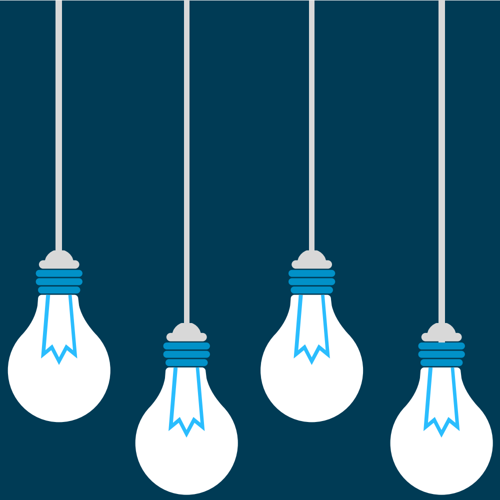


WCE HACKATHON 2020

IDEA SUBMISSION ABSTRACT

PROBLEM

SOLUTION

Team Information :

1. Team Name : Pied_Pipers
2. Team Leader : Pragati Gaikwad
3. College Name : MIT Academy of Engineering, Alandi (D)
4. Theme : Open Innovation (O.P1)
5. Subtheme : Security

Team Members' Roles and Responsibilities :

- UI Designing & Data Collection

Shoyab Shaikh
Pragati Gaikwad

- Pre-processing Data & Training the Model

Atharva Deshpande
Sarang Barshikar

Project Abstract :

- The demand for modern tools and techniques to restrict access to applications and services which contain delicate data is increasing exponentially.
- Traditional methods such as Personal Identification Number (PINs), tokens, or passwords fail to keep up with the challenges presented because they can be lost or stolen, which compromises the system security.
- The most promising approach can be Keystroke biometrics which refers to the **habitual patterns** an individual exhibits while typing on a keyboard.
- Every user has a certain way of typing, which separates them from other users. Keystroke dynamics is one of the major evolving biometrics, which involves authentication based on typing patterns of its users, which distinguishes them from one another.
- This technology can be used with any form of authentication such as PINs and passwords. It helps decrease the dependency on primary forms of authentication.

Market Research :

- As enterprise customers constantly focus on adding an additional layer of security to secure their data. Rise in number of online frauds in digital transactions, need of advanced security mechanisms increases the need for keystroke dynamics, thereby driving the market growth.

- Keystroke dynamics has tremendous potential for cyber security applications. Keystroke dynamics facilitates a natural and cost effective way for security and access protection of computers and mobile devices.

- It also allows for continuous authentication by monitoring a user’s typing behavior during the entire login session without any interruption to the user’s routine work.

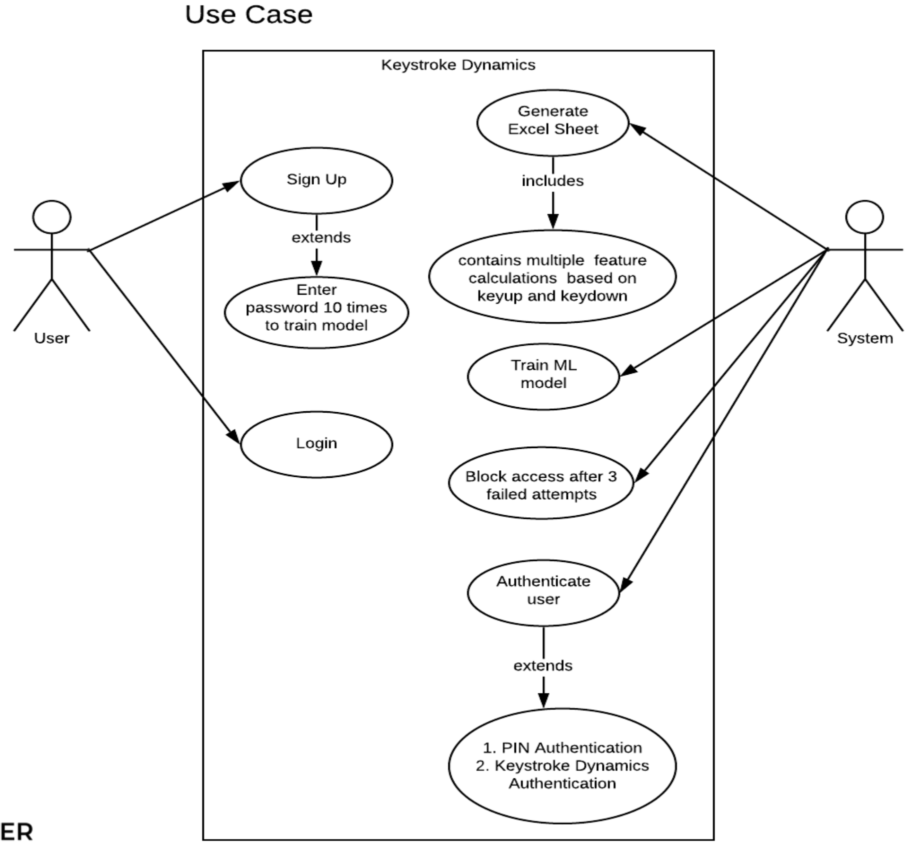
Compared to other biometric techniques, keystroke has the primary advantages that:

- No external hardware requirement like scanner or detector . All that is needed is a keyboard.
- The “rhythm” or the pattern of the users is a very reliable statistic.
- It can easily be deployed in conjunction with existing authentication system.
- Without awareness of intruder a security mechanism is being implemented.
- Dictionary or Brute Force Attack & Cross Side Scripting are restricted.

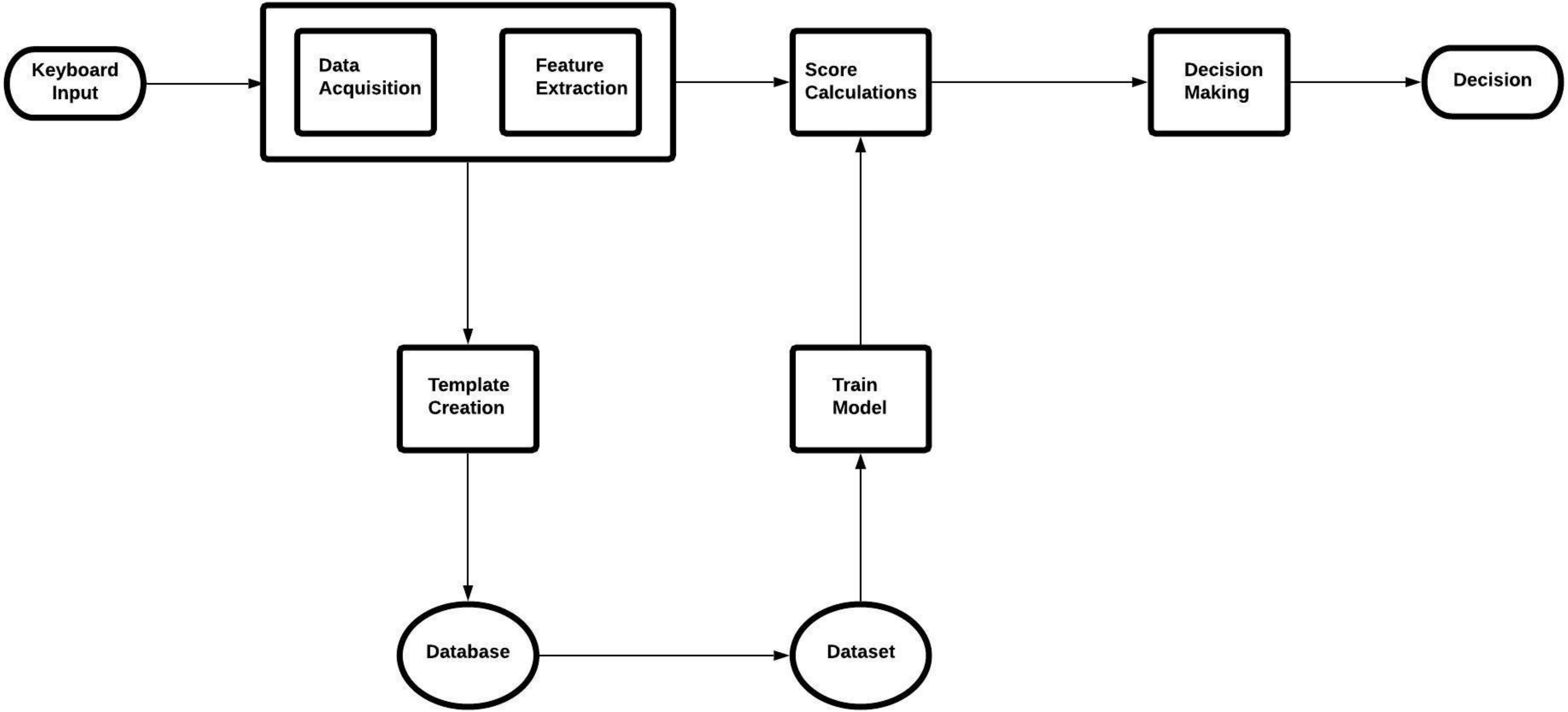
Technology Stack :

- Front End: HTML, CSS, JavaScript
- Back End: Django
- Database: Mongo DB
- Machine Learning Algorithm

Use Case Diagram:


Use Case
Keystroke Dynamics
User
System
Sign Up
extends
Enter password 10 times to train model
Login
Generate Excel Sheet
includes
contains multiple feature calculations based on keyup and keydown
Train ML model
Block access after 3 failed attempts
Authenticate user
extends
1. PIN Authentication
2. Keystroke Dynamics Authentication

Flow Diagram :



Description of the flow diagram

1. The individual register their name and password with the database. Then the user has to type his username and password and train the model.

2. Features are extracted when individual press and release keys. More specifically the delay between the key-down and key-up time.

3. The algorithm is applied and the threshold is generated based on the variations that the user has done while typing.

4. Calculate the Euclidean distance between training and the test samples to get the user's score.

5. Finally, the user's score is compared against its threshold to make the decision. If the Euclidean measure generated from the test sample is too high when compared to the training set then the user is classified to be an imposter.

Innovativeness :

- Our solution will be used as a **multifactor authentication**.
- Solution will track the typing pattern of the user.
- Keystroke dynamics is used to analyze whether accounts are being shared. Reasons for such an implementation could be verification of users to verify that no password sharing is being done.
- Intrusions through dictionary or Brute Force Attack & Cross Site Scripting are restricted.