बैंक ऑफ़ बड़ौदा
Bank of Baroda

Technology Partner
Microsoft Azure

Bank of Baroda Hackathon - 2022

Team Name :1001001

Title : **Keystroke.io**

Team bio : Final year CSE students from M S Ramaiah Institute of Technology, Bangalore

Date : 20/09/2022

Problem Statement

More than ever before the Internet is changing computing as we know it. Unfortunately, with these advances in technology comes increased chances of malicious attack and intrusion and have unveiled new threats to computer system security.

As we press into the twenty-first century, Digital banking has become the single most effective channel for financial institutions to drive growth, increase revenue and attract new customers. However, advanced safeguards against fraud and impersonation, as well as more foolproof measures against unauthorized access to computer resources and data are now being sought.

Username and password pairs as authentication factors are as weak as they are ubiquitous. Usernames and passwords can be "phished," stolen, discovered, and cracked in a number of ways. Therefore, a neuro-physiological approach would enhance the current authentication methods compared to only facial recognition or fingerprints which can be cracked in number of ways.

We present Keystroke.io, a safeguard mechanism which authenticates access by recognizing certain unique and habitual patterns in a user's typing rhythm.

User Segment & Pain Points

Keystroke dynamics contributes to a new revolution authentication: continuous authentication. Previously, authentication would stop at the login stage. If you knew the password you received access, no further questions asked.

Continuous authentication by contrast constantly verifies users, looking for any sign they may be victims of infiltration. Any sign of malicious subversion can trigger alerts and incident response, speeding up response times and thus mitigating damage from a breach. Therefore keystroke dynamics can be used by banks, surveillance facilities and anyone for their personal use.

User Segment & Pain Points

Therefore keystroke dynamics can be used by banks, surveillance facilities and anyone for their personal use.

- **Banks:** Banks can implement our idea in their mobile applications to track the behavioral patterns of their users to continuously authenticate the identity of their users apart from the usual authentication.

- **Surveillance and Security Facilities:** To operate the security equipment and computers, a site under monitoring needs a specialized control room. To monitor the systems and make sure an unauthorised individual is not occupying the control room, it is crucial to constantly confirm the authorized personnel's identification. Keystroke dynamics and behavioral pattern recognition can be used in such a situation.

- **Personal use:** Users who want to keep their data secured and ensure their privacy can use our idea to trigger a response in case of a third person accesses their phone or computer system.

Azure tools or resources

Microsoft Azure Cognitive Services are a set of prebuilt APIs, SDKs and customizable services for developers, including perceptual and cognitive intelligence covering speech recognition, speaker recognition, neural speech synthesis, face recognition, computer vision, OCR/form understanding, natural language processing, machine translation, and business decision services. Most AI features appeared in Microsoft's own products and services (Bing, Office, Teams, Xbox, and Windows) are powered by Azure Cognitive Services.

Azure SDK for Python - The libraries support Python 3.6 or later, and it is also tested with PyPy 5.4+.
The Azure SDK for Python is composed solely of over 180 individual Python libraries that relate to specific Azure services.

Methodology

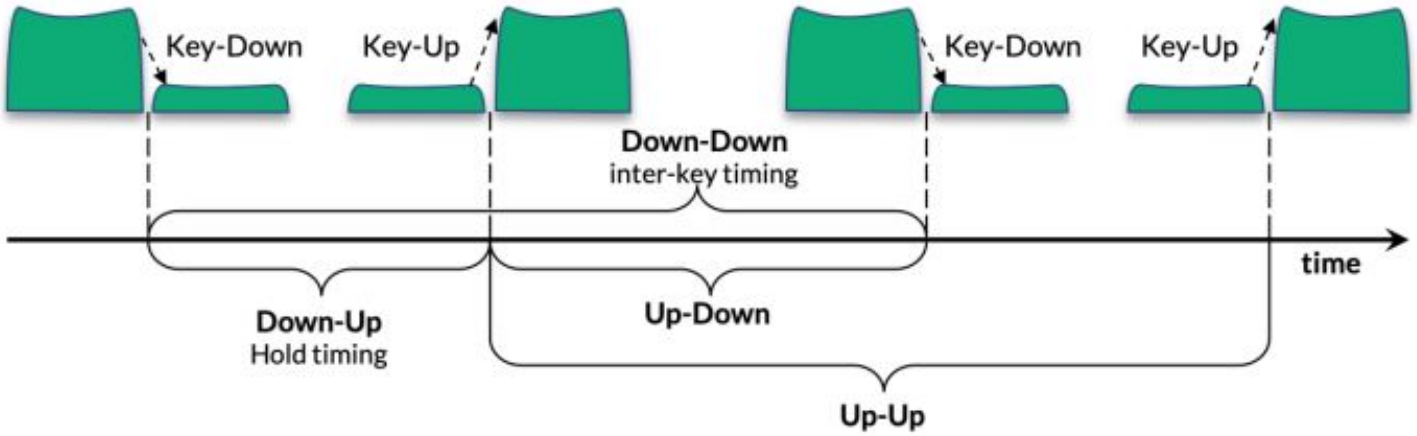
Our project considers various machine learning and deep learning techniques like CNN and RNN based on **free-text keystroke features.** Free text feature extraction, involves the most common features used today, and other keyboard dynamic works such as-

1. **Hold time (dwell time):** The duration for which the key is held down means the time between pressing the button and releasing the button.

2. **Down-Down time:** This is a time between when key1 was pressed, and key2 was pressed.

3. **Up-Down Time:** This is the time between when key1 was released to when key2 was pressed.

Methodology



The keystroke timing scheme in addition to these features, we will experiment with adding the ASCII code of the pressed buttons.

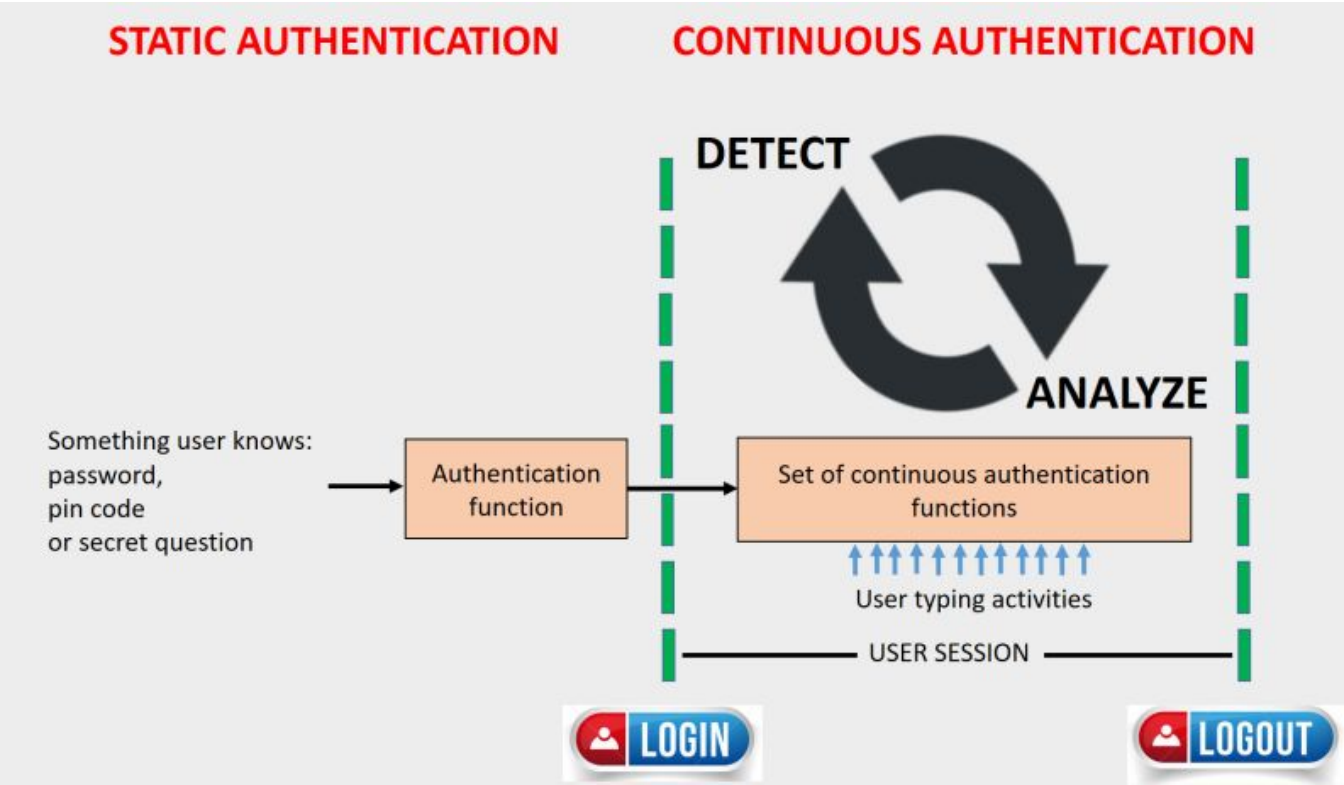
Key Differentiators & Adoption Plan

- The proposed solution is based on **Behavioral biometrics** which analyzes a user's digital physical and cognitive behavior to distinguish between cybercriminal activity and legitimate customers, identifying fraud and identity theft.
- The behavioral biometric of **Keystroke Dynamics** uses the manner and rhythm in which an individual types characters on a keyboard or keypad.
- The keystroke rhythms of a user are measured to develop a **unique biometric template** of the user's typing pattern for future authentication.
- It works **passively in the background** of a user web or mobile session to monitor thousands of parameters, such as the way a person holds the phone or how they scroll or toggle between fields, the typing speed etc.
- Once a user's profile has been learned, their gestures are secretly observed in real time to ensure that their identification is maintained. If the system notices irregularities in the behavioral patterns that don't fit the profile, it can prompt for **additional forms of verification, prohibit access, or lock the device down completely.**

Societal Impact

- Stolen phones/e-gadgets cannot be used which reduces misuse of banking information.
- ATM frauds due to card skimming can be nullified.
- Stolen credentials become useless.
- Prevents User Substitution.
- Employee productivity and accountability.
- Personal Privacy Protection.
- Helps create a world of TRUST and EASE.

GitHub Repository Link & supporting diagrams, screenshots



https://github.com/kush2702/behavioral-biometric

TECHGIG

WELCOME to the new world of AUTHENTICATION

Thank You

Team member names -

1. K Divyasri
2. Kushagra Gupta
3. Lakshya Khandelwal
4. Praneeth Shetty