🔐Smart Behavior-Based Keylogger

Author: YUVARAJ S

Table of Contents:

1. Abstract

This project presents a basic Python-based keylogger system capable of capturing and classifying user keystrokes based on behavior. The logged data is saved in plain text as well as encrypted format to ensure secure storage. The project is designed for educational and research purposes, primarily targeting cybersecurity learning environments.

2. Introduction

In the world of cybersecurity, understanding how malicious software operates is crucial for developing robust defenses. This keylogger project helps ethical hacking and cybersecurity students to understand the fundamentals of keystroke logging, secure data storage, and basic user behavior classification. This tool captures keystrokes, measures typing delays, and stores data securely.

3. Tools & Technologies Used

1. Python 3 – Core programming language
2. pynput – For capturing keyboard events
3. cryptography (Fernet) – To securely encrypt log files
4. datetime – For timestamping each logged entry
5. re – To classify behavior (e.g., URL, command, general text)
6. virtual environment – Isolated Python environment for project dependencies

4. Steps Involved in Building the Project

Environment Setup

- Created a virtual environment
- Installed required Python packages (pynput, cryptography)

Project Structure

- Created keylogger_uv/ module with core.py, clic.py, and __init__.py
- Added setup.py for packaging
- Configured CLI using entry_points to create the keyvi command

Keylogger Core Functionality

- Captures keyboard events
- Measures typing delay between keys
- Uses rule-based logic (heuristics) to classify input as password, command, URL, or general text

Encryption & Logging

- Generates and stores a secure encryption key (Fernet)
- Logs data in both plain text and encrypted binary format

Command-Line Interface (CLI)

- Provides options to start logging, analyze plain logs, and decrypt encrypted logs

Packaging & Execution

- Used setuptools for project packaging
- Enabled keyvi command execution from terminal

5. Conclusion

This project provides a hands-on understanding of how keyloggers function and how logs can be securely stored. It serves as a useful tool for cybersecurity enthusiasts and ethical hackers to explore behavioral data collection and protection mechanisms. While no AI was integrated, the project lays a foundation that can be expanded with AI-based analysis in the future.