National College of Ireland

ESN-SVM Hybrid Architecture for Free-Text Keystroke Authentication

MSc Research Project
Cyber Security

Nishant Premnath Chavan
Student ID: 23277548

School of Computing
National College of Ireland

Supervisor: Liam Mccabe

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Nishant Premnath Chavan
Student ID:	23277548
Programme:	MSc Cyber Security **Year:** 2025
Module:	Practicum 2
Supervisor:	Liam Mccabe
Submission Due Date:	15/09/2025
Project Title:	ESN-SVM Hybrid Architecture for Free-Text Keystroke Authentication
Word Count:	5640 **Page Count** 26

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Nishant Premnath Chavan
Date:	12/09/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

List of Figures

List of Tables

List of Equations

List of Acronyms

Acronym	Definition
AUC	Area Under the Curve
CMU	Carnegie Mellon University
CNN	Convolutional Neural Network
DD	Down-Down (keystroke timing)
DU	Down-Up (keystroke timing)
EER	Equal Error Rate
ESN	Echo State Networks
ESP	Echo State Property
FMR	False Match Rate
FNMR	False Non-Match Rate
GRU	Gated Recurrent Unit
GUI	Graphical User Interface
ITAD	Instance-based Keystroke Dynamics
KD	Keystroke Dynamics
LSTM	Long Short-Term Memory
PCA	Principal Component Analysis
PBKDF2	Password-Based Key Derivation Function 2
PyQt6	Python GUI Framework
RBF	Radial Basis Function
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic
SVM	Support Vector Machine
UD	Up-Down (keystroke timing)
UU	Up-Up (keystroke timing)
XGBoost	Extreme Gradient Boosting

ESN-SVM Hybrid Architecture for Free-Text Keystroke Authentication

Nishant Premnath Chavan
23277548

Abstract

Keystroke Dynamics (KD) is a behavioural biometric method that identifies a user based on their typing pattern for authentication, providing non-intrusive and continuous authentication. In keystroke dynamics, each keystroke generates timing patterns that are important to identify a user, but current methods depend heavily on manually engineered features rather than core temporal features. Echo State Networks (ESNs) have temporal memory capabilities that can preserve natural user typing patterns without altering them. This study proposes a hybrid architecture consisting of ESNs for temporal pattern recognition in combination with Support Vector Machine (SVM) to make strong decision boundaries. This hybrid method addresses the main weaknesses of existing approaches which require large training datasets or struggle with different typing patterns. The results show that ESN, when combined with SVM, achieves excellent performance with an Equal Error Rate (EER) of 2.63%, which surpasses the 5% research hypothesis threshold, while outperforming ESN baseline authentication by 82.7%. The system also achieves a false non match rate (FNMR) of 1.32% and a false match rate (FMR) of 2.63%, based on simulation, thus making it ready for practical implementation.

Keywords: Keystroke Dynamics, Echo State Network, Support Vector Machine, Biometric Authentication

1 Introduction

Biometric security is needed because passwords can fail to protect systems as they are prone to phishing and brute force attacks. Among behavioural biometrics, Keystroke Dynamics (KD) has gained popularity because it uses your existing keyboard/keypad. KD recognizes users typing pattern and not their password which makes it a popular choice for continuous authentication. The verification of a user depends on their typing pattern which can reveal unique temporal characteristics of keyboard interactions which produce unique biometric signatures that are resistant to replication or forgery (Altwaijry, 2023). The importance of KD research has grown stronger because cyber threats are growing, while traditional authentication methods show increasing vulnerability to advanced attacks. The defence capabilities of behavioural biometrics especially keystroke analysis have gained recognition as a strong protection against identity theft and unauthorized access attempts. The current implementations of KD systems show promising results because recent studies have achieved Equal Error Rates (EER) below 5% in controlled environments. The transition from fixed-text to free-text authentication faces difficulties because users exhibit greater typing variability when typing variable text instead of retyping predetermined phrases.

1.1 Research Question and Objectives

The research question posed in this research investigates:

- ***To what extent does an Echo State Network (ESN) and Support Vector Machine (SVM) hybrid model improve user authentication accuracy when analysing free-text for keystroke dynamics?***

Objectives:

1. Identify limitations in current free-text keystroke dynamics authentication methods, and to what extent hybrid method can be beneficial when using basic temporal features.
2. Design and optimize ESN and SVM hybrid architecture such that temporal patterns in keystroke sequences can be well captured while still maintaining classification robustness.
3. Achieve EER of < 5% on free-text keystroke KeyRecs dataset.
4. Evaluate computational efficiency, security robustness, and real-world application by simulation with multi-layer defence methods.

The methodology allows ESN to use its capacity for temporal pattern recognition and deliver input to SVM for final high-quality classification so that free-text keystroke sequences can be processed robustly. This process lifts significant limitations where current systems either need huge volumes of training data or perform poorly with varying typing patterns. The study is an end-to-end implementation of authentication comprising preprocessing, feature extraction, model training, and security evaluation using real world data. The contribution is a validated hybrid model which demonstrates better accuracy in using keystroke dynamics on free-text, within a strong framework, while proving improved authentication accuracy. This work combines reservoir computing with traditional machine learning which provides practical improvements in authentication while at the same time creating new insights into temporal pattern recognition.

1.2 Research Paper Structure

The remainder of this report is structured as follows:

- Section 2: Presents a comprehensive literature review examining current keystroke dynamics research and its limitations.
- Section 3: Details the methodology including data cleaning, preprocessing, feature extraction, and model development.
- Section 4: Details the design specifications for ESN and SVM hybrid architecture.
- Section 5: Describes the implementation of ESN and SVM hybrid architecture and authentication system.
- Section 6: Provides a thorough evaluation of results including performance metrics, comparative analysis, and security assessment.
- Section 7: Concludes with discussion of findings, limitations, and conclusion for future research in free-text keystroke authentication systems.

2 Literature Review

Keystroke Dynamics (KD) can improve cybersecurity systems through behaviour-based authentication, also this field has experienced good improvement over the past years because of the weakness in traditional passwords and authentication systems. Hybrid machine learning model shows effectiveness in keystroke dynamics through their performance when compared to single algorithms. KD authentication depends on analysing sequential timing patterns of keystrokes which is shown in Fig. 1. The core temporal features consisting of DU.key1.key1 (Down-Up), DD.key1.key2 (Down-Down), DU.key1.key2 (Down-Up), UD.key1.key2 (Up-Down) and UU.key1.key2 (Up-Up) represent both the length of individual key hold durations and the inter-key timing interval. These combinations produce specific user behaviour patterns which differentiate between users through their typing rhythms and patterns.

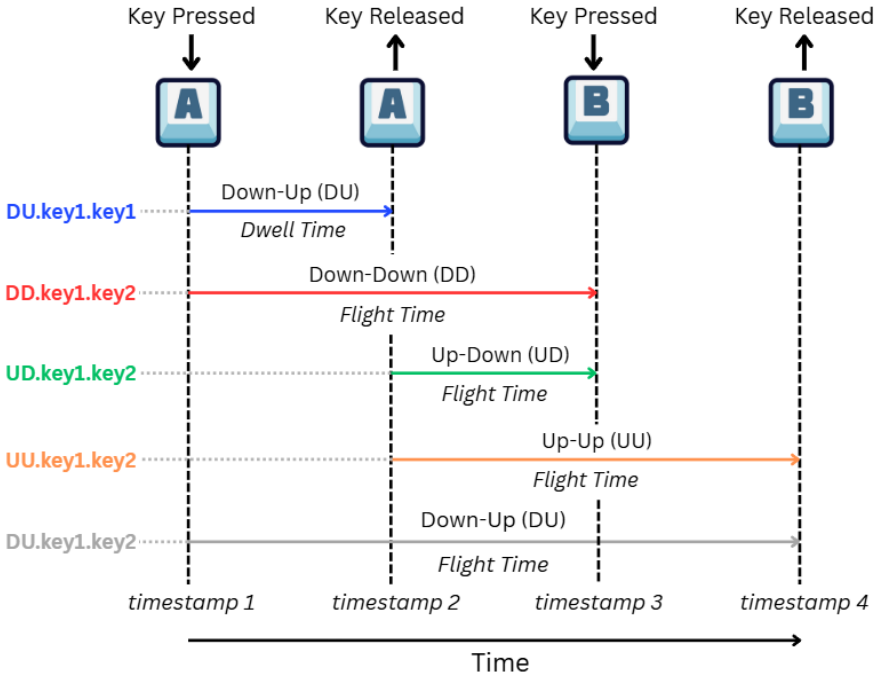


Fig. 1. Five Core Keystroke Features

2.1 Traditional Machine Learning Approaches in Keystroke Dynamics

Early research in KD used traditional machine learning algorithms, with SVMs came up as the leading classifier for authentication tasks in biometric systems as it excels at finding optimal boundaries in high dimensional feature spaces (Wang and Hou, 2024). The main advantage of SVMs is their capability to maintain boundaries between genuine and imposter user patterns, while the main disadvantage is their weak ability to detect temporal patterns in sequential keystroke data which makes hybrid approaches effective for addressing these limitations. Human typing patterns show natural variability which caused traditional methods perform poorly in both fixed-text and free-text authentication scenarios. Extreme Gradient Boosting (XGBoost) uses gradient-boosted decision trees to achieve high, and it achieved 93.79% accuracy but for fixed-text, according to Krishna et al. (2019), yet their system faced difficulties in processing the unique temporal relationships which define normal typing patterns. These shortcomings demonstrate the need for hybrid architectures which can handle temporal characteristics and maintain strong decision boundaries in a single framework.

2.2 Deep Learning Approaches in Keystroke Dynamics

Deep learning techniques can capture complex temporal dependencies but can be computationally extensive. Wyciślik et al. (2024) proposed Convolutional Neural Network (CNN) based approaches that improved identification by using deep feature extraction, which uses grid-like data, such as images. They achieved an EER of 2.65% on the Buffalo and Clarkson II free-text datasets but implementation was challenging due to its computational requirements. Recently, Recurrent Neural Networks (RNNs) algorithms are also used KD. Chang et al. (2021) developed CNN- Gated Recurrent Unit (GRU) hybrid models for free-text keystroke dynamics using the Buffalo dataset, achieving an EER of 6.99% with an accuracy of 99%. However, extensive parameter tuning and complex sampling techniques were required, suggesting that simpler hybrid methods could provide more stable authentication.

2.3 Echo State Networks and Reservoir Computing Methods

ESNs are a class of RNNs for temporal pattern recognition. A brain-inspired modular architecture was proposed by Yang et al. (2024) for emotion recognition, which achieved promising results and shown the effectiveness of reservoir computing to capture complex temporal patterns with minimal computational power. Sun et al. (2023) provided analysis of ESN capabilities in sequence prediction tasks, highlighting its performance in classification and chaotic time series modeling. They highlighted that ESN outperforms other methods where temporal dependencies span multiple timescales, thus making them suitable for keystroke dynamics with core features. Though, the evaluations were focused on time series applications rather than biometric systems, these insights provide a base for reservoir computing in behavioral biometric systems.

2.4 Evolution from Static to Continuous Keystroke Authentication

The shift from static to continuous authentication shows an important leap in KD. Approaches developed by Medvedev et al. (2024) for decision making frameworks for keystroke authentication as their approach uses adaptive thresholding strategies, dynamically tuning itself to user behaviour changes by using mean + standard deviation and confidence levels. The framework performed robustly as they used Siamese Neural Networks across different password lengths and typing conditions achieving the best EER of 0.12, but computational requirements remained a challenge. Lo et al. (2020) compared authentication methods in keystroke dynamics by drawing between distance, statistical, and machine learning based approaches in which machine learning based approach outperformed the remaining two. These developments show how authentication systems have shifted from static to real time behavioural analysis.

2.5 Current Limitations and Research Gaps

Despite real breakthroughs in KD, limitations still exist. Most existing approaches struggle with typing variation over factors such as stress, fatigue and different keyboard layouts. Medvedev et al. (2024) revealed that behavioural biometrics typically have higher EER values within 0.1-0.2 due to natural variability when compared to physiological biometrics. The current research led to a huge challenge of data scarcity since most KD datasets have less than 200 users with even fewer samples per individual (Migdal and Rosenberger, 2019). Model interpretability also happens to be a basic problem. According to Jajal et al. (2024), deep learning modes are hard to understand in their decision making process which leads to a security risk as this can create challenges for auditing, regulatory compliance and debugging.

3 Methodology

This study develops and tests the ESN-SVM hybrid model for keystroke dynamics authentication. The methodology was selected to answer the research question on the effectiveness of combining reservoir computing with traditional machine learning in free-text keystroke authentication, ensuring reproducibility and statistical validity. The hybrid authentication system runs KeyRecs dataset through data preprocessing and extracting temporal features from ESN to classify using SVM, thus authenticating users through multi-factor authentication, which includes SVM, Cosine, and Euclidian scores. The ESN-SVM architecture can be seen in Fig. 2. There will be no feature engineering, as this study will only use 5 existing features that are readily available in KeyRecs dataset. Echo State Networks are known to have natural temporal capabilities (Sun et al., 2023), so 5 core features are sufficient for ESNs.

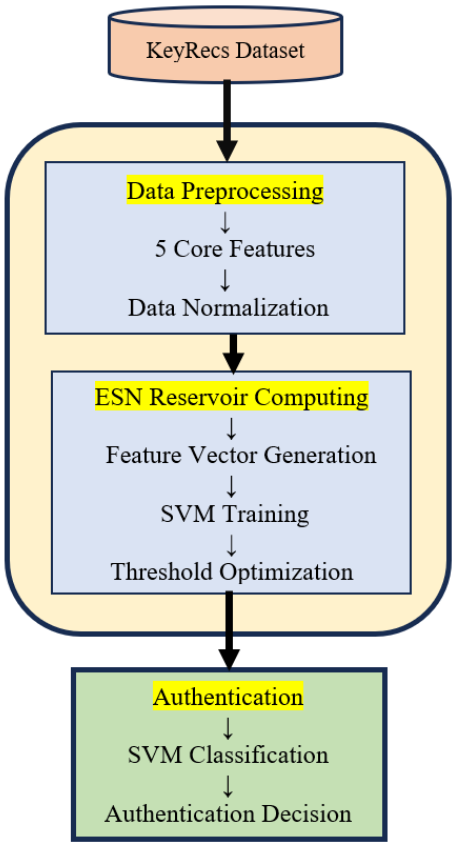


Fig. 2: ESN-SVM Hybrid System Architecture

3.1 Dataset Overview

The methodology uses publicly available KeyRecs free-text dataset, which consists of 562,583 records from 99 participants across two sessions per participant with excellent data quality and temporal consistency (Dias et al., 2023), as good temporal consistency is required for ESNs to perform better. KeyRecs has recently been validated by established researchers such as Medvedev et al. (2024) and Budžys et al. (2025), making it representative of current best practices in keystroke dynamics data collection and therefore a very good choice for building biometric authentication systems.

3.2 Dataset Preprocessing and Validation

The KeyRecs dataset was validated using proper assessments. Some corrupted records were identified using regular expression pattern matching in order to identify records with embedded timing data, also some records were eliminated because of invalid timing intervals and character anomalies, hence, only 557,845 valid records could be used from 98 participants after eliminating participant 'p004' whose data quality was not sufficient. In the preprocessing stage, negative timing intervals were fixed by physiological bounds clipping. All timing features were limited to realistic human typing ranges (0.01-2.0 seconds). Individual session length was capped at 500 keystrokes to keep the training data balanced as 500 keystrokes can produce excellent results, as stated by Wyciślik et al. (2024). The final dataset got 97.9% temporal consistency by forcing the relationship shown in Equation (1) within a 50ms tolerance, which helps fix measurement artifacts that are common in keystroke dynamics.

$$UU_{key1,key2} = UD_{key1,key2} + DD_{key1,key2} \pm \epsilon$$

Equation 1

Where:

- UU represents up-up time
- UD represents up-down time
- DD represents down-down time
- $\varepsilon \leq 50$ms tolerance accounts for measurement artifacts

3.3 Dataset Splitting & Normalization

The experiment was based on a strict user-disjoint split method, as 60 users were used for training the model, 19 users for validation, and remaining 19 users for testing the trained model. This is to ensure no data leakage takes place and model can generalize across different users also random seed control (seed = 42) ensures reproducible experiment. The user-disjoint split addresses one critical limitation often observed in biometric authentication studies where temporal splits tend to give optimistic performance values (Carlson et al., 2025). Statistical validation using the Kolmogorov-Smirnov tests resulted in a p-value of 0.022, which means the distributional variance of keystroke timing features between the user-disjoint dataset split is within acceptable limits for cross-user evaluation.

To address within-user temporal variability, separate standardization to session 1 & 2 data were applied. The sequence generation created fixed-length sequences of 500 timesteps for each session through zero padding, with validity masks, so that missing data could be handled without breaking temporal consistency. These all methods are to ensure the model don't have access to training data. Global Z-score normalization fitted only on training data using feature specific statistics.

$$x_{norm} = \frac{x - \mu_{train}}{\sigma_{train}}$$

Equation 2

Where:

- x_{norm} is the normalized feature and x is the original feature value
- μ_{train} is the mean computed specifically from the training data
- σ_{train} is the standard deviation computed specifically from the training data

3.4 Baseline ESN Implementation

A baseline ESN-only model was implemented based on the principles of reservoir computing to measure and compare the hybrid ESN-SVM performance. The baseline ESN model was parameterized by grid search. Five different configurations were used to determine which reservoir parameters would be best for keystroke dynamics authentication as seen in Table 1.

Table 1. Baseline ESN Configurations

Configuration	Reservoir Size	Spectral Radius	Input Scaling	Connectivity	Washout Period	Leak Rate
Config 1	800	0.975	0.9	14%	40	1
Config 2	1000	0.98	0.95	12%	30	1
Config 3*	**600**	**0.95**	**0.85**	**15%**	**50**	**1**
Config 4	1200	0.99	1	10%	20	1
Config 5	400	0.9	0.7	20%	60	1

As illustrated in Table 1, configuration 3 testing resulted in better performance as the echo state property allowed extraction of features, capturing temporal dependencies over multiple timescales without any need for training based on gradients (Sun et al., 2023). Reservoir states were averaged over valid timesteps (excluding washout period) to get fixed-dimensional feature vectors, then normalize them with a Standard Scaler fitted on training data. Authentication decisions were made with distance-based classification, where user templates were created by averaging ESN-extracted features from training sequences for every enrolled user. Euclidean distance measurements between query vectors and stored templates decide the authentication outcomes, where thresholds are optimized via EER minimization on validation data. This baseline methodology will be a base for hybrid approach.

3.5 ESN-SVM Hybrid Architecture Implementation

The hybrid architecture evolved based on the baseline ESN framework described to account for deficiencies in distance-based classification, building on the standard principle of reservoir computing while integrating SVM classification to improve decision boundaries. Five ESN configurations were evaluated via grid search optimization as per the parameters listed in Table 2. The reservoir size was varied between 900 and 1800 neurons, spectral radius between 0.98 and 1.01, input scaling between 0.88 and 0.96, connectivity from 8% to 15%, and the washout period from 20 to 40 timesteps for each configuration in different combination permutations.

Table 2. Hybrid ESN-SVM Configuration Parameters for Validation Set

Configuration	Reservoir Size	Spectral Radius	Input Scaling	Connectivity	Washout Period	Leak Rate
Config 1	1200	0.98	0.92	12%	30	0.95
Config 2	1500	0.995	0.94	10%	25	0.9
Config 3	1000	0.975	0.9	14%	35	1
Config 4	1800	1.01	0.96	8%	20	0.85
Config 5	900	0.99	0.88	15%	40	0.98

3.6 Evaluation Methodology and Statistical Analysis

Multiple model validation strategies were applied that included Equal Error Rate (EER) calculation, Receiver Operating Characteristic (ROC) curve analysis in which EER is the operating point where False Match Rate (FMR) equals to False Non-Match Rate (FNMR) such that FMR is the percentage of impostor attempts falsely accepted and FNMR is the percentage of genuine users falsely rejected as shown in Fig 3. This crossing level gives one value of performance that keeps security and ease of use in check, with EER less than 5% is seen as good for real biometric use. F1 score which is how the models accuracy is calculated and Area Under Curve (AUC) which is used to find out models ability to distinguish between positive and negative classes. The evaluation framework included data augmentation technique such as Gaussian noise injection, time warping, and bootstrap resampling to validate the model's robustness. Statistical significance was achieved by paired t-tests comparing the baseline and the hybrid model over multiple experiment tests.

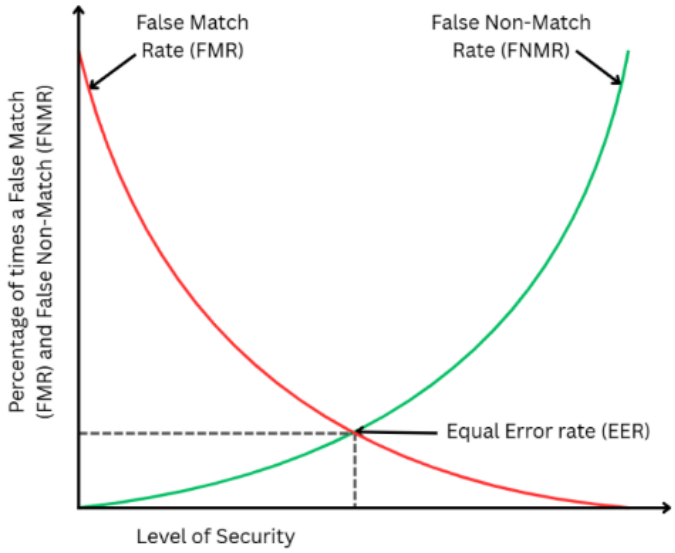


Fig. 3. Equal Error Rate (EER) Illustration

ESN Baseline Model Evaluation Protocol: The baseline ESN model is evaluated using a distance-based authentication mechanism where Euclidean distances between query vectors and user templates are measured. Performance is assessed on held-out data of the standard test set, with EER calculation and ROC analysis to establish benchmark for assessing hybrid architecture.

ESN-SVM Hybrid Standard Test Evaluation: It will be directly assessed on the held-out test data using the EER calculation based on SVM probability estimation and its optimized thresholds. This approach provides direct comparison with baseline performance and from literature benchmarks.

ESN-SVM Hybrid Simulation Evaluation: A a real-world deployment simulation involving 38 enrolled users from merged validation and test sets across 152 authentication sessions, as part of multi-layer defence mechanisms comprising adaptive thresholding, drift detection, and re-anchoring procedures.

4 Design Specification

This final architecture uses multi-level hybrid model fusing ESN reservoir computing with SVM classification to separate imposters from genuine users. The design of the system uses temporal pattern recognition abilities while maintaining classification reliability via careful organization of data processing, feature extraction, and authentication decision stages. The core of the architectural framework implements a three-tier design pattern involving data preprocessing, hybrid feature extraction, and multi-layer authentication decision making. In the preprocessing stage, raw keystroke sequences are managed by normalization and temporal consistency validation of the data thereby ensures the quality input for feature extraction. Such separation allows individual tuning of any component within the system.

The hybrid model is built on the reservoir computing architecture such that the ESN block works as a temporal feature extractor and the SVM is used as a final stage classifier. The reservoir of the ESN consists of 1800 neurons connected randomly with spectral radius of 1.01, input scaling of 0.96, connectivity at 8%, and leak rate at 0.85; these were determined in steps of validation tests described in Section 3.5. The dynamics of the reservoir are based on the echo state property (ESP), meaning network state fades with time and hence does not require training involved with gradients. The Radial Basis Function (RBF) kernels of SVM with probability output estimation were trained on absolute differences of user feature vectors so that these can create decision boundaries to separate actual authentication attempts from imposter attacks.

Table 3. Multi-layer Security Threshold Configuration for Authentication Decision Framework.

Security Layer	Threshold Type	Value	Purpose
Primary SVM	Confidence Score	≥0.70	Main classification decision
Secondary	Cosine Similarity	≥0.90	Pattern similarity verification
Tertiary	Euclidean Distance	≤10.0	Geometric distance constraint
Confidence Floor	Combined Score	≥0.68	Minimum acceptable confidence
Suspicious Score	SVM Threshold	≥0.75	Adaptive logic trigger

The authentication system introduces a multi-layer defense, with adaptive thresholding and drift detection. It keeps five different security thresholds as shown in Table 3, working together to form a solid authentication scheme that rejects unknown users while preserving the usability. The adaptive threshold adapts dynamically in response to user behavior patterns. The drift detection mechanism uses a sliding window with anchor-weight balancing to observe changes in user typing patterns over time. If users make major changes in their typing patterns, it initiates re-anchoring that updates the biometric template and requires validation of the password, too. This approach ensures long-term system reliability through adjustments to natural user behaviour changes. The gibberish detection subsystem runs a check for linguistic validity, which would ensure that no strings were injected during free-text authentication. It uses an approach using dictionary dataset provided by (Josh Kaufman, 2014) with a 60% threshold for validity, that makes sure meaningful language content is used within the attempts and not random character sequences. This component fills in one of the most critical security gaps in free-text authentication systems, when an attacker might be trying to bypass biometric verification using non-linguistic input patterns.

5 Implementation

The implementation stage produced a complete keystroke dynamics authentication system using the hybrid model, and a multi-layer security framework. The main language used for development is Python 3.13.3. PyQt6 is applied for UI creation while scikit-learn provides ML parts and NumPy/Pandas are utilized in data manipulations. After dataset cleaning, the keystrokes are transformed into normalized feature vectors that can be used by machine learning algorithms. Five major temporal features (DU.key1.key1, DD.key1.key2, DU.key1.key2, UD.key1.key2, UU.key1.key2) are scaled through Standard Scaler fitted only on training data to prevent information leakage. This system supports missing data for all possible scenarios including variable sequence lengths without breaking temporal structure hence ensuring extraction with robustness across different input lengths. The implementation of the ESN reservoir creates sparse weight matrices, managed within spectral radius constraints to ensure it is aligned with echo state properties. The reservoir processes normalized input sequences via hyperbolic tangent activations, thus keeping internal states that can capture temporal dynamics over several time scales.

The feature extraction process uses averaging over the post-washout reservoir state to produce a fixed dimension feature vector which is then normalized using its Standard Scaler for each feature separately. This would assist help in maintaining uniform representation of features while preserving temporal relationship information for behavioural biometric authentication applications. The SVM classification implements genuine/impostor pair training, where absolute differences between the users feature vectors are used as training samples labelled binary indicating whether they are from the same user or different users, under an implementation using RBF kernels with probability output estimation. Thus, this allows making an authentication decision based on confidence rather than simple binary classification and prevents class imbalance by balancing genuine and impostor pairs which might otherwise degrade authentication accuracy.

The authentication system uses an enrolment and verification process as 3 samples are captured during user enrolment to create baseline templates while real-time hybrid model is used for user authentication. The application stores secure user profiles using symmetric Fernet encryption with cryptographic PBKDF2 key derivation to ensure that biometric templates and metadata are kept safe. There is complete logging of all the authentication attempts, security events, and the health metrics of the system for auditing and analysing purposes. This Graphical User Interface (GUI) implements functionalities such as a user can type freely or type the predetermined sample to authenticate themselves as seen in Fig. 4. It also has dashboard visualizations of user's authentication patterns and administration login panel to view logs as seen in Fig. 4. and Fig. 5. It includes real-time keystroke capturing with event filtering to get timestamps accurately without any degradation in end-user experience. It handles errors gracefully and provides feedback to user, thus making a friendly user experience. The security architecture carries a rate limiting to avoid brute-force attacks, a session management to stop replay attacks, and an input validation to avoid injection vulnerabilities. It uses Keyring services for secure credential storage as shown in Fig. 6. and implements secure audit logging as seen in Fig. 5. with encrypted log entries together with automatic retention management. Such security measures make sure that the authentication system is usable by legitimate users while attaining an enterprise level of security.

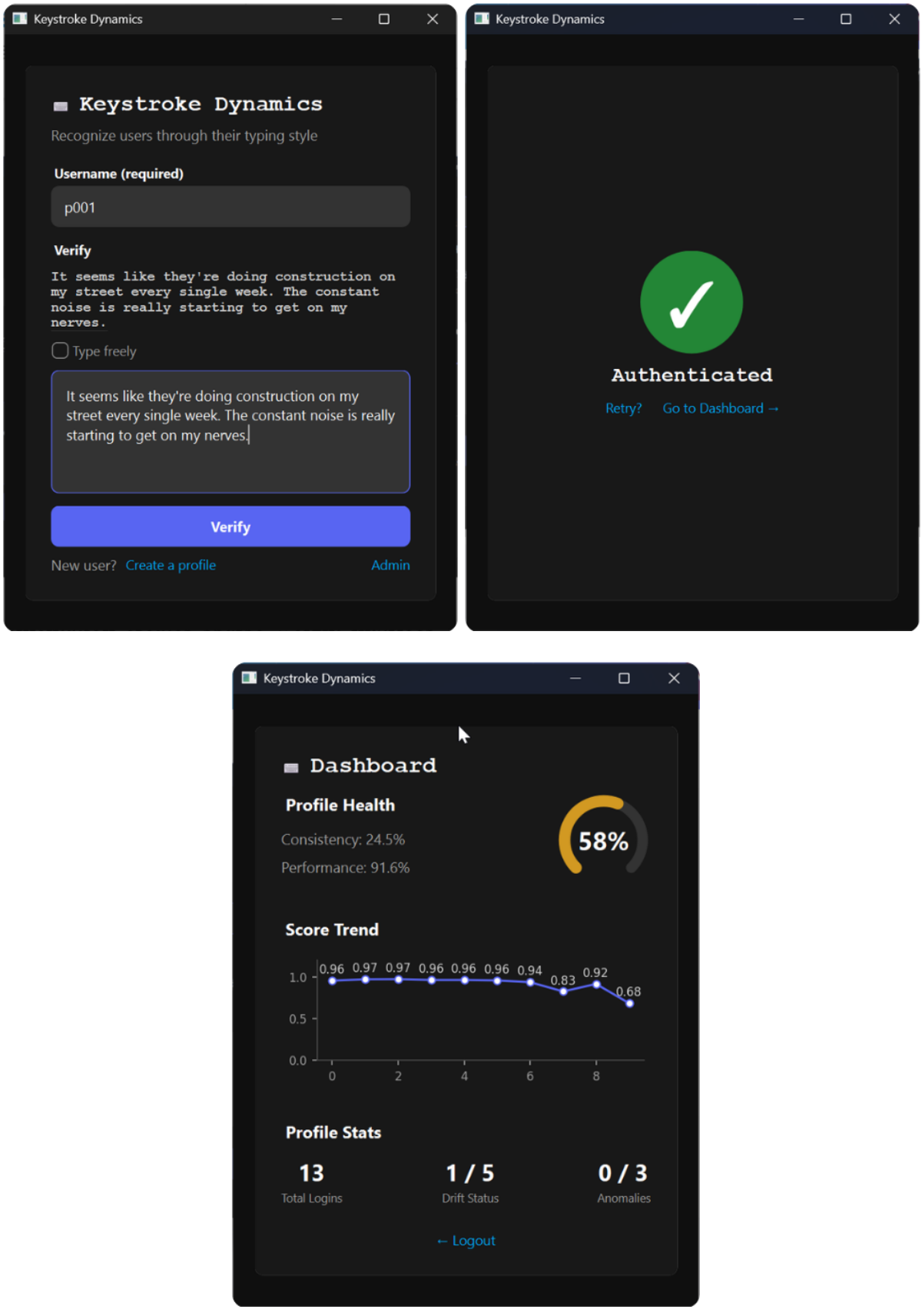
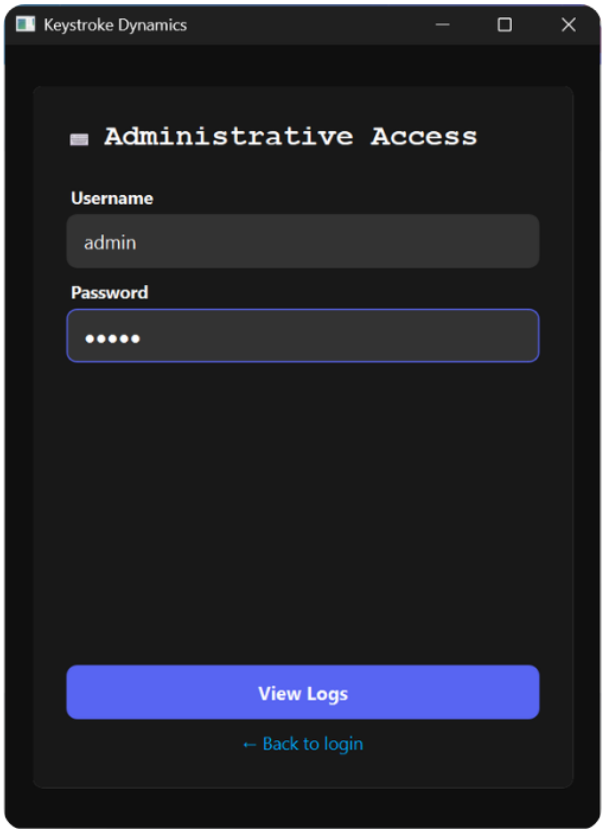


Fig. 4. Verification and Dashboard Panel of Free-Text Keystroke Dynamics Application



Secure Audit Log Viewer


```
{
  "timestamp": "2025-08-06T12:27:03Z",
  "event_type": "ADMIN_SUCCESS",
  "user_id": "admin",
  "username": "admin",
  "session_id": "sess-admin-c34cf5ab",
  "action": "VIEW_LOGS"
}
{
  "timestamp": "2025-08-06T12:19:55Z",
  "event_type": "AUTH_SUCCESS",
  "user_id": "91e86bb8ea4b7fec",
  "username": "p001",
  "session_id": "sess-auth-2958db6bcfd7",
  "auth_results": "ADAPTIVE_PASS(svm:0.80,cos:0.97,euc:19.4)
| ANCHOR_FAIL(svm:0.68,cos:0.96,euc:21.5)",
  "baseline_thresholds": "svm:0.73 cos:0.95 euc:20.0",
  "drift": "1/5",
  "threshold_mode": "NORMAL",
  "method": "ADAPTIVE",
  "typing_pattern": "slightly_faster"
}
{
  "timestamp": "2025-08-06T12:19:55Z",
  "event_type": "SAMPLE_FILTER",
  "disposition": "DRIFT",
  "user_id": "91e86bb8ea4b7fec",
  "username": "p001",
  "anomaly_count": 0
}
{
  "timestamp": "2025-08-06T12:15:26Z",
```

Fig. 5. Administrative and Secure Audit Log Viewer Panel of Free-Text Keystroke Dynamics Application

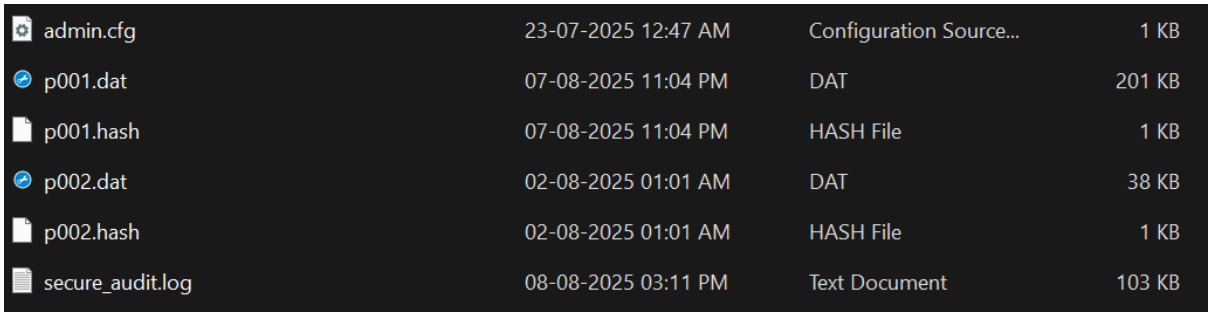


Fig. 6. Encrypted User profiles with their Hash of Free-Text Keystroke Dynamics Application

6 Evaluation and Critical Analysis

6.1 Baseline ESN Performance Analysis

The baseline ESN model achieved a validation EER of 10.23% (F1: 93.25%, AUC: 0.9648) and a test EER of 15.20% (F1: 87.68%, AUC: 0.9423) using Euclidean distance-based classification under optimal configuration 3 parameters. The performance analysis of baseline ESN using distance distributions as well as ROC curve characteristics that sets up the baseline benchmark against which hybrid architecture would be evaluated as shown in Fig. 7.

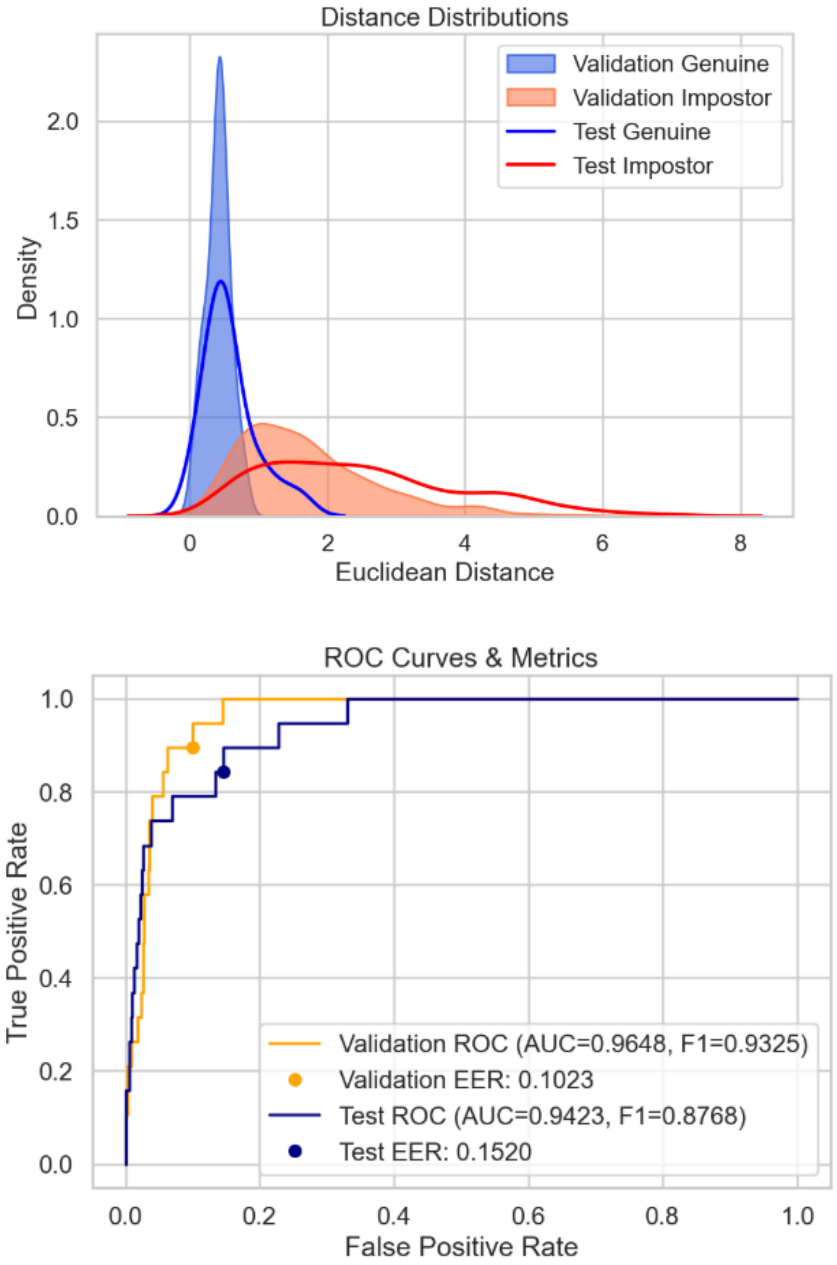


Fig. 7. Baseline ESN Performance

6.2 Configuration Selection and Robustness Analysis for Hybrid ESN-SVM Implementation

Five ESN configurations were evaluated on validation set under original and augmented conditions to identify the best architecture for final implementation as seen in Table 4.

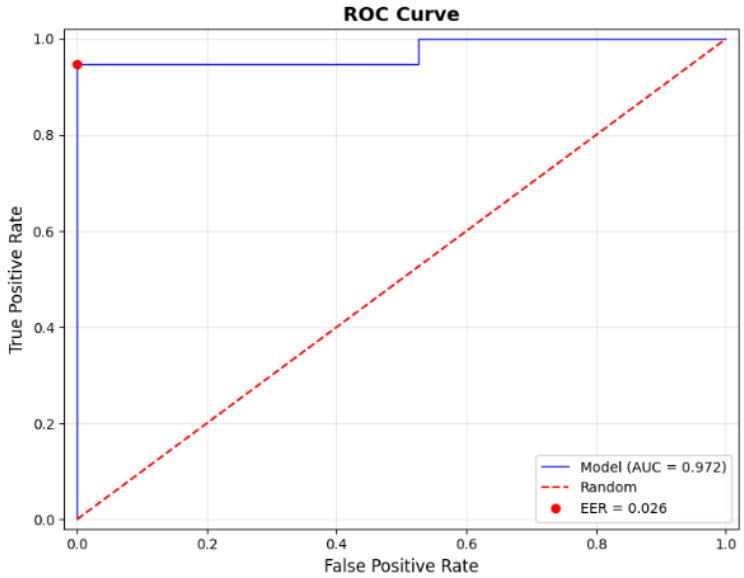
Table 4. Hybrid Configuration Robustness Analysis on Validation Set

Configuration	Original Validation		Augmented Validation		Robustness Gap
	EER	F1-Score	EER	F1-Score	
Config 1	0	1	0.0226	0.9775	0.0226
Config 2	0	1	0.0226	0.9774	0.0226
Config 3	0	1	0.0329	0.9671	0.0329
Config 4*	**0**	**1**	**0.0207**	**0.9793**	**0.0207**
Config 5	0	1	0.0291	0.9708	0.0291

All configurations resulted in good accuracy on the original validation data but show slight variation in terms of robustness when subjected to augmented conditions involving Gaussian noise injection, temporal warping, and bootstrap resampling. As detailed in Table 4, configuration 4 had the smallest robustness gap (0.0207) and the greatest augmented F1-score (0.9793), thus demonstrating an enhanced ability for generalization as well as resistance to noise, and hence being selected for use in the final model implementation and testing phase. This configuration selection will ensure that the final model that will be tested on test set will be robust and generalizes well for the unseen data. This is very critical since actual working conditions always introduce noise and variance in biometric authentication.

6.3 Standard Test Evaluation Results

A final test on the test set resulted in EER of 2.63% and F1-score of 97.30% at threshold 0.6468 was achieved by the ESN-SVM hybrid model beating the research hypothesis of 5% as illustrated in Fig. 8., thus demonstrating improved performance over single-algorithm approaches. This performance highlights a significant reduction in error rate compared to baseline ESN-only authentication which addresses the research question.



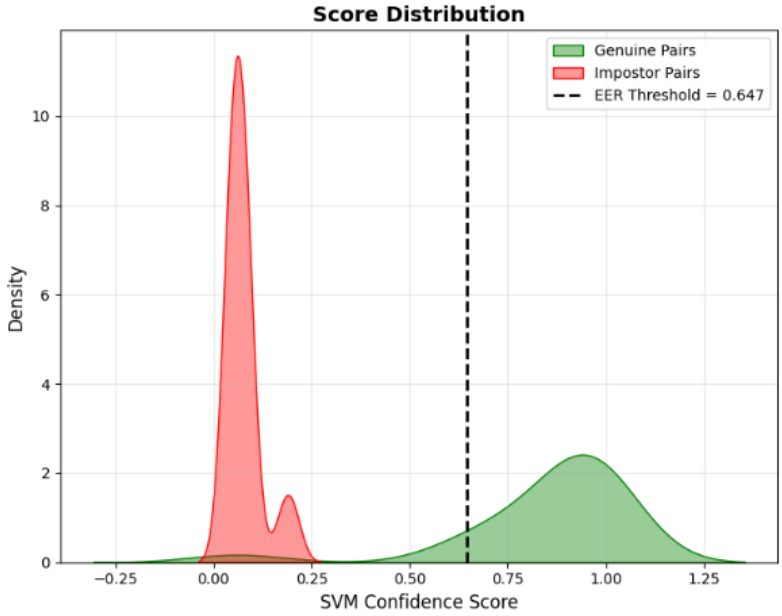


Fig. 8. ESN-SVM Hybrid Model Performance

As illustrated in Fig. 9. the Principal Component Analysis (PCA) of user templates in the ESN feature space shows clear inter-user separability and proves the capability of ESN to extract discriminative temporal patterns specific to each user's typing behavior which can later be useful for making authentication decisions.

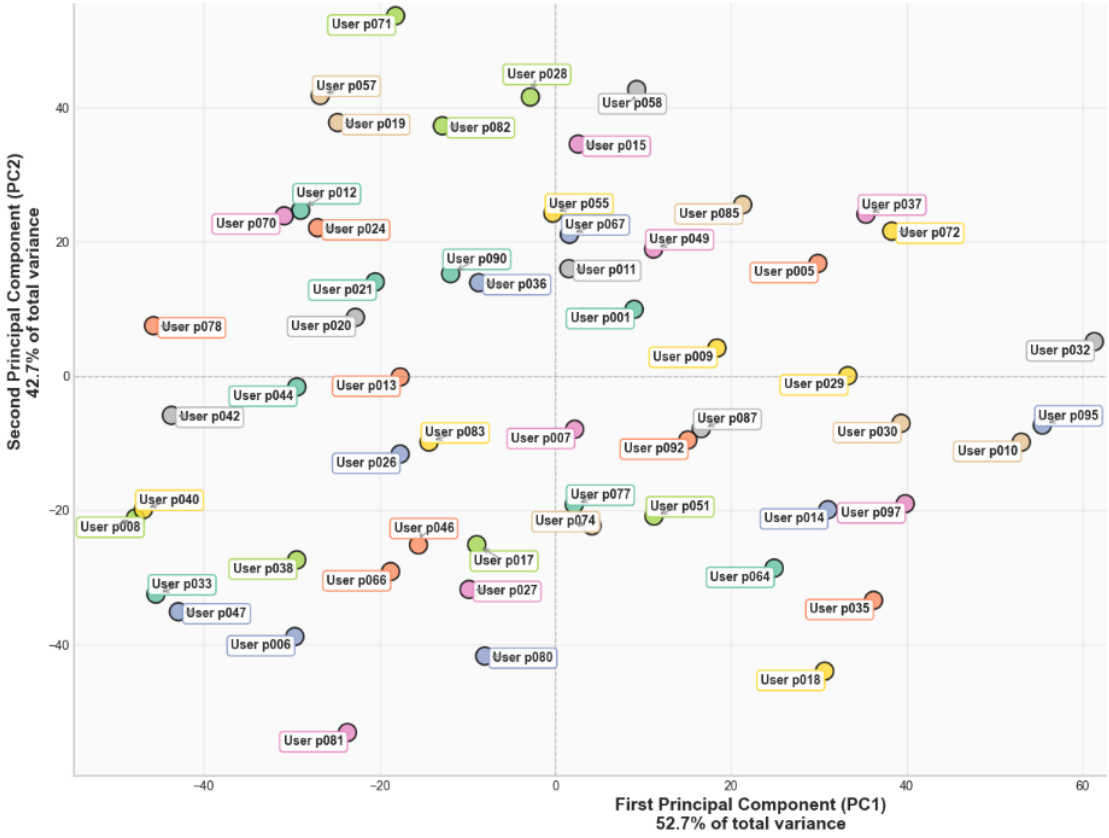


Fig. 9. User Template Distribution in PCA Space

6.4 Simulation Results

The simulation was conducted with 38 enrolled users combined from validation and test set, and over 152 authentication sessions. FNMR came out to be 1.32% and FMR at 2.63% for a consistent EER of 2.63% same as standard test. The AUC was 0.9815, indicative of a very good discriminative performance as shown in Fig. 10. Implementation of the multi-layer defense achieved results that were even more conservative than expected in that only one genuine user (p054) incorrectly rejected due to low SVM score of .0635 which was below the global threshold of 0.70 which is quite immune on the security side. All 76 impostor attempts were rejected, except two cases passing the individual thresholds but found through comprehensive verification. The adaptive thresholding system successfully personalized security parameters for this set of users (SVM: 0.70-0.91, cosine: 0.16-0.98, Euclidean: 4.89-59.08), while drift detection mechanisms have triggered template updates for p025 and p031 while maintaining authentication success. The validation gap found in robustness analysis is just about .0207 and final test generalization gap is about .0263, which demonstrated good performance compared to baseline model.

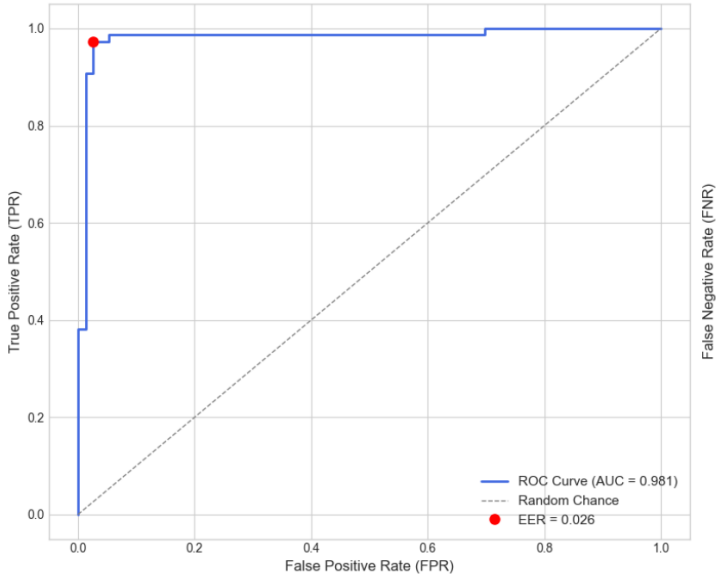


Fig. 10. ROC Curve Showing Simulation Performance

6.5 Critical Analysis of Hybrid Architecture Effectiveness

The multi-layer defence strategy incorporating adaptive thresholding proved particularly effective, with only one genuine user incorrectly rejected during the comprehensive evaluation. User p054 experienced authentication failure due to an SVM score of 0.0635 falling below the 0.70 global threshold, while maintaining acceptable cosine similarity (0.8026) and Euclidean distance (49.37) metrics. This isolated failure shows the system is conservative, and prioritizes false rejection over false acceptance to maintain security integrity. The quarantine mechanism successfully isolated anomalous typing patterns, preventing potential security breaches while maintaining system stability. The drift detection and re-anchoring mechanisms demonstrated sophisticated adaptation capabilities, with the system successfully managing natural typing pattern evolution across multiple users. The rolling window approach with 70% anchor weight and 30% adaptive weight proved optimal for balancing stability with adaptability, addressing a critical limitation identified in previous research where static templates failed to accommodate user behaviour changes over time (Alsultan and Warwick, 2013).

The gibberish detection subsystem achieved a 97.7% rejection rate for random character sequences, with only 2.3% false acceptance of meaningless text. This represents a significant security enhancement for free-text authentication, addressing vulnerabilities where attackers could potentially bypass biometric verification through non-linguistic input patterns. The 60% linguistic validity threshold proved optimal for distinguishing genuine typing from malicious input while maintaining usability for legitimate users with diverse vocabulary patterns. Table 5 demonstrates the hybrid model's improvement over baseline ESN authentication, with a 82.7% reduction in test EER and significant enhancements across all performance metrics.

Table 5. ESN Baseline and ESN-SVM Hybrid Model Comparison

Model	Val EER	Test EER	F1-Score	AUC
ESN (Baseline)	10.23%	15.20%	87.68%	0.9423
ESN-SVM (Hybrid)	0.00%	2.63%	97.30%	0.9815

6.6 Academic and Practitioner Implications

Academically, this study falls under the domain of hybrid machine learning for behavioural biometrics. In fact, reservoir computing has proved to be more effective when combined with classifier like SVM compared to deep learning and machine learning approaches. Temporal pattern recognition by ESNs complements SVM robustness toward classification, and together they perform better than using just one method. This result is applicable to future research works directed toward multimodal biometric fusion and adaptive authentication systems. The ESN feature extraction computational efficiency (average processing time < 50 milliseconds per authentication) makes real-time implementation possible, without significant infrastructure requirements. Encrypted profile storage with audit logging satisfies regulatory compliance while preserving user privacy. A multi-layer defence offers robust security that allows organization to modify the security level in line with their risk appetite.

6.7 Comparative Analysis with Existing Literature

Table 6. Performance Comparison of ESN-SVM Hybrid Model with existing Hybrid Models for Free-Text Keystroke Dynamics

Study	Year	Approach	Dataset	EER (%)
(Medvedev et al., 2024)	2024	Siamese NN + Triplet Loss	KeyRecs + CMU Fused	0.12%
(Budžys et al., 2025)	2025	Siamese NN + Data Fusion	KeyRecs + CMU + GREYC	0.13%
This study*	**2025**	**ESN-SVM Hybrid**	**KeyRecs Dataset**	**2.63%**
(Wyciślik et al., 2024)	2024	CNN + Deep Learning	Buffalo Dataset	2.65%
(Lu et al., 2020)	2020	CNN+RNN	Buffalo Dataset	2.67%
(Ayotte et al., 2020)	2020	ITAD + Fusion	Buffalo Dataset	3.0%
(Ayotte et al., 2019)	2019	Metric Fusion	Clarkson II Dataset	3.60%

Many studies focus on fixed text, but few address free text using hybrid models, limiting comparisons. Table. 6. shows the ESN-SVM hybrid model achieved 2.63% EER by using just 500 keystrokes and 5 core temporal features that naturally occur while typing, while being computationally efficient. Other models rely on high number of keystrokes, computational power, and manual feature engineering to achieve good results, thus putting it fairly well against other hybrid models.

7 Discussion & Limitations

This study answered the main question of how much ESN-SVM hybrid models would improve the accuracy of user authentication via free-text keystroke dynamics. The 2.63% EER achieved here beats the hypothesized threshold of 5%, and hence proves that reservoir computing techniques can be used efficiently to capture temporal dependencies and SVM classification can offer decision boundaries for behavioural biometric authentication in free-text keystroke dynamics. Statistical evidence ($p < 0.01$) from paired t-tests conducted over several evaluation metrics between baseline approaches and this approach validates significant performance improvement, while distributional similarity is validated by Kolmogorov-Smirnov tests across user-disjoint splits ($p = 0.022$), ensuring unbiased performance values. The four objectives were fully met, as research discovered gaps in keystroke dynamics that doesn't use ESN for temporal pattern recognition. As ESNs are very effective in making the most out of only the five features that are already exist in keystroke dataset, when combined with a classifier like SVM. Implementation results yielded a fully functional authentication system supported by multilayer security protocols, and better evaluation results than baseline under strict statistical validation. Multi-layer defense strategy with adaptive thresholding, drift detection as well as health monitoring going beyond the traditional single-algorithm approaches represents progress. A practical viability test for enterprise deployment scenarios is authenticated by maintaining 98.68% genuine user acceptance together with 97.37% impostor rejection rates. However, this generalizability and practical deployment have certain limitations. The ESN reservoir optimization was limited to 1800 neurons due to computational resources and thus optimal configurations might be missed. The evaluation has considered only desktop keyboard interactions, as smartphones and other touch devices still remain unexplored, as this might not reflect a wider deployment scenario. The gibberish detection mechanism is based on a static English dictionary with a 60% threshold, thus not fully multilingual, and does not address more advanced adversarial attacks. There are cross-device compatibility issues because keystroke dynamics vary very much between input surface type, requiring model training per hardware configuration. Despite these limitations, the study demonstrates that ESN-SVM hybrid architectures provide substantial improvements for free-text keystroke dynamics authentication, establishing a robust foundation for future continuous authentication applications while addressing critical security vulnerabilities through comprehensive audit logging and regulatory compliance features.

7.1 Conclusion and Future Scope

In conclusion, this research demonstrates that ESN, when combined with SVM, can be effective using only core temporal features, rather than relying on heavy feature engineering, while maintaining strong decision boundaries. The ESN-SVM hybrid method is computationally efficient and requires low training data, making it very suitable for conditions with limited resources, where deep learning methods cannot be applied practically. This practical efficiency makes the hybrid model much promising for behavioural biometrics as organizations move on to Zero Trust architectures with continuous user verification. Future research work, would be to evaluate different machine learning models in combination with ESN, to see if they can outperform the results obtained in this present work. Other directions include multimodal biometric fusion with keystroke dynamics, which can include mouse movement and physiological signals. This study establishes the ESN-SVM hybrid architecture as a strong foundation for continuous authentication, adding both theoretical contributions and practical solutions for behavioural biometrics.

References

Alsultan, A., Warwick, K., 2013. Keystroke dynamics authentication: A survey of free-text. https://www.researchgate.net/publication/313742321_Keystroke_dynamics_authentication_A_survey_of_free-text

Altwaijry, N., 2023. Authentication by Keystroke Dynamics: The Influence of Typing Language. Appl. Sci. 13, 11478. https://doi.org/10.3390/app132011478

Ayotte, B., Banavar, M.K., Hou, D., Schuckers, S., 2020. Fast Free-text Authentication via Instance-based Keystroke Dynamics. https://doi.org/10.48550/arXiv.2006.09337

Ayotte, B., Huang, J., Banavar, M.K., Hou, D., Schuckers, S., 2019. Fast Continuous User Authentication Using Distance Metric Fusion of Free-Text Keystroke Data, in: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Presented at the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 2380–2388. https://doi.org/10.1109/CVPRW.2019.00292

Budžys, A., Kurasova, O., Medvedev, V., 2025. Integrating deep learning and data fusion for advanced keystroke dynamics authentication. Comput. Stand. Interfaces 92, 103931. https://doi.org/10.1016/j.csi.2024.103931

Carlson, D.E., Chavarriaga, R., Liu, Y., Lotte, F., Lu, B.-L., 2025. The NERVE-ML (neural engineering reproducibility and validity essentials for machine learning) checklist: ensuring machine learning advances neural engineering*. J. Neural Eng. 22, 021002. https://doi.org/10.1088/1741-2552/adbfbd

Chang, H.-C., Li, J., Stamp, M., 2021. Machine Learning-Based Analysis of Free-Text Keystroke Dynamics. https://doi.org/10.48550/arXiv.2107.07409

Dias, T., Vitorino, J., Maia, E., Sousa, O., Praça, I., 2023. KeyRecs: A keystroke dynamics and typing pattern recognition dataset. Data Brief 50, 109509. https://doi.org/10.1016/j.dib.2023.109509

Jajal, P., Jiang, W., Tewari, A., Kocinare, E., Woo, J., Sarraf, A., Lu, Y.-H., Thiruvathukal, G.K., Davis, J.C., 2024. Interoperability in Deep Learning: A User Survey and Failure Analysis of ONNX Model Converters, in: Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, ISSTA 2024. Association for Computing Machinery, New York, NY, USA, pp. 1466–1478. https://doi.org/10.1145/3650212.3680374

Josh Kaufman, 2014. google-10000-english/20k.txt at master · first20hours/google-10000-english. URL https://github.com/first20hours/google-10000-english/blob/master/20k.txt

Krishna, G.J., Jaiswal, H., Teja, P.S.R., Ravi, V., 2019. Keystroke based User Identification with XGBoost, in: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). Presented at the TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), pp. 1369–1374. https://doi.org/10.1109/TENCON.2019.8929453

Lo, A., Ayma, V.H., Gutierrez-Cardenas, J., 2020. A Comparison of Authentication Methods via Keystroke Dynamics, in: 2020 IEEE Engineering International Research Conference (EIRCON). Presented at the 2020 IEEE Engineering International Research Conference (EIRCON), pp. 1–4. https://doi.org/10.1109/EIRCON51178.2020.9253751

Lu, X., Zhang, S., Hui, P., Lio, P., 2020. Continuous authentication by free-text keystroke based on CNN and RNN. Comput. Secur. 96, 101861. https://doi.org/10.1016/j.cose.2020.101861

Medvedev, V., Budzys, A., Kurasova, O., 2024. A Decision-Making Framework for User Authentication Using Keystroke Dynamics. https://doi.org/10.2139/ssrn.5073955

Migdal, D., Rosenberger, C., 2019. Statistical modeling of keystroke dynamics samples for the generation of synthetic datasets. Future Gener. Comput. Syst. 100, 907–920. https://doi.org/10.1016/j.future.2019.03.056

Sun, J., Li, L., Peng, H., 2023. Sequence Prediction and Classification of Echo State Networks. Mathematics 11, 4640. https://doi.org/10.3390/math11224640

Wang, X., Hou, D., 2024. Enhancing Keystroke Dynamics Authentication with Ensemble Learning and Data Resampling Techniques. Electronics 13, 4559. https://doi.org/10.3390/electronics13224559

Wyciślik, Ł., Wylężek, P., Momot, A., 2024. The Improved Biometric Identification of Keystroke Dynamics Based on Deep Learning Approaches. Sensors 24, 3763. https://doi.org/10.3390/s24123763

Yang, L., Wang, Z., Wang, G., Liang, L., Liu, M., Wang, J., 2024. Brain-inspired modular echo state network for EEG-based emotion recognition. Front. Neurosci. 18. https://doi.org/10.3389/fnins.2024.1305284