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

BB-MAS	Behavioral Biometrics Multi-device and multi-Activity from Same users
CMU	Carnegie Mellon University
Deep SVDD	Deep Support Vector Data Description
EER	Equal Error Rate
HE	Homomorphic Encryption
JL	Johnson-Lindenstrauss
LSTM	Long Short-Term Memory
PIN	Personal Identification Number
RNN	Recurrent Neural Network
SU-AIS	Syracuse University and Assured Information Security
SVDD	Support Vector Data Description

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 [1], [2] and Mouse Dynamics [3], 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 [4], [5].

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 [6]. 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 [7].

The state-of-the-art solutions to this privacy issue involve the use of heavy cryptographic techniques, including Homomorphic Encryption (HE) [8], 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 [9]. 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 [10]. 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 [11]. In order to fill this gap, this study suggests a brand-new, lightweight framework that combines Deep Support Vector Data Description (Deep SVDD) [12] with Keyed

Johnson-Lindenstrauss (JL) Projections [13]. 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:

- **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, achieve high recognition accuracy but typically necessitate the storage of raw or minimally transformed behavioral features. This creates a vulnerability where templates are susceptible to reverse-engineering or replay attacks.
- **Efficiency Gaps in Cryptographic Methods:** Strong cryptographic solutions, such as Homomorphic Encryption (HE), allow for secure computation on encrypted data. However, these schemes introduce prohibitive computational overhead and latencies that often render them impractical for real-time monitoring on resource-constrained edge devices.
- **Lack of Integrated Revocability:** Most existing frameworks focus on verification accuracy but lack a mechanism for "cancelable" biometrics. If a template is stolen, there is currently no unified lightweight implementation that allows a user to "reset" their biometric identity without an entirely new enrollment or a total loss of privacy.

There is currently no unified framework that effectively balances these conflicting requirements. This research seeks to bridge this gap by proposing an architecture

that utilizes Keyed Johnson-Lindenstrauss (JL) Projections for lightweight, non-invertible feature transformation and Deep Support Vector Data Description (Deep SVDD) for efficient server-side anomaly detection. This approach ensures mathematical irreversibility and template revocability while maintaining the sub-second latency required for continuous authentication.

1.2 Research Aim and Objectives

The primary aim of this research is to develop a lightweight, privacy-preserving framework for continuous behavioral authentication that effectively balances recognition accuracy, system latency, and template revocability. This framework utilizes Keyed Johnson-Lindenstrauss (JL) Projections to ensure the mathematical irreversibility of biometric templates while employing Deep Support Vector Data Description (Deep SVDD) for efficient, one-class anomaly detection in desktop environments.

To achieve this aim, the following specific objectives have been identified:

1. **To design a privacy-preserving feature transformation pipeline:** Develop a mechanism using Keyed-JL Projections that transforms high-dimensional multimodal features (keystroke and mouse) into a lower-dimensional subspace, ensuring templates are mathematically irreversible and revocable through key renewal.

2. **To implement a multimodal behavioral fusion layer:** Integrate independent streams of keystroke dynamics, such as dwell and flight times, and mouse dynamics, including velocity and curvature, into synchronized behavioral frames to increase the entropy of the user profile.

3. **To develop a lightweight server-side anomaly detection model:** Implement a Deep SVDD classifier capable of distinguishing between legitimate users and impostors by learning a compact hypersphere boundary around the projected privacy-preserving embeddings.

4. **To evaluate the trade-off between privacy, accuracy, and latency:** Quantify the impact of projection dimension k on authentication performance (Equal Error Rate), system latency (targeting < 200ms), and resistance to feature recovery attacks.

1.3 Research Questions

To address the identified problem and achieve the research objectives, the following research questions have been formulated. These questions guide the investigation into the viability and performance of the proposed privacy-preserving behavioral authentication framework:

- **RQ1:** To what extent can Keyed-JL Projections preserve the uniqueness of multimodal behavioral biometrics while ensuring the mathematical irreversibility of the stored templates?
- **RQ2:** What is the optimal projection dimension k that minimizes the Equal Error Rate (EER) of the Deep SVDD model without exceeding the computational latency constraints of real-time monitoring?
- **RQ3:** How effectively does the fusion of keystroke and mouse dynamics mitigate the accuracy degradation typically associated with privacy-preserving feature transformations?
- **RQ4:** How resilient is the Keyed-JL transformed template against feature recovery and replay attacks compared to traditional deep learning-based authentication models?

2.0 Background

2.1 Theoretical and Technical Background

The proposed research integrates concepts from high-dimensional geometry, privacy-preserving machine learning, and multimodal behavioral biometrics. This section outlines the mathematical and architectural foundations required to understand the Keyed-JL and Deep SVDD framework.

2.1.1 The Johnson-Lindenstrauss (JL) Lemma

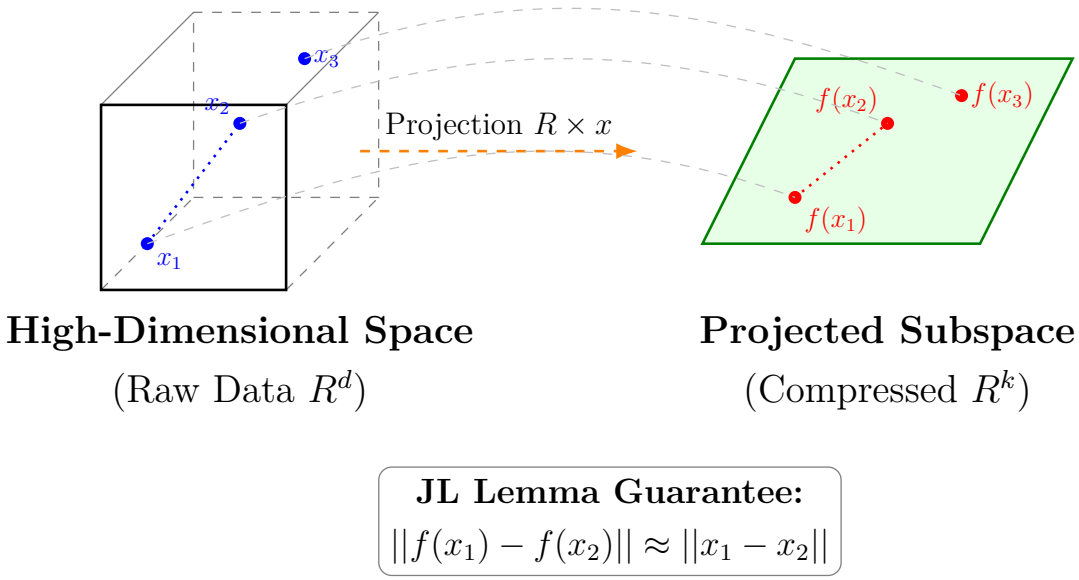

Figure 1: Conceptual Visualization of the JL Lemma [13]. Points from a high-dimensional feature space (Left) are projected onto a lower-dimensional subspace (Right). The blue and red dotted lines illustrate that the relative Euclidean distances between points are approximately preserved despite the massive reduction in dimensions.

The foundational principle for the privacy-preserving component of this research is the Johnson-Lindenstrauss Lemma. The lemma states that a set of n points in a high-dimensional space can be projected into a lower-dimensional space of dimension k while nearly preserving the pairwise distances between all points.

For any $0 < \epsilon < 1$, there exists a linear mapping $f : \mathbb{R}^d \to \mathbb{R}^k$ such that for all $u, v \in X$:

$$(1 - \epsilon)\|u - v\|^2 \leq \|f(u) - f(v)\|^2 \leq (1 + \epsilon)\|u - v\|^2 \tag{1}$$

Where ϵ represents the error tolerance and f is the projection mapping.

In this research, the projection matrix is generated using a secret key, ensuring that the transformation is non-invertible and providing revocability.

2.1.2 Deep Support Vector Data Description (Deep SVDD)

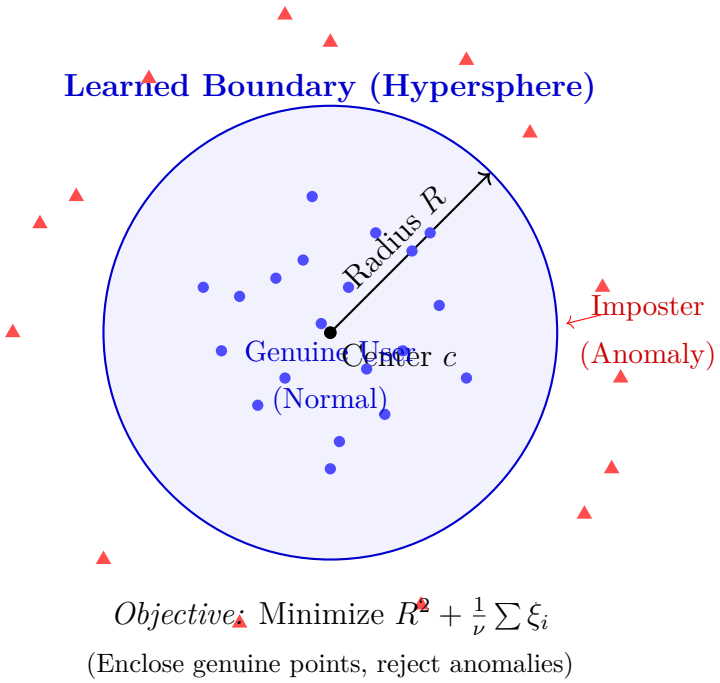

Figure 2: Visualizing the Deep SVDD Decision Boundary. The model learns a compact hypersphere of radius R around center c that encapsulates the majority of legitimate user data (blue dots). Any input falling outside this boundary is flagged as an anomaly (red triangles), representing a potential impostor.

The authentication engine utilizes Deep SVDD, an unsupervised method for one-class classification. It maps legitimate user features into a minimum-volume hypersphere in a latent space.

The objective function minimizes the distance of the network outputs to the center c of the hypersphere:

$$\min_{\mathcal{W}} \sum_{i=1}^{n} \|\phi(x_i; \mathcal{W}) - c\|^2 + \lambda \|\mathcal{W}\|_F^2 \tag{2}$$

Where $\phi(x_i; \mathcal{W})$ is the neural network mapping, c is the hypersphere center, and $\lambda\|\mathcal{W}\|_F^2$ is the weight decay regularization term.

2.1.3 Multimodal Behavioral Fusion

The system architecture relies on the fusion of keystroke timing and mouse movement patterns. This multimodal approach increases the entropy of the biometric

profile, compensating for the information loss during privacy-preserving projection.

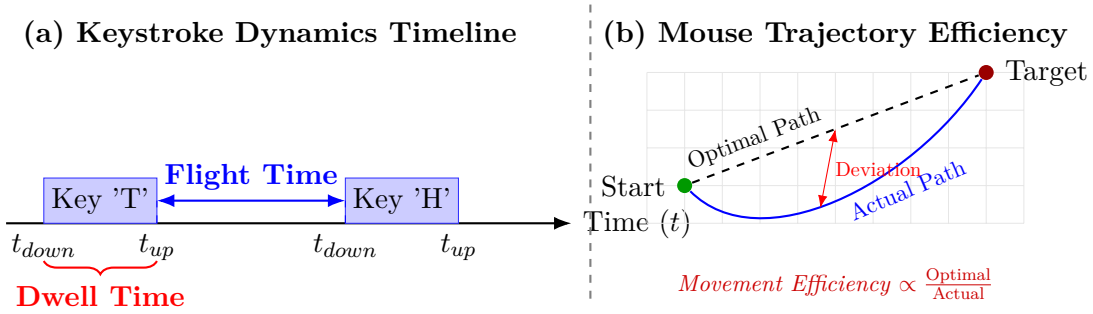

Figure 3: Visual Representation of Biometric Features. **(a)** Keystroke Dynamics: Dwell Time represents the key press duration, while Flight Time measures the latency between distinct keystrokes. **(b)** Mouse Dynamics: Comparison between the optimal straight-line path and the actual user trajectory, used to calculate movement efficiency and curvature.

2.2 Literature Review

The evolution of behavioral authentication has transitioned from simple timing analysis to complex multimodal deep learning frameworks. This section categorizes previous research into key subdomains applicable to the proposed Keyed-JL and Deep SVDD framework.

2.2.1 Foundational Keystroke Dynamics

Early research established the feasibility of using typing patterns as a biometric. Foundational studies by Gaines et al. identified that keystroke timing—specifically dwell times and flight times—is unique to individuals. While initial systems focused on static login verification [2], subsequent work by Shepherd introduced continuous authentication, allowing for persistent session monitoring. Monrose and Rubin further demonstrated the utility of these patterns in hardening traditional password-based security.

2.2.2 Multimodal Fusion and Mouse Dynamics

To improve recognition robustness, researchers integrated mouse dynamics and fusion techniques. Ahmed and Traore proved that mouse movement trajectories and click frequencies provide a distinct behavioral signature. Mondal and Bours showed that a multimodal approach, fusing keystroke and mouse data, significantly improves the Equal Error Rate (EER) over unimodal systems. Recent datasets,

Table 1: Summary of Key Related Studies

Reference & Study	**Key Contribution to This Project**	**Identified Gap / Limitation**
Gaines et al. (1980) [1] & Joyce et al. (1990) [2]	**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) [5]	**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) [7]	**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. (2024) [14]	**Deep Support Vector Data Description (Deep SVDD) Validation:** Demonstrated that Deep SVDD outperforms traditional models (6.7% EER) by encoding time-series data into images.	Restricted to *mobile Personal Identification Numbers (PINs)* (touch interactions) and lacked cryptographic encryption (Homomorphic Encryption (HE)) or multimodal fusion (Mouse).
Kiyani et al. (2020) [10]	**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.
Rahman et al. (2021) [9]	**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).

such as those by Reddy, emphasize feature-engineered mouse dynamics for anomaly detection.

2.2.3 Deep Learning and Privacy Methodologies

Modern research utilizes deep learning but highlights growing privacy concerns. High-accuracy models using Recurrent Neural Networks (RNN) and Bayesian neural networks have become standard for behavior modeling. However, as shown by Kim et al. in the KDPrint framework, encoding behavioral data into standardized images can leave templates vulnerable if not properly secured. While Homomorphic Encryption (HE) offers a mathematical solution for privacy, its latency often exceeds the requirements for continuous monitoring. This research addresses this gap by combining the privacy of Keyed-JL projections with the efficiency of Deep SVDD.

2.3 Research Gap

Despite advancements in behavioral biometrics, a critical gap exists in providing simultaneous mathematical privacy, low latency, and template revocability.

2.3.1 Technical Dichotomy: Privacy vs. Performance

A significant gap exists between high-accuracy Deep Learning models and privacy-preserving cryptographic methods. Standard models often store reversible templates, while Homomorphic Encryption introduces prohibitive latencies (often > 1.5s) that are unsuitable for continuous monitoring on edge devices.

2.3.2 Vulnerability of Static Biometric Templates

Current literature lacks a standardized mechanism for "cancelable" behavioral biometrics. Unlike traditional credentials, behavioral patterns are immutable; if a stored template is compromised, the user's digital identity is permanently at risk because existing systems do not offer a lightweight way to re-issue a new, uncorrelated behavioral profile.

2.3.3 Limitations of Unimodal Authentication

Most privacy-preserving transformations result in some degree of information loss. Existing unimodal research (keystroke only or mouse only) often fails to maintain high recognition accuracy when aggressive dimensionality reduction is applied. There is a gap in research exploring how multimodal fusion can specifically compensate for the entropy loss caused by privacy-preserving projections.

2.3.4 Gap Definition

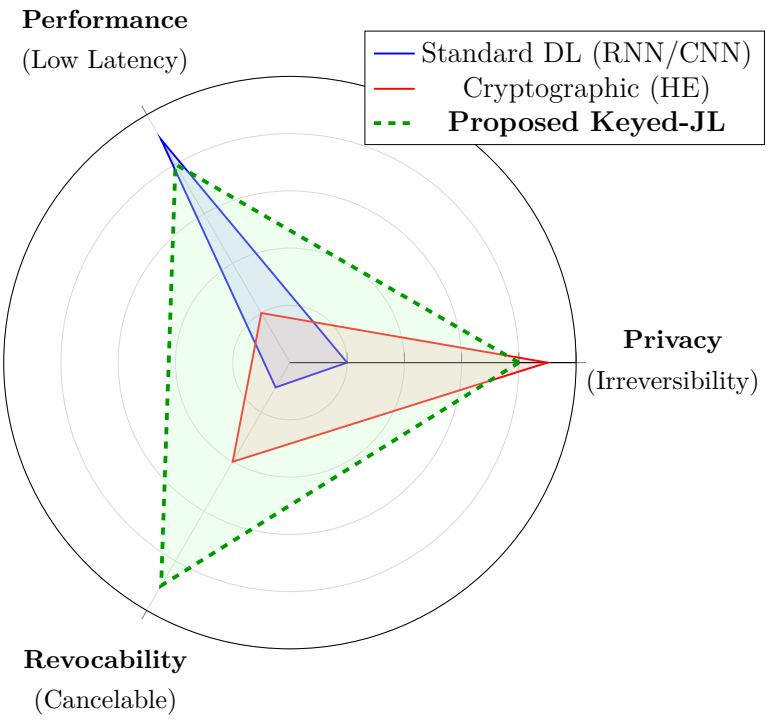

Figure 4: The Technical Dichotomy in Behavioral Authentication.

The research gap is formally defined as the lack of a unified behavioral authentication framework that provides **provable non-invertibility** without sacrificing the **sub-second latency** required for continuous monitoring. While existing studies achieve high accuracy using Deep Learning, they fail to provide a mechanism for template revocability, meaning a compromised biometric profile is permanently lost. Conversely, cryptographic methods that provide privacy are too computationally expensive for real-time use on standard hardware.

2.4 Assumptions and Constraints

This section outlines the foundational assumptions made during the research design and the technical constraints that bound the scope of the proposed privacy-preserving behavioral authentication system.

2.4.1 Assumptions

The validity of the experimental results and the effectiveness of the framework rely on several key assumptions:

- **Consistency of User Behavior:** It is assumed that the primary user's

typing and mouse usage patterns remain relatively stable over the duration of the study.

- **Integrity of Enrollment:** The research assumes the initial enrollment occurs in a secure environment, ensuring the Deep SVDD model is trained on verified legitimate data.
- **Security of the Secret Key:** The mathematical irreversibility of the JL-projection relies on the secret key being stored securely on the client side.
- **Hardware Sufficiency:** It is assumed that the target hardware can perform the linear JL-projections and inference within the required latency bounds.

2.4.2 Constraints and Limitations

The study is conducted within the following constraints:

- **Modality Limitation:** The system is restricted to desktop inputs (keyboard and mouse) and does not include mobile-specific biometrics.
- **Data Availability:** Evaluation is limited to the diversity and volume of data present in selected benchmark datasets.
- **Latency vs. Privacy Bound:** A critical constraint is the trade-off between projection dimension k and system performance, targeting a real-time latency of < 200ms.
- **Environmental Noise:** Variations in hardware peripherals may introduce noise, potentially affecting the overall Equal Error Rate (EER).

3.0 Methodology and Project Design

The proposed methodology adopts a quantitative experimental approach to evaluate the performance of privacy-preserving continuous authentication. The research design is centered on the "Privacy-by-Design" principle, ensuring that sensitive behavioral templates are never transmitted or stored in an invertible format.

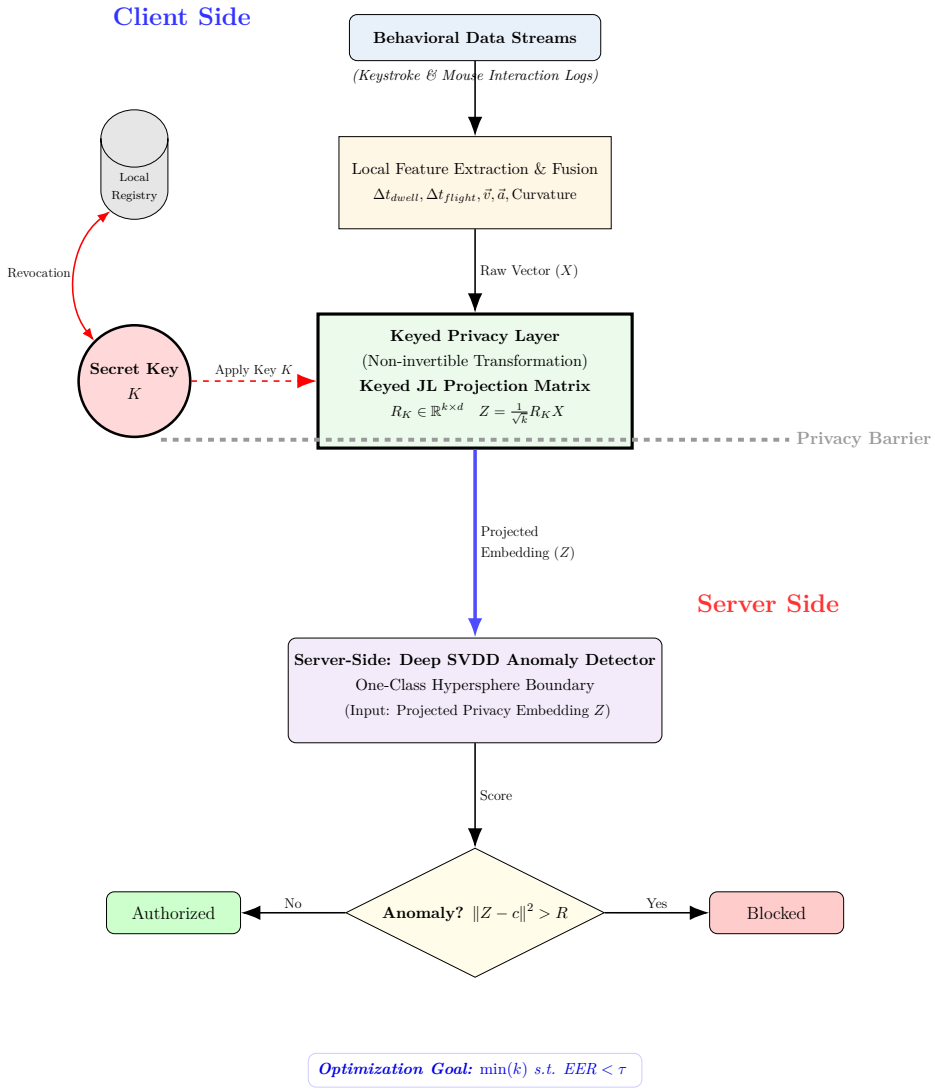

Figure 5: System Architecture: Keyed-JL Privacy and Server-Side Deep SVDD Detection

3.1 Overview of the Proposed Research Design

The system architecture is divided into two distinct environments separated by a **Privacy Barrier**: the **Client Side**, where data is captured and transformed, and the **Server Side**, where authentication decisions are made.

The methodology follows a structured pipeline: (1) **Data Acquisition** from

logs, (2) **Feature Engineering** for multimodal fusion, (3) **Keyed-JL Transformation** for privacy, and (4) **Deep SVDD Detection** for real-time authentication.

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 repositories, covering fixed-text, free-text, and multimodal (Keystroke + Mouse) interactions.

The behavioral features selected—specifically Dwell Time and Flight Time—represent high-quality biomechanical signatures. The validity of these metrics is demonstrated in Appendix B, where a baseline SVM classifier was tested on real-world behavioral data points.

3.2.1 Primary Datasets (Multimodal & Cross-Device)

The core training and fusion phases utilize datasets offering high-granularity sensor data:

- **Syracuse University and Assured Information Security (SU-AIS) Behavioral Biometrics Multi-device and multi-Activity from Same users (BB-MAS) [15]:** This serves as the primary source for training the Support Vector Data Description (SVDD) model.
  - **Population:** $N = 117$ unique subjects.
  - **Volume:** Approximately 11,760 keystrokes per user (Desktop subset).
  - **Relevance:** Facilitates analysis of behavioral stability across different physical interfaces.
- **Edge Hill KMT [16]:** Critical for the multimodal fusion layer, capturing simultaneous mouse and keyboard interactions.
  - **Scenario:** High-security financial form filling context.
  - **Population:** 88 user sessions with 1,760 interaction instances.
  - **Features:** Captures Keystroke, Mouse trajectory, velocity, and click events.

3.2.2 Benchmark Datasets (Scalability & Standardization)

Two benchmark datasets ensure scalability and baseline comparisons:

- **Aalto University "136M Keystrokes" Dataset [17]:** Used for pre-training feature extractors on general typing patterns.
  - **Scale:** Largest available public keystroke dataset ($>$ 136 million keystrokes).
  - **Population:** Over 168,000 participants.
  - **Type:** Free-text typing collected via web-based tests.
- **Carnegie Mellon University (CMU) Keystroke Dynamics Benchmark [18]:** Used as a baseline control group to compare EERs against existing literature.
  - **Population:** 51 subjects.
  - **Type:** Fixed-text password entry.

3.2.3 Supplementary Data

- **Feature Engineered Mouse Data [19]:** 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 [16]	Key + Mouse	88	Multimodal Fusion Training
SU-AIS BB-MAS [15]	Key + Sensors	117	LSTM Training
Aalto 136M [17]	Keystroke	168k+	Transfer Learning
CMU Benchmark [18]	Keystroke	51	Baseline Validation
Mouse Features [19]	Mouse	Aggregated	Feature Engineering

3.3 Ethical Considerations

In accordance with the research standards for the University of Peradeniya, this study addresses the ethical implications of using human behavioral data for biometric authentication. The research design prioritizes data privacy and the minimization of risks associated with the storage of biometric identifiers.

3.3.1 Use of Human-Generated Behavioral Data

This research utilizes secondary behavioral data consisting of keystroke and mouse interaction logs from five high-impact repositories.

- **Data Nature:** The logs represent biomechanical patterns (dwell times, flight times, and mouse trajectories) rather than sensitive content or personal information.
- **Non-intrusive Capture:** No keystroke logging of sensitive text is performed; the study focuses solely on temporal characteristics.

3.3.2 Anonymization and De-identification

The datasets employed, such as the Aalto 136M and SU-AIS BB-MAS, have been previously anonymized.

- **Participant Privacy:** Individual data points are mapped to randomized identifiers, precluding the possibility of identity reconstruction.
- **Privacy-by-Design:** The use of Keyed-JL Projections ensures that biometric templates are mathematically irreversible, providing a second layer of ethical protection against feature recovery attacks.

3.3.3 Data Storage and Integrity

During the experimental phase, data integrity is maintained through encrypted storage protocols. Only projected embeddings are transmitted for server-side processing, adhering to the principle of data minimization.

3.4 Evaluation and Validation

To rigorously assess the performance and privacy of the proposed Keyed-JL and Deep SVDD framework, a comprehensive experimental design is employed. This section outlines the quantitative metrics and validation strategies used to measure authentication accuracy and system efficiency.

3.4.1 Authentication Performance Metrics

The system's ability to distinguish between a legitimate user and an impostor is evaluated using standard biometric error rates:

- **False Acceptance Rate (FAR):** Measures the frequency with which the system incorrectly grants access to an unauthorized impostor.

$$FAR = \frac{FP}{FP + TN} \times 100\% \tag{3}$$

- **False Rejection Rate (FRR):** Measures the frequency with which the system incorrectly denies access to the legitimate user.

$$FRR = \frac{FN}{FN + TP} \times 100\% \tag{4}$$

- **Equal Error Rate (EER):** The point where $FAR = FRR$. A lower EER indicates higher system robustness.

3.4.2 Privacy and Efficiency Validation

To validate the privacy-preserving component and real-time viability, the following metrics are analyzed:

- **Template Irreversibility:** Testing the mathematical resilience of the JL-transformation against feature recovery attacks.
- **Revocability:** Ensuring that regenerating the projection matrix R_K creates uncorrelated templates for the same user, satisfying the requirement for cancelable biometrics.
- **System Latency:** Measuring the total processing time from feature extraction to server-side decision, targeting a sub-200ms threshold.

4.0 Anticipated Results/Final Products

5.0 Project Schedule

References

[1] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: Some preliminary results," *Rand Report R-256-NSF*, 1980.

[2] R. Joyce and G. Gupta, "Identity verification based on keystroke latency patterns," *Communications of the ACM*, vol. 33, no. 2, pp. 168–176, 1990.

[3] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 165–179, 2007.

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

[5] S. Mondal and P. Bours, "Continuous authentication using a combination of keystroke and mouse dynamics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2017.

[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] J. Kim et al., "User-adaptive feature extraction for keystroke dynamics-based authentication," *Computers & Security*, 2018.

[8] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," *Advances in Cryptology–ASIACRYPT 2017*, pp. 409–437, 2017.

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

[10] 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.

[11] N. Zheng, M. Palaniswami, and K. Rao, "An efficient user verification system via mouse movements," in *Proceedings of the 8th ACM journal on access control models and technologies*, 2011.

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

[13] 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.

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

[15] S. University and A. I. Security, "Behavioral biometrics multi-device and multi-activity from same users (bb-mas)," *IEEE Dataport*, 2019. DOI: 10.21227/2q3r-8m28

[16] P. Bours, "The edge hill university keystroke and mouse dynamics dataset," in *International Conference on Biometrics*, 2012.

[17] V. Dhakal, A. M. Feit, P. O. Kristensson, and A. Oulasvirta, "136 million keystrokes: A large-scale dataset for keystroke dynamics," *Scientific Data*, vol. 5, 2018.

[18] K. S. Killourhy and R. A. Maxion, *Keystroke dynamics benchmark dataset*, Carnegie Mellon University, 2009.

[19] D. Reddy, *Feature-engineered mouse dynamics dataset for anomaly detection*, Figshare, 2025. DOI: 10.6084/m9.figshare.29386898

A Appendices