**Different Scenarios**

**Scenario 1: Jumbled QWERTY Alphabet keyboard training**

Approach:

Implementing an alphabet keyboard password typing based user patterns to analyse the legitimacy of the user.

Collect behavioral biometrics, such as typing speed, dwell time (time spent on each key), flight time (time between key presses), and pressure applied to each key. Pixel measurement. Surface area covered. (research papers)

Xiomi, Vivo, Oppo, Oneplus.

Technologies:

Keystroke Dynamics Analysis using RNNs (Recurrent Neural Networks) to model the temporal sequence of key presses.

Pressure Sensitivity Analysis using sensors available in modern touchscreens to measure the intensity of each touch.

**Scenario 2: Behavioral Biometrics with Dynamic Keypad**

Approach:

Use a dynamic, jumbled keypad for each login attempt, where the position of the digits changes randomly.

Collect behavioral biometrics, such as typing speed, dwell time (time spent on each key), flight time (time between key presses), and pressure applied to each key.

Technologies:

Keystroke Dynamics Analysis using RNNs (Recurrent Neural Networks) to model the temporal sequence of key presses.

Pressure Sensitivity Analysis using sensors available in modern touchscreens to measure the intensity of each touch.

**Scenario 3: Multi-Modal Authentication System (future)**

Approach:

Combine the jumbled number pad authentication with other modalities, such as facial recognition or fingerprint scanning, to create a multi-modal system.

Use machine learning to analyze the combined probability scores from each modality to make a final authentication decision.

Technologies:

Implementation of Convolutional Neural Networks (CNNs) for facial recognition.

Sensor Fusion techniques to integrate data from different sources (e.g., touchscreen, camera, fingerprint sensor) effectively.

**Scenario 4: Adversarial Machine Learning for Enhanced Security**

Approach:

Employ adversarial machine learning techniques to continuously test and improve the security of the authentication system.

Generate adversarial examples to simulate potential attack vectors and use them to train the model, enhancing its ability to withstand real-world attacks.

Technologies:

Adversarial Training Frameworks to generate and defend against adversarial attacks.

Robust Machine Learning Models that can generalize well from both authentic and adversarial data.

**Scenario 5: Context-Aware Authentication**

Approach:

Integrate contextual information, such as location, time of day, and device usage patterns, into the authentication decision-making process.

Adjust the authentication requirements based on the assessed risk level, potentially simplifying the process in trusted environments.

Technologies:

Contextual Analysis using Decision Trees or Bayesian Networks to infer the level of risk based on environmental factors.

Dynamic Security Policies that can adjust authentication challenges in real-time based on contextual analysis.

|  |  |  |
| --- | --- | --- |
|  | Normal Data (.text) | Similar Data (Weaviate db) |
| N\_layer (HP) | 3 | 3 |
| N\_head (HP) | 3 | 3 |
| Training Time | 6 hrs 21 mins | 11 hrs 11 mins |
| Initial Train Loss | 4.1795 | 4.1404 |
| Final Train Loss | 1.2245 | 1.1523 |
| Final validation loss | 1.5644 | 1.2589 |
| RAM usage | 8 GB | 3 GB |
| Query Time |  | 13 mins |
| BLEU score | 1.9928716133531454e-155 | 1 |
| F1 score | 0.3814 | 0.7992 |