Informatics Institute of Technology

In Collaboration With

The University of Westminster, UK

AEGIS PROTOCOL

An Advanced Hybrid Continuous Authentication Approach using Behavioural Biometrics

Final Project Report

Mr. Gapilesh Pirabaharan

W1898932 | 20211306

Supervised by

Mr. Guhanathan Poravi

July 2025

Submitted in partial fulfilment of the requirements for the BEng (Hons) Software Engineering degree at the University of Westminster.

ABSTRACT

Traditional, static authentication systems leave user sessions vulnerable to post-login threats like session hijacking. This research project, the Aegis Protocol, addresses this gap by developing an advanced continuous authentication (CA) system based on free-text keystroke dynamics. The core of this work is the design and implementation of a novel hybrid deep learning architecture that captures the nuanced, temporal patterns of an individual's typing rhythm to provide persistent, passive security.

The methodology involved using the large-scale Buffalo Keystroke Dataset to train the proposed EnhancedHybridModel. A comprehensive feature engineering pipeline was implemented to create a rich 30-dimensional feature vector, which was then fed into a model combining a multi-scale Convolutional Neural Network (CNN), a deep Bidirectional LSTM (BiLSTM), and a self-attention mechanism. The entire system, developed in Python with PyTorch, was realised as a functional proof-of-concept with a demonstration UI and a Flask API.

The final model was rigorously evaluated on an unseen test set, achieving a competitive Equal Error Rate (EER) of 22.58%, a security-focused False Acceptance Rate (FAR) of 8.06%, and an Area Under the ROC Curve (AUC) of 0.839. These results, supported by qualitative expert feedback, validate the effectiveness of the proposed architecture. The Aegis Protocol contributes a novel and robust architectural blueprint to the field of behavioural biometrics, demonstrating a powerful approach for developing next-generation continuous authentication systems.

Subject Descriptors:

- Security and privacy → Security services → Authentication → Biometrics
- Computing methodologies → Machine learning → Machine learning approaches → Neural networks

Keywords: Behavioural Biometrics, Continuous Authentication, Deep Learning, Keystroke Dynamics, Attention Mechanism, Convolutional Neural Network, Long Short-Term Memory, Classifier