# PROJECT REPORT – KEYLOGGER IMPLEMENTATION

**Internship Project – Cybersecurity & Ethical Hacking**

**Author:** D. Sai Srinivas Reddy

**B.Tech – Computer Science and Engineering**

**Vignan's LARA Institute of Technology and Science**

**Email:** saisrinivasreddy456@gmail.com

**Date:** 08-07-2025

## 🔍 PROJECT OBJECTIVE

The objective of this project is to implement a keylogger strictly for educational and ethical cybersecurity awareness purposes. This tool helps demonstrate how malicious keyloggers operate and how one can detect or prevent such attacks. It serves as a learning tool to understand threats related to keystroke logging and how attackers can misuse them.

## 🚀 KEY FEATURES

- Logs every keystroke with accurate timestamp
- Runs silently in the background (stealth mode using `--noconsole`)
- Automatically creates log files inside a `logs/` folder
- Multi-threaded listener ensures smooth performance
- Can be packaged into a `.exe` using PyInstaller
- Includes clear ethical use disclaimer in source code

## 🛠️ TECHNOLOGIES USED

| Area | Tool / Library |
|---|---|
| Language | Python 3.12 |
| Keystroke Logging | pynput |
| Log Management | logging, datetime |
| Background Execution | Python threading |
| Packaging to Executable | pyinstaller |

## ⚠ ETHICAL USE DISCLAIMER

This project is intended strictly for cybersecurity education and research. It must not be used for spying, illegal surveillance, or unauthorized activity. Misuse of this tool is unethical and legally punishable. The tool was developed solely for training and awareness under professional guidance.

## 📘 HOW IT WORKS

- The Python script uses `pynput` to listen to keyboard events.
- Every key pressed is recorded and written to a log file.
- Log files are timestamped and stored in a `/logs/` folder.
- The tool runs in the background and can be compiled into a `.exe` for real-world simulation.
- It demonstrates what data a malicious keylogger could capture if deployed.

## 📁 FINAL FOLDER STRUCTURE

```
Keylogger_Project/
├── keylogger.py
├── keylogger.exe
├── logs/
│   └── keystroke_log_<timestamp>.txt
├── README.md
└── Project_Report_Keylogger.pdf
```

## ✅ CONCLUSION

This keylogger project demonstrates a realistic attack vector used in cybersecurity breaches. Through this exercise, I understood how keyloggers work internally and the seriousness of such threats. The project strengthened my skills in ethical hacking, Python automation, and defensive thinking in cybersecurity. This tool will remain part of my ethical toolkit for awareness, prevention, and education.