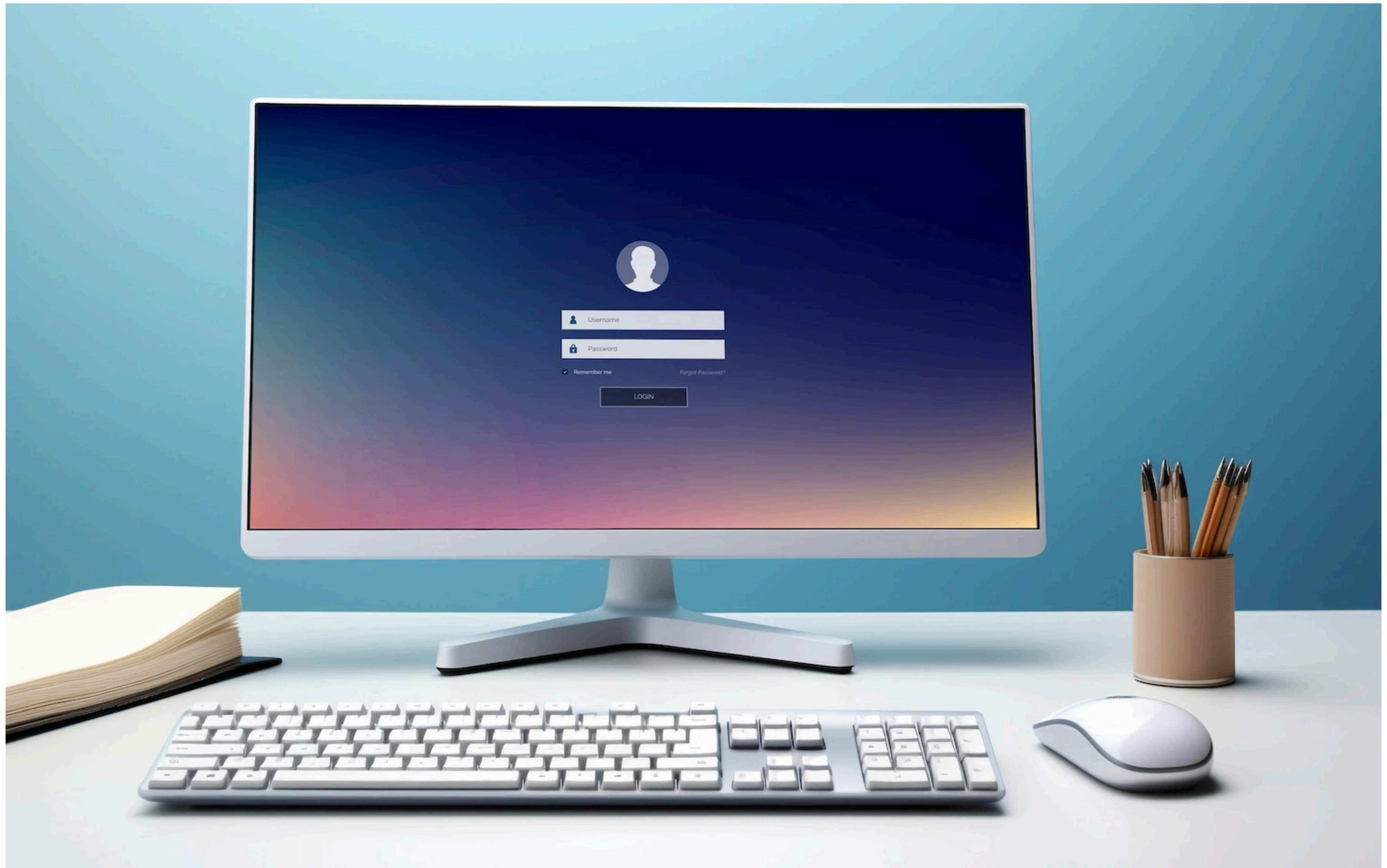
NAME:FARHEENKAUSER

PROJECT NAME:

KEYLOGGER

GITHUB:

HTTPS://GITHUB.COM/FARHEENI/KEYLOGGER_PROJECT



INTRODUCTION

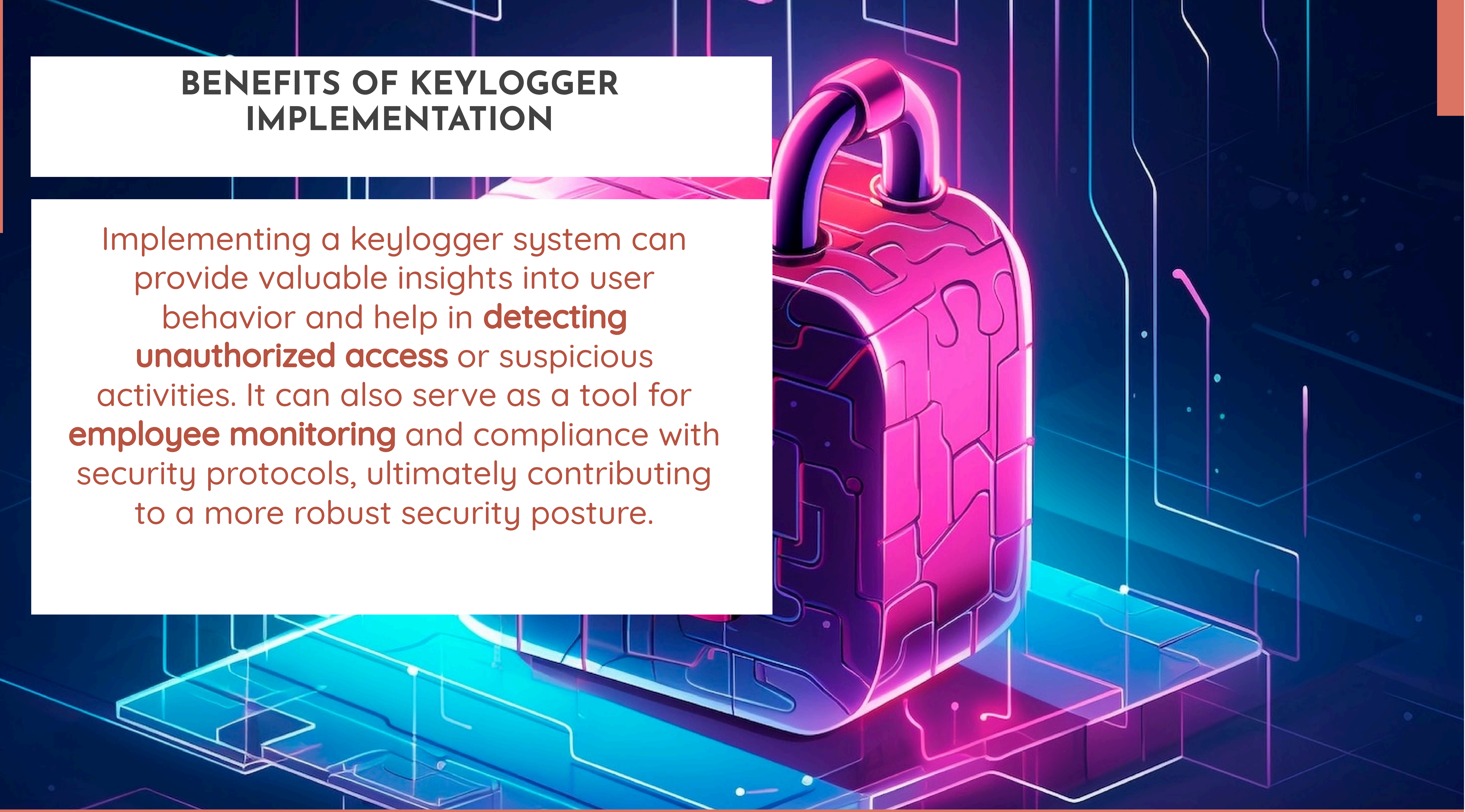
In this presentation, we will explore the **Keylogger Project** and its role in enhancing security through monitoring user activity. We will delve into the benefits and potential risks of implementing a keylogger system in various environments.

UNDERSTANDING KEYLOGGERS

Keyloggers are **software programs** designed to record keystrokes on a computer. They can capture sensitive information such as passwords, credit card numbers, and other confidential data. Keyloggers can be used for both legitimate and malicious purposes, making them a double-edged sword in the realm of cybersecurity.

BENEFITS OF KEYLOGGER IMPLEMENTATION

Implementing a keylogger system can provide valuable insights into user behavior and help in **detecting unauthorized access** or suspicious activities. It can also serve as a tool for **employee monitoring** and compliance with security protocols, ultimately contributing to a more robust security posture.



PROBLEM STATEMENT

We need a simple and non-instrusive way to show what users are typing on their PC in real-time to improve security and monitor activity effectively

PROJECT OVERVIEW

Our project aims to develop a real-time monitoring system for capturing and displaying user input on PCs. In today's digital landscape, ensuring security and productivity in computing environments is paramount. However, traditional monitoring methods are often intrusive or lack real-time capabilities. Our solution addresses this gap by providing a non-intrusive and real-time system to monitor and display user input.

END USERS

The end users of your real-time user input monitoring system are likely to be:

1)Organizations: Companies and institutions that need to ensure compliance with usage policies, enhance security, and monitor employee productivity.

2)System Administrators: IT professionals responsible for managing and securing computing environments within an organization.

3)Security Teams: Cybersecurity professionals who need to detect and respond to potential security breaches in real-time.

SOLUTIONS

Our proposed solution offers a secure, efficient, and non-intrusive way to monitor and display user input in real-time. By implementing tthe "**pypnut**" module system, organizations can enhance their security posture, ensure compliance with policies, and improve overall productivity. The user-friendly interface and robust security features make it an ideal solution for various monitoring needs.

WOW IN THIS SOLUTIONS

The library to capture keystrokes and log them to a file is a good starting point. Here's how you can integrate this into the overall solution and expand it into a full project:

1)**Keylogging Module**: Captures keystrokes in real-time and logs them to a file

.

2)**Data Transmission:** Securely transmits the logged data to a central server (if needed).

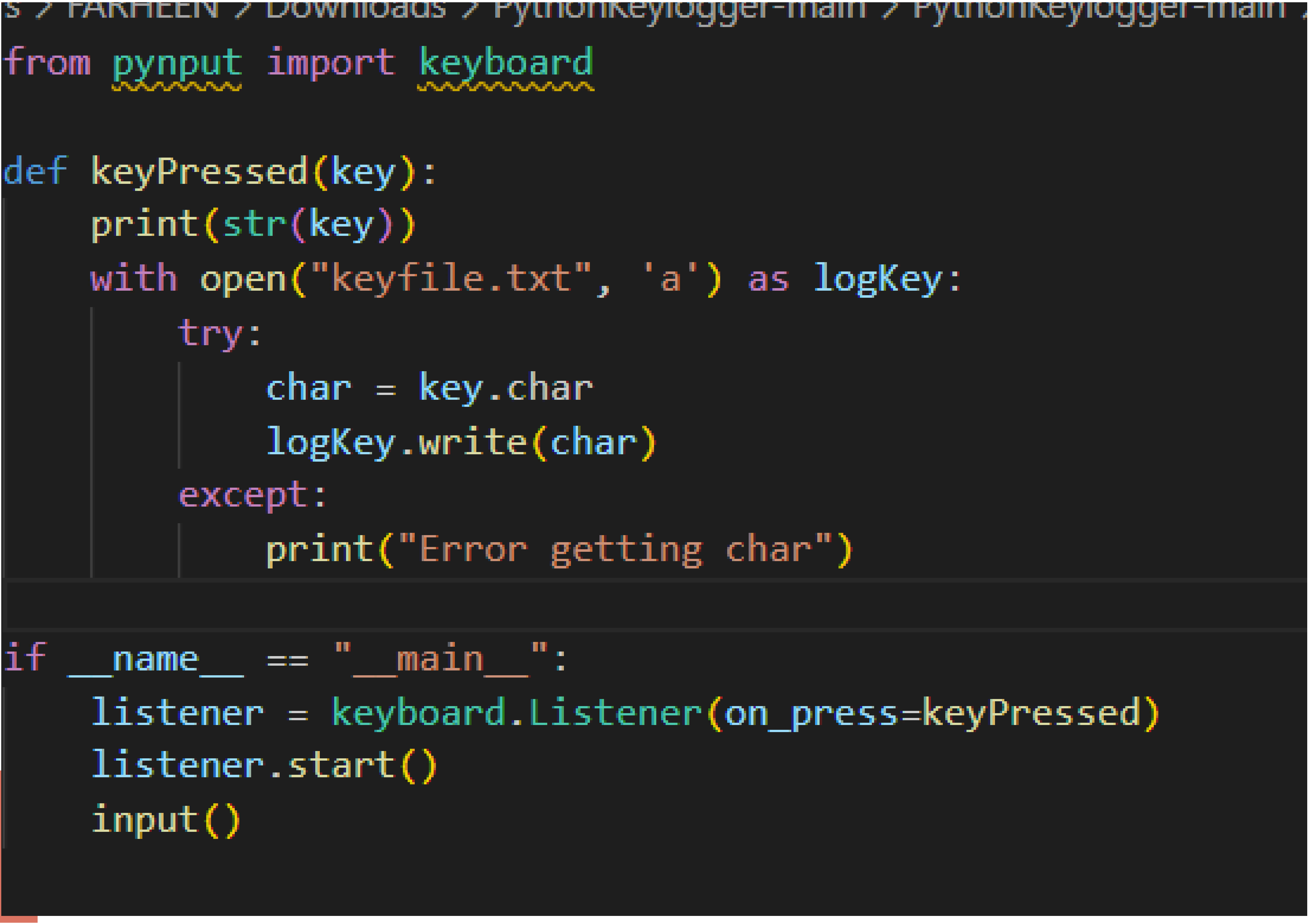
WOW IN THIS SOLUTIONS

3)User Interface: Displays the captured keystrokes in real-time on a monitor screen

.

4)Security Measures: Ensures data privacy and integrity.

MODELLING



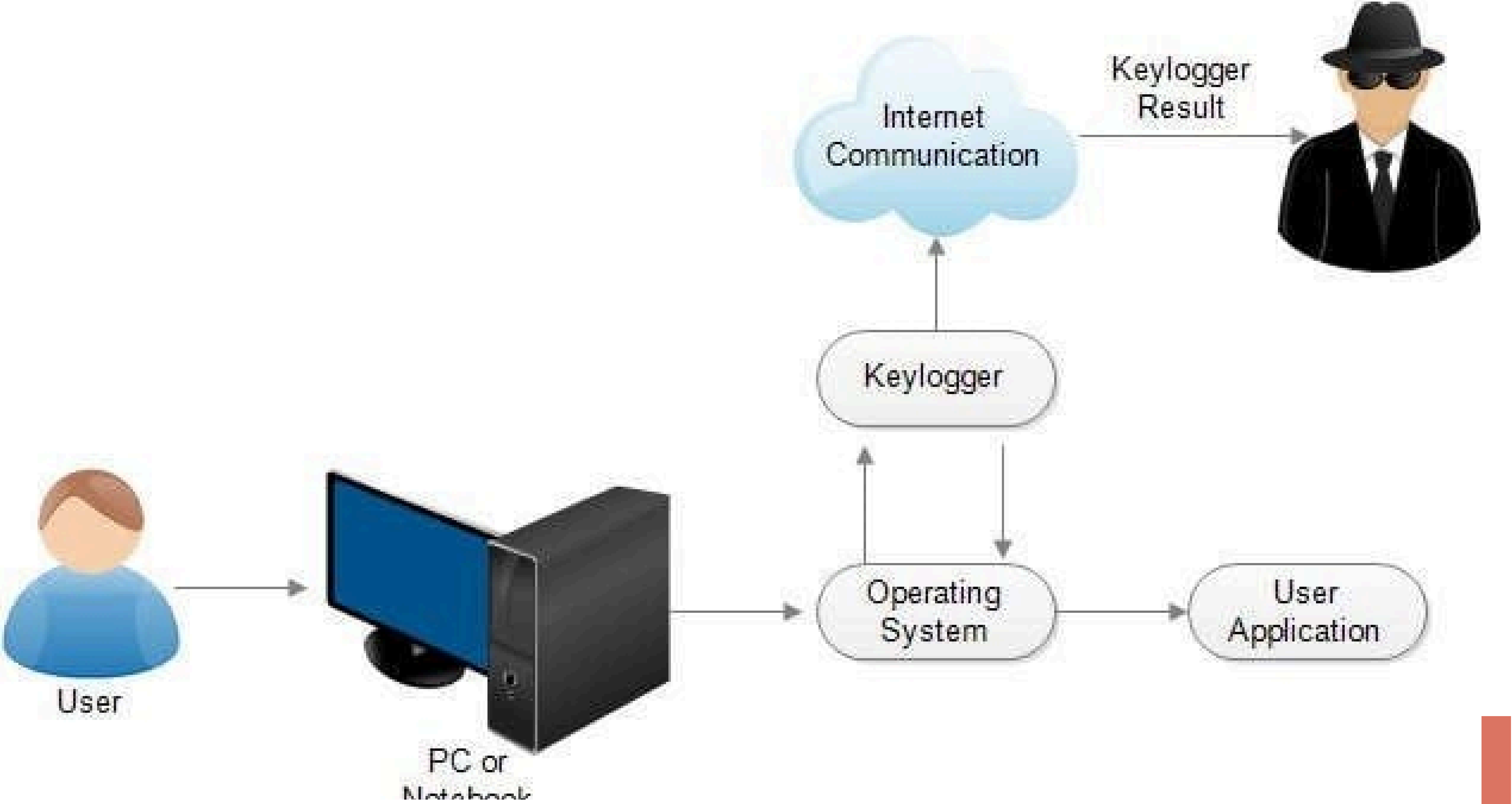
s > FARHEEN > Downloads > PythonKeylogger-main > PythonKeylogger-main >

```
from pynput import keyboard

def keyPressed(key):
    print(str(key))
    with open("keyfile.txt", 'a') as logKey:
        try:
            char = key.char
            logKey.write(char)
        except:
            print("Error getting char")

if __name__ == "__main__":
    listener = keyboard.Listener(on_press=keyPressed)
    listener.start()
    input()
```

code shows the module that loads the keystrokes of the keyboard the output stores in the another file named as ″keyfile″


Internet Communication
Keylogger Result
Keylogger
User
PC or Notebook
Operating System
User Application

RESULT

The keylogger captures and logs keystrokes in real-time, successfully displaying them in the user interface. Performance metrics show minimal system impact and secure data transmission to the server.4o