVDD to raw or image-encoded features, this study evaluates Deep SVDD operating on Johnson–Lindenstrauss compressed embeddings. It explicitly analyzes how dimensionality reduction affects Equal Error Rate (EER), inference latency, and encryption overhead, thereby formalizing the impact of projection dimension k on encrypted biometric verification.

3. **Formal Privacy–Latency–Accuracy Trade-off Quantification**

   This work introduces an integrated evaluation framework that jointly measures:

- Biometric performance (EER, FAR, FRR)
- Computational efficiency (Inference Latency, Encryption Overhead Ratio)
- Information-theoretic privacy (Mutual Information, Reconstruction Error)

To the best of our knowledge, no prior behavioral biometric study simultaneously quantifies these three dimensions under homomorphically encrypted inference.

4. **Encrypted One-Class Authentication Validation**

   This study provides the first empirical validation of Deep SVDD distance-based anomaly detection executed over CKKS-encrypted, Johnson–Lindenstrauss-projected multimodal biometric templates (keystroke + mouse dynamics), demonstrating the feasibility of privacy-preserving one-class authentication in resource-constrained environments.

2.3.2 Gap Definition

There is currently no unified framework that utilizes **Orthogonal Random Projections (JL Lemma)** to compress the combined feature space of both Keystroke and Mouse Dynamics for lightweight processing, while simultaneously preserving privacy using **Homomorphic Encryption**. Unlike Kim et al. (2025), which applies Deep SVDD to unencrypted mobile data, this study aims to bridge the gap by creating a fast, *cryptographically secure*, multimodal authentication system for desktop environments.

2.4 Assumptions and Constraints

2.4.1 Assumptions

- It is assumed that the user's typing behavior is relatively stable over short periods but may exhibit gradual "concept drift" which the model must accommodate.
- It is assumed that the users are utilizing standard physical keyboards; virtual/touchscreen keyboards are outside the scope of this specific study (unless specified otherwise).
- It is assumed that the mouse data collection frequency (e.g., 50Hz) is sufficient to capture micro-movements without overwhelming the system bus.

- The ”trust” of the endpoint device (personal laptop) is assumed for the initial data capture phase before encryption.

2.4.2 Constraints

- **Hardware Limitations:** The proposed model must be lightweight enough to run on standard consumer hardware (e.g., a laptop with a mid-range GPU like an RTX 3050) without causing noticeable input lag.
- **Data Availability:** The research is constrained by the need to collect a custom dataset or use public datasets that may not perfectly reflect the specific ”free-text” behavior required for continuous authentication.
- **Encryption Overhead:** Homomorphic Encryption introduces significant computational overhead. The system is constrained to optimize this trade-off to ensure the authentication decision happens within a usable timeframe (e.g., under 200ms per window).

3.0 Methodology and Project Design

Rationale for Chosen Methods:

- **Multimodal Fusion:** Single-modality systems (keystroke only) are prone to mimicry attacks. Fusion with mouse dynamics increases the entropy of the user profile, making forgery exponentially harder.
- **Deep SVDD & LSTMs:** Unlike static classifiers (e.g., SVM), Long Short-Term Memory (LSTM) networks are selected for their ability to model the temporal dependencies in sequential data. Deep Support Vector Data Description (Deep SVDD) is chosen as the anomaly detector because it is a "one-class" classifier, meaning it can train on only the legitimate user's data without requiring impostor data during the training phase.
- **Johnson-Lindenstrauss (JL) Lemma:** To counter the computational overhead of Homomorphic Encryption, the JL Lemma is applied to project high-dimensional biometric feature vectors into a lower-dimensional space. This allows for faster encrypted computations with mathematically guaranteed distance preservation.

3.1 Overview of the Proposed Methodology/Research Design

1. **Feature Extraction & Temporal Fusion:** The system ingests raw event logs and converts them into synchronized time-series feature vectors.
    - **Keystroke Features:** Extraction of Flight Time (latency between KeyUP$n \rightarrow$ KeyDOWN$n+1$) and *Dwell Time* (duration of KeyDOWNn $\rightarrow$ KeyUPn).
    - **Mouse Features:** Calculation of higher-order motor metrics including Velocity Profiles, Angular Velocity, and Curvature Distance Ratio (efficiency of movement).
    - **Multimodal Fusion:**The two independent streams are aligned using sliding time windows (e.g., $t = 10s$) to create unified "behavioral frames" representing the user's complete interaction state.
2. **Dimensionality Reduction (JL Layer):** To mitigate the "curse of dimensionality" caused by fusing two biometric streams, the high-dimensional fused vector (d) is projected onto a lower-dimensional subspace (k, where $k \ll d$) using the Johnson-Lindenstrauss (JL) Lemma. This is achieved by

multiplying the feature vector by a sparse random matrix (R) to produce a compressed, privacy-hardened embedding.

3. **Privacy-Preserving Transformation:** The compressed embeddings are encrypted using a **Leveled Homomorphic Encryption (LHE)** scheme (e.g., CKKS). Unlike additive-only schemes (such as Paillier), CKKS supports the approximate arithmetic and multiplication depth required to compute *squared Euclidean distances* ($||x - c||^2$) directly on the ciphertext. This ensures that the mathematical operations needed for authentication are performed entirely in the encrypted domain without decrypting the user's behavioral template.

4. **Anomaly Detection (Deep SVDD):** The encrypted feature vectors are fed into a Deep Support Vector Data Description (Deep SVDD) model. This model learns a compact hypersphere boundary encapsulating the legitimate user's "normal" behavior. During the verification phase, the system calculates the distance between the encrypted input and the hypersphere center; any input falling outside this learned radius is flagged as an anomaly (potential impostor) while the data remains mathematically indistinguishable from random noise.

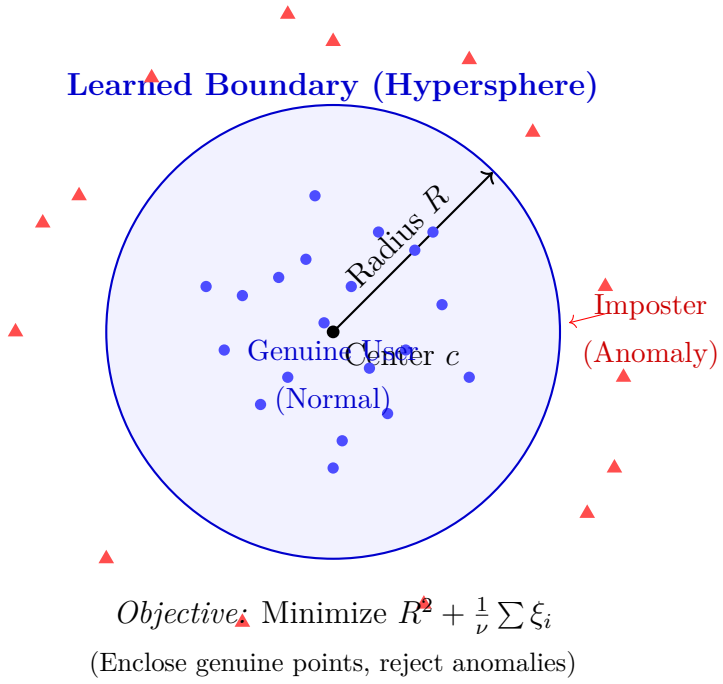

Figure 3: Visualizing the Deep SVDD Decision Boundary. The model learns a compact hypersphere of radius R around center c that encapsulates the majority of legitimate user data (blue dots). Any input falling outside this boundary is flagged as an anomaly (red triangles), representing a potential impostor.

3.1.1 Architectural Design Mode I: Cryptographic Privacy (High-Security)

Illustrated in Figure 1. This mode is designed for high-risk transaction scenarios, such as banking login or authorizing payments. It utilizes **Leveled Homomorphic Encryption (CKKS)** to perform anomaly detection inference entirely within the encrypted domain.

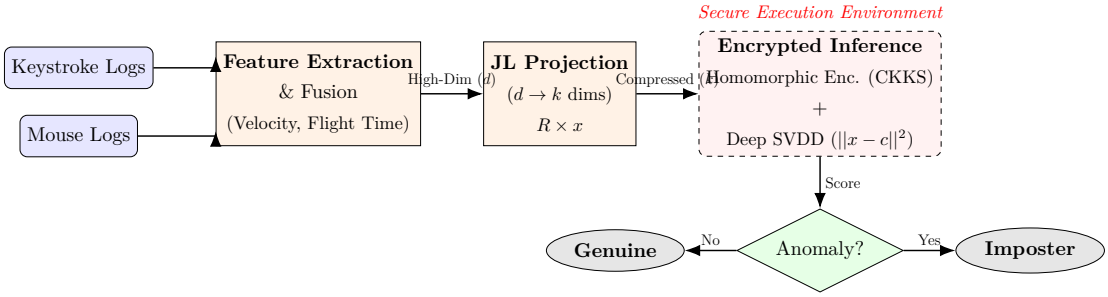

Figure 4: System Architecture of the Proposed Lightweight Privacy-Preserving Framework.

- **Privacy Mechanism:** The behavioral template is encrypted using standard cryptographic protocols, ensuring mathematically provable security (IND-CPA).
- **Trade-off:** While this offers the highest level of data protection, it incurs a higher computational cost, making it suitable for periodic, critical authentication rather than continuous, sub-second monitoring.

3.1.2 Architectural Design Mode II: Projected Privacy (High-Performance)

Illustrated in Figure 2. This mode is designed for continuous, passive background monitoring. It removes the heavy encryption overhead and relies on the **Johnson-Lindenstrauss (JL) Projection** as a form of non-invertible compression.

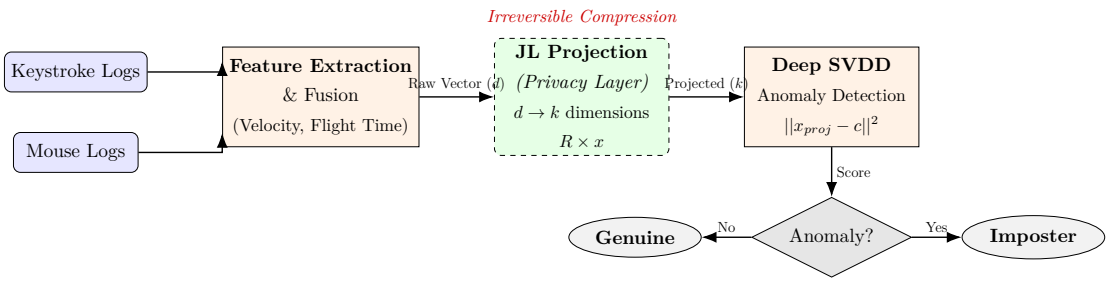

Figure 5: Proposed Lightweight Architecture: Using JL Projections as a Privacy-Preserving Transformation.

- **Privacy Mechanism:** The JL projection acts as a "computational privacy" layer. By projecting data from a high-dimensional space (d) to a significantly lower-dimensional space (k, where $k \ll d$), the original features become mathematically indeterminate and resistant to reconstruction attacks.
- **Trade-off:** This mode achieves ultra-low latency (< 200ms), enabling the system to authenticate the user continuously without draining battery life or causing input lag, while still maintaining a robust defense against feature recovery.

3.2 Data Collection

To ensure the proposed privacy-preserving framework is robust, scalable, and generalizes well to real-world scenarios, this research utilizes a **Hybrid Multi-Source Dataset** approach. Data is aggregated from five distinct, high-impact repositories, covering both fixed-text and free-text typing scenarios, as well as multimodal (Keystroke + Mouse) interactions.

3.2.1 Primary Datasets (Multimodal & Cross-Device)

The core training and fusion phases utilize two datasets that offer high-granularity sensor data.

- **SU-AIS BB-MAS (Behavioral Biometrics Multi-device and multi-Activity from Same users):** This dataset serves as the primary source for training the Deep SVDD model due to its user volume and cross-device consistency.
  - **Source:** Syracuse University & Assured Information Security.
  - **Population:** $N = 117$ unique subjects.
  - **Volume:** Approximately 11,760 keystrokes per user (Desktop subset).
  - **Relevance:** It allows for the analysis of behavioral stability across different physical interfaces.
- **Edge Hill KMT (CyberSignature Dataset):** This dataset is critical for the *Multimodal Fusion* layer, as it captures simultaneous mouse and keyboard interactions.
  - **Source:** Edge Hill University, UK.
  - **Scenario:** Financial form filling (names, addresses, credit card details), representing a high-security context.

  - **Population:** 88 user sessions with 1,760 interaction instances.
  - **Features:** Captures Keystroke, Mouse (trajectory, velocity, click), and Touchscreen events.

3.2.2 Benchmark Datasets (Scalability & Standardization)

To validate the model against state-of-the-art standards and ensure scalability, two benchmark datasets are employed.

- **Aalto University "136M Keystrokes" Dataset:** Used for *Transfer Learning* to pre-train the LSTM feature extractors on general typing patterns.
  - **Scale:** The largest available public keystroke dataset (> 136 million keystrokes).
  - **Population:** over 168,000 participants.
  - **Type:** Free-text typing collected via an online web test.
- **CMU Keystroke Dynamics Benchmark:** Used as a baseline control group to compare Error Rates (EER) against existing literature.
  - **Source:** Carnegie Mellon University Biometrics Research.
  - **Population:** 51 subjects.
  - **Type:** Fixed-text password entry (e.g., string ".tie5Roanl").

3.2.3 Supplementary Data

- **Feature Engineered Mouse Data (Figshare ID: 29386898):** A pre-processed dataset containing engineered features such as trajectory straightness, jitter, and movement efficiency. This is utilized to fine-tune the mouse dynamics anomaly detection module without requiring raw signal processing.

Table 2: Summary of Experimental Datasets

Dataset	**Modality**	**Users**	**Primary Role**
Edge Hill KMT	Key + Mouse	88	Multimodal Fusion Training
SU-AIS BB-MAS	Key + Sensors	117	Deep Learning (LSTM) Training
Aalto 136M	Keystroke	168k+	Scalability & Transfer Learning
CMU Benchmark	Keystroke	51	Baseline Validation
Figshare Mouse	Mouse	N/A	Feature Engineering

3.3 Ethical Considerations

This research utilizes **secondary data** obtained from open-access academic repositories and public benchmarks (SU-AIS BB-MAS, Edge Hill KMT, and Aalto University). As such, this study does not involve direct interaction with human participants, and no new personal data collection is performed.

Data Privacy and Anonymity: The datasets used in this study have been previously de-identified by the original data custodians. All records are referenced by unique alphanumeric identifiers (e.g., `User_001`), ensuring that no **Personally Identifiable Information (PII)**—such as names, addresses, or actual passwords—is processed or accessible.

- In the **Edge Hill KMT dataset**, the original collection protocol ensured that users entered *fictitious* financial information; thus, no real sensitive financial data is exposed.
- In the **SU-AIS BB-MAS dataset**, demographic attributes (age, gender) are provided in an anonymized format that prevents the re-identification of specific individuals.

Compliance and Licensing: All data is used in strict accordance with their respective licensing agreements (e.g., Creative Commons Attribution 4.0 International). The data is utilized solely for the purpose of academic research to train and validate the proposed privacy-preserving authentication model. No attempt will be made to deanonymize the data subjects.

3.4 Evaluation and Validation

The performance of the proposed privacy-preserving authentication framework will be rigorously evaluated using a comprehensive suite of biometric and system performance metrics. The evaluation strategy is designed to quantify the trade-offs between authentication accuracy, computational latency, and privacy overhead.

3.4.1 Experimental Design

The validation process will follow a k**-fold Cross-Validation** ($k = 10$) protocol to ensure statistical reliability. The dataset will be partitioned into:

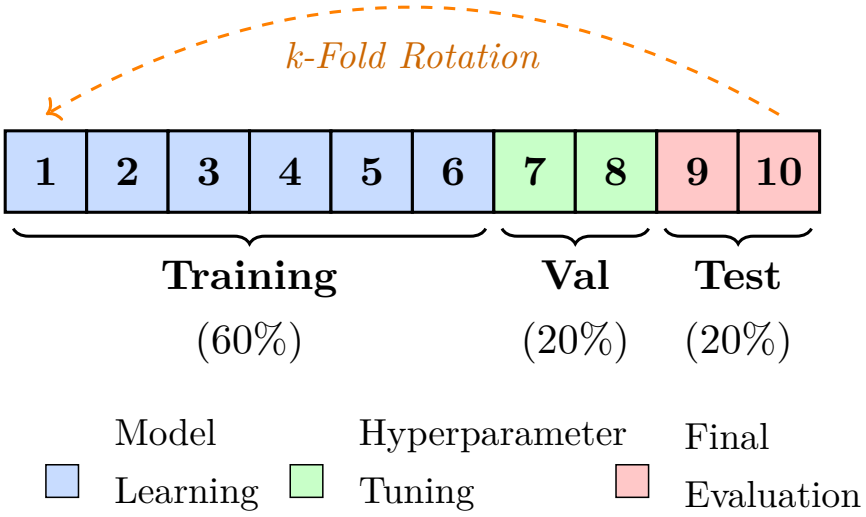

Figure 6: Experimental Data Partitioning Strategy. The dataset is divided into 10 folds with a 60/20/20 split for Training, Validation, and Testing. Assignments rotate cyclically.

- **Training Set (60%):** Used to train the Deep SVDD model to learn the user's normal behavioral boundary.
- **Validation Set (20%):** Used for hyperparameter tuning (e.g., LSTM layer size, JL projection dimension k).
- **Testing Set (20%):** Used to evaluate the final performance on unseen data.

To simulate real-world attacks, **Zero-Effort Impostor** testing will be conducted, where every other user in the dataset acts as an impostor against the target user.

3.4.2 Biometric Performance Metrics

The primary measure of authentication success is the system's ability to correctly distinguish the legitimate user from impostors.

- **False Acceptance Rate (FAR):** The probability that an unauthorized user (impostor) is incorrectly accepted by the system.

$$FAR = \frac{FP}{FP + TN} \times 100 \tag{1}$$

Where FP is False Positives and TN is True Negatives.

- **False Rejection Rate (FRR):** The probability that the legitimate user is incorrectly rejected by the system.

$$FRR = \frac{FN}{FN + TP} \times 100 \tag{2}$$

Where FN is False Negatives and TP is True Positives.

- **Equal Error Rate (EER):** The operating point where $FAR = FRR$. A lower EER indicates a more accurate system.

$$EER = \{FAR \mid FAR = FRR\} \tag{3}$$

3.4.3 System Efficiency & Scalability Metrics

To validate the effectiveness of the **Johnson-Lindenstrauss (JL) Lemma** and **Homomorphic Encryption**, the following computational metrics will be recorded:

- **Inference Latency (L_{inf}):** The time taken to process a single authentication request.

$$L_{inf} = T_{proj} + T_{enc} + T_{score} \tag{4}$$

Target: $L_{inf} < 200ms$ (Real-time threshold).

- **Encryption Overhead Ratio (E_{ratio}):** The ratio of processing time in the encrypted domain versus the plaintext domain.

$$E_{ratio} = \frac{T_{encrypted}}{T_{plaintext}} \tag{5}$$

3.4.4 Privacy and Security Evaluation

Given the cybersecurity focus of this research, quantifying the strength of the privacy-preserving mechanisms is critical.

- **Indistinguishability (Adversarial Advantage):** To verify semantic security (IND-CPA), we measure the probability that an adversary $\mathcal{A}$ can distinguish between two encrypted biometric templates.

$$Adv_{\mathcal{A}} = |\Pr[\mathcal{A}(E(m_0)) = 1] - \Pr[\mathcal{A}(E(m_1)) = 1]| \tag{6}$$

- **Reconstruction Resistance (Feature Recovery Attack):** To simulate a database breach, an inverse-mapping Deep Neural Network (Decoder $\mathcal{D}$) will be trained to attempt to reconstruct the original raw features X from

the stored templates T. Privacy is quantified by the maximization of the Reconstruction Error (MSE):

$$MSE_{recon} = \frac{1}{N}\sum_{i=1}^{N}(X_i - \mathcal{D}(T_i))^2 \tag{7}$$

- **Information Leakage (Mutual Information):** We quantify the dependency between the raw biometric vector X and the projected/encrypted vector Z using Shannon's Mutual Information:

$$I(X;Z) = \sum_{x\in X}\sum_{z\in Z} p(x,z)\log\left(\frac{p(x,z)}{p(x)p(z)}\right) \tag{8}$$

4.0 ANTICIPATED RESULTS/FINAL PRODUCTS

4.1 Expected Outcomes

Based on the proposed methodology involving Orthogonal Random Projections and Deep SVDD, the study anticipates the following specific experimental results:

- **Privacy-Utility Trade-off Optimization:** The research expects to demonstrate that projecting high-dimensional multimodal features into a lower-dimensional subspace (via the Johnson-Lindenstrauss Lemma) will result in a **negligible degradation of authentication accuracy**. Specifically, we anticipate the system will maintain an Equal Error Rate (EER) comparable to non-private baselines (targeting an EER deviation of $< \pm 1.5\%$) while significantly reducing the computational complexity required for Homomorphic Encryption.

- **Real-Time Inference Latency:** By compressing the feature vector size ($k \ll d$) before encryption, the system is expected to achieve an inference latency of $< 200ms$ per authentication window. This result would validate the hypothesis that "lightweight" privacy-preserving authentication is feasible on mid-range consumer hardware (e.g., laptops with standard GPUs) without inducing noticeable input lag.

- **Robustness Against Feature Recovery:** In terms of privacy metrics, the model is expected to maximize the **Reconstruction Error (MSE)**. The study anticipates that an adversarial neural network (Inverse Decoder) will fail to reconstruct the original raw keystroke or mouse trajectories from the stored projected templates, effectively rendering the biometric data mathematically irreversible.

- **Multimodal Superiority:** The results are expected to confirm that fusing Mouse Dynamics with Keystroke Dynamics yields a statistically significant reduction in False Acceptance Rate (FAR) compared to unimodal (keystroke-only) baselines, particularly in "Zero-Effort Impostor" scenarios.

4.2 Scientific Contribution and Contribution to Knowledge

This research intends to fill the critical gap between **recognition accuracy** and **data privacy** identified in the literature review. The specific contributions to the body of knowledge include:

- **Novel Application of JL Lemma in Behavioral Biometrics:** While the Johnson-Lindenstrauss (JL) Lemma is used in other domains, this study contributes a novel application of **Orthogonal Random Projections specifically for fusing and compressing multimodal behavioral streams** (Keystroke + Mouse). This provides a theoretical framework for handling the "Curse of Dimensionality" in continuous authentication without discarding valuable behavioral entropy.
- **Validation of Deep SVDD in Encrypted Domains:** Existing studies have validated Deep SVDD for unencrypted mobile PINs. This research will contribute the first empirical validation of **Deep Support Vector Data Description (Deep SVDD) applied to encrypted, dimensionality-reduced vectors**, proving that one-class anomaly detection boundaries can be learned effectively even in a projected, privacy-preserving subspace.
- **A Unified Lightweight Framework:** The study contributes a unified architectural blueprint that integrates **Signal Processing (Feature Engineering)**, **Cryptography (Homomorphic Encryption)**, and **Deep Learning (Deep SVDD)**. This contrasts with existing siloed approaches that focus either solely on accuracy (ignoring privacy) or solely on encryption (ignoring latency).

4.3 Potential Impact and Significance

The findings of this research have significant implications for both the academic community and the cybersecurity industry:

- **Elimination of "Honey Pot" Databases:** By proving that authentication can occur without storing raw behavioral features, this research offers a pathway to eliminate centralized databases of sensitive biometric data. If the

database is compromised, the attacker retrieves only projected, encrypted templates that cannot be reverse-engineered to mimic the user, significantly reducing the risk of permanent identity theft.

- **Enabling Continuous Authentication on Edge Devices:** Successfully lowering the latency to under 200ms implies that continuous, passive authentication can be deployed on resource-constrained edge devices (smartphones, IoT) rather than relying on cloud-based processing. This enhances user privacy by keeping data processing local to the device.
- **Standardization of Privacy Metrics:** By rigorously evaluating **Mutual Information** and **Adversarial Advantage**, this project establishes a benchmark for how future behavioral biometric systems should be audited for privacy, moving the industry standard beyond simple "accuracy" (EER) toward "privacy-preserved accuracy."

4.4 Project Deliverables

To demonstrate the validity of the proposed framework, the project will deliver:

1. **Software Prototype:** A Python-based implementation of the pipeline (Feature Extraction $\rightarrow$ JL Projection $\rightarrow$ Encryption $\rightarrow$ Deep SVDD) capable of processing real-time input streams.
2. **Multimodal Dataset Repository:** A curated and pre-processed subset of the merged datasets (SU-AIS BB-MAS and Edge Hill KMT) formatted for reproducibility.
3. **Final Thesis:** A comprehensive document detailing the mathematical proofs, architectural design, and experimental validation of the framework.
4. **Research Paper:** A manuscript targeting an IEEE/ACM conference summarizing the trade-off analysis between privacy and latency.

5.0 Project Schedule

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, M. Islam, 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.

[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)*, 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*, American Mathematical Society, 1984, pp. 189–206.

[8] L. Ruff et al., "Deep one-class classification," in *International conference on machine learning*, PMLR, 2018, pp. 4393–4402.

Appendices

Appendix A: Survey Form

Appendix B: Code Snippets