



**INFORMATION SECURITY ANALYSIS AND AUDIT
CSE 3501
J-COMPONENT REPORT**

**TOPIC:
MONITORING STUDENT ACTIVITY DURING ONLINE
EXAMS USING KEYLOGGING**

TEAM MEMBERS:

IMMANI SRI SATYA SAI	(18BIT0084)	immanisri.satyasai2018@vitstudent.ac.in
MYSORE VENKATA SIVA SAI SANDEEP	(18BIT0015)	venkata.sivasandeep2018@vitstudent.ac.in
GVSS JAYANTH ANISH	(18BIT0204)	gvssjayanth.anish2018@vitstudent.ac.in

SLOT: G1+TG1

**UNDER THE GUIDANCE OF
PROF. JEYANTHI.N
NOVEMBER,2020**

ABSTRACT:

In this present situation everything has become online. From paying a small bill to a vast education system, most of the work is just processed in online format. One of the core parts of the education system is their examination which require strict monitoring and evaluation. The monitoring part is one of the key issues as invigilators or teachers cannot manually check each person in between exam as it is hard and time consuming. In our work, we designed a keylogger which monitors student online as well as basic computer activities by capturing certain patterns they inputted to the computer to cheat or malpractice and notifies that student name to the invigilator. This algorithm benefits the existing online examination portals and ensures best of the education system. There are several keylogging techniques in the market which are efficient and unique. Most of the keyloggers are based on Kernel code manipulation. But in our work, we just execute a simple code which logs everything in txt file, and this file evaluated to know repeated unauthorized patterns typed or inputted by students.

LITERATURE SURVEY:

1. Keyloggers: silent cyber security weapons Dr. Akashdeep Bhardwaj, Dr. Sam Goundar

There are keylogging systems based on hardware and software.

Software Key loggers:

- This kind of keyloggers is hidden inside trojans which in turn deploy keyloggers in to the system.
- These kinds of trojans entice users to click on the email attachments, download applications etc.
- Most keyloggers have predefined instructions but C&C (Command and Control) Servers may give further instructions.
- These applications have ability to hide itself from anti malware scans and be undetected.
- They are used to capture screen recording, keystrokes, and transfer specific user documents based on the attacker's command.
- In Microsoft Windows operating systems, kernel-based keyloggers execute hidden dynamic link libraries (DLLs) using hooking mechanisms.

Hardware Key loggers:

- Small physical devices connected to user system to capture data using a hardware device.
- These devices are untraceable as they use their in-built storage to store keystrokes.
- Major disadvantage is that these keyloggers need physical access and installation.

Authors divided Keylogger functionalities into five aspects:

1. **Security Functionality:** This relates to how the keylogger become invisible to the task manager and encrypting the log files and sending them to SMTP servers without user knowing about it.
2. **Monitoring options present in the keyloggers:** This relates to the operations done by keyloggers such as intercepting system logon credentials, as well as keys pressed including alphanumeric and special characters. Latest technology is also known to the keyloggers which also record File operations, copying from system memory or clipboard to other source. Some keyloggers are also know to switching on and off the camera, shutting down the applications and sometimes the whole system. Monitoring name of the applications clicked by the mouse is some advanced features of present keyloggers. Some keyloggers even monitor the on-mouse clicks and web cam and audio recorder.
3. **Monitoring user's Online activity:** This relates to logging user's online activity by capturing the

URL's and web portals accessed in various internet portals. Generating lists of incoming and outgoing emails by browser or email clients and capturing social media conversations is one of the most interesting operations of key loggers.
4. **Reporting and filtering of logs and sending them to attacker:** The reports typically contain the events, their duration for predefined applications as well as a report summary based on specific keywords.
5. **Customization:** Sends alerts based on specific key words. Some keyloggers are even scheduled to log or just limited log keystrokes only in specific websites.

Backdoor Algorithm:

In this Algorithm , Keylogger malware is silently Auto executed in the background.

User remains unknown of this malware activity.

To achieve this C&C server and user's windows operating system are used.

The attackers, set up Kali Linux System to develop a keylogger and sends it via email to user's system such that it will be embedded in a word document.

The attacker creates a keyboard listener object using pynput module and makes it ready at the C&C server such that once the user opens the email attachment, the keylogger malware will immediately start to get executed in the background, gathers and sends sensitive user information to the attacker.

They create a keylogger executable file and embed it with adobe reader. Now they set up the exploit for windows and embed the keylogger payload with the pdf. Now they set the name of the pdf such that it resembles a trustful source. Then, they send this pdf via email to the user. It also could give the attacker access to the user's system.

2) Advanced keylogger for ethical hacking

Sarita Yadav, Anuj Mahajan, Monika Prasad, Avinash Kumar

Keylogger is a malware that tracks the client's composed keystroke on the console. The goal of the keylogger is to record sensitive data of the user and send this data to the attacker. The console is the central technique for contributing printed and numerical data on the PC through creating. No knowledge is acquired from key logger but the logs recorded gives sensitive information of the console activities to the attacker.

3) You Can Type, but You Cannot Hide: A Stealthy GPU-based Keylogger Evangelos Ladakis, Lazaros Koromilas, Giorgos Vasiliadis, Michalis Polychronakis, Sotiris Ioannidis

In this paper they are using GPU instead of CPU to achieve keylogging activities. The proposed method is to monitor the system's keyboard buffer via Direct Memory Access (DMA). Here, neither any Hooks are used nor the kernel's code and data structures besides the page table are modified. The prototype implementation showed us an effective keylogger which records all user keystrokes, store them in GPU memory and even analyze the recorded data in-place, with negligible runtime overhead.

Points learned:

1) Software Keylogger are divided into two classifications:

- I. Kernel Level
- II. User Level

2. User-level keyloggers use high-level APIs to monitor keystrokes.

3. Kernel level keylogger run inside OS kernel, capture every keystroke, and hooks specific system calls or driver functions. Although kernel level keylogger is more sophisticated

and stealthier than user level keyloggers, they mostly depend on kernel code modifications and can be easily detected by kernel integrity and code attestation tools.

4. GPU based malware runs on different processors so this loop hole is used load a device specific code on the GPU. Major advantage of this system is that execution of the GPU operations does not require any administration privileges.

5. The GPU based keystroke logger consists of two main components:

1) a CPU based component that will be executed once during the bootstrap phase, with the task of locating the address of the keyboard buffer in main memory .

2. a GPU-based component via DMA, that monitors the keyboard buffer and records all keystroke events.

GPU based algorithm:

Initially the controller process periodically makes a function call instructing the GPU to invoke the keylogging GPU kernel function.

The time taken for the controller process is considered as CPU Time.

The GPU Kernel function reads the keyboard event buffer, occasionally performs simple data analysis tasks, returns to the controller process, and stays idle for a while. The Whole process will be repeated periodically with a time interval gap of around 90ms, for optimum functionality of keylogging.

4)Developing Software Based Key logger and a Method to Protect from Unknown Key loggers Sivarajeshwaran S., Ramya G., Priya G

In this paper they described about two types of key loggers

Software based keylogger is a set of computer program implanted on a machine to capture the user activity by logging keystrokes and delivering them to a third party through their email account and save them as a file in a specified folder without knowing to the owner of the computer. Keyloggers are also used for legitimate purposes such as surveillance in company and parental monitoring infrastructures.

Software based Anti keylogger are used to detect and close software in which keylogger running in stealth mode. It will be done by comparing the executable files of the running software.

Software-based keylogger have several categories based on the privileges they require to execute.

1)Keylogger with full privileges will work in kernel space

2)unprivileged keylogger work in user space.

Kernel-based: A program on the machine 'gets root' and hides itself in the OS, and starts intercepting keystrokes. Such keyloggers reside at the kernel level are difficult to detect, especially for user-mode applications that do not have root access. A keylogger using this method can act as a keyboard device driver for example, and gain access to any information typed on the keyboard as it goes to the operating system.

API-based: These keyloggers hook keyboard APIs inside a running application. The keylogger registers for keystroke events, as it is a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it. Get Async Key State, Get Foreground Window. These functions are used to get the keyboard events, mouse events and current window titles.

Protection:

Software based anti keylogger used to protect from unknown keyloggers. It will get all process running in the computer and compare the executable files of the software, if it matches then all running process of the specified software will be killed. So, keylogger running in stealth mode will also get closed.

Description of module:

Two parts:

1)keylogger

2)anti key logger

Keylogger: user based does not require any exclusive access. easy to access and get all information from user.

i.MONITORING USER DATA

Function will start and captures all the keystrokes along with title of current window.it hooks all keystrokes using keyboard API so the data will be monitored without knowledge of user.

ii.SENDING SECRET INFORMATION

2 options->save monitored data =information will be stored in a file in a particular time interval

Send data through email=send information to specified mail in particular time interval.

Can select any one

iii. MAKE THE SOFTWARE IN STEALTH MODE

Can hide software from owner but in running state. Will be runned in hidden mode.

To unhide need to press certain combination of keys mentioned by developer.

Stop button=to stop running function

Anti keylogger: detect and close the software in which keylogger is running in stealth mode in the system.

Once start scan button is pressed, we will get all running process from the operating system. It will compare whether specified executable file name and the running process executable file name get matches. If it matches then the software will be closed.

So, if any keylogger running in that software in stealth mode will also get closed. Stop scan button will stop the scanning process.

5) Keystroke logging (keylogging)T Olzak - Adventures in Security, April, 2008adventuresinsecurity.com

From this paper we learned how keyboard works. A keyboard consists of a matrix of circuits overlaid with keys. These circuits matrix is known as a key matrix, can differ between keyboard manufacturers. However, keycodes sent to a specified OS are same. The keyboard's memory buffer temporarily stores the translated character or control code and then sends it to the computer's keyboard interface. The computer's keyboard controller receives the incoming keyboard data and forwards it to the operating system. A keyboard driver is typically used to manage this part of the process. The operating system processes the keyboard input based on the current state of the OS and applications.

We also learned how keyloggers work. 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 may include Quality assurance testers, Developers and analysts studying user interaction with systems, Employee monitoring, Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behavior

6) Mobile Keylogger Detection Using Machine Learning Technique

Mobile Keylogger will be installed onto a mobile phone to monitor the activities of the user of the mobile. This system focuses to build a detection approach on mobile phones because of a Machine Learning Algorithm. This system improves the overall protection and confidentiality of mobile phone users. It observes the features based on permissions and analyses

the features with the usage of a learning model. The proposed system here is used to obtain and analyze the mobile applications by using Support Vector Machine (SVM). With this algorithm, the system is capable enough to make a differentiation between the normal and hazardous applications

7) Advantages of Remote Proctoring in Online Exams

Anny Watson

Remote Proctoring is an effective technique that helps in conducting cheat-proof exams from a remote location. It lets you assess your students/candidates/trainees across the borders by creating a secure test environment. Arranging for exam centers is a big hassle especially when the exam is being conducted on a big scale. It becomes a painful challenge for colleges and universities to provide exam centers in every location that is close to students. In the case of proctored exams, you can easily eliminate such problems and entirely depend on a good online proctoring solution that can help you manage the exams hassle-free from a remote location. Online exam proctoring gives the feasibility to the proctor to monitor candidates attempting exams from their remote location. The remote proctoring solution provides the advantage to the administrator to conduct exams with a flexible schedule. Even when the offline exams are conducted under the nose of experienced invigilators still it has high chances of being affected because of the candidate's unfavorable activities such as cheating. In online exam proctoring, the proctor has gotten multiple means to keep strict vigilance on test-takers

8) Keyloggers – content monitoring exploits

SV Krasavin - URL: <http://skrasavi.ds.uiuc.edu/Info/Keyloggers> ..., 2000 - thevespiary.org

There are many several types of exploits that can infringe on privacy and confidentiality at the machine level. Among them are interceptors, spies, trojans, and web bugs. Their main function is monitoring user's activity on a computer.

One of the higher known programs is Invisible Keylogger Stealth (IKS) which may be a commercial utility (more likely to be employed by employers than hackers)⁵ . Invisible Keylogger Stealth for Windows NT by the producer's words is that the world's first keystroke recorder which will capture even NT's "trusted path" -- alt-ctrl-del logon. According to the same commercial the program has gained favorable reviews from some of the most prominent security auditors in the business. The program is predicated on kernel-mode driver that runs silently at rock bottom level of Windows NT OS. The company assures the user will never find the driving force apart from the growing binary keystroke log file together with your input of keystrokes. All keystrokes are recorded, including the "trusted" alt-ctrl-del NT logon and keystrokes into a DOS box or Java chat room.

The champions of hardware keyloggers are Key Ghost and KeyKatcher. They have similar appearance and purposes. An attacker can install such device in but 10 seconds, regardless of what state the computer in - is logged out, password protected, locked or transitioned. to put in the

keylogger the attacker simply unplugs the keyboard cable from the rear of the PC, plugs it into one end of the device, then plug the opposite end back to the PC.

9) Implementation and Embellishment of Prevention of Keylogger Spyware Attacks

The malware attack becomes extremely deadly if they are used as a combination. In this work, they have designed an attacking scenario for keylogger spyware, which will be a combination of keylogger and spyware program. The keylogger script will store each and every keystroke which will be inserted into a file and generates a log file then the spy script emails this log file to the designer's specified address. The prevention mechanism implemented is distributed into 3 phases keylogger spyware attack, honey pot-based detection and prevention of keylogger spyware program.

10) Create a Keylogger with Python – Tutorial

<https://youtu.be/TbMKw11itQ>

Learned:

How to code a basic keystroke capturing key logger using python which captures keystrokes once you executed the python file and stores all the keystrokes in a log file and when the user pressed esc the file ends its execution and all the keystrokes are recorded in the log file.

We use a third-party module named as pynput and create a keyboard listener and then capture the keystrokes. It also refreshes the buffer in which keystrokes are temporarily stored for every 10 characters in-order to assure the efficiency of the code and secrecy to not show any lagging symptoms due to execution of code. This loop runs continuously until the user pressed the exit key assigned.

Code: (Source: Youtube)

```
import pynput

from pynput.keyboard import Key, Listener

count=0

keys=[]

def on_press(key):

    global keys,count

    keys.append(str(key))
```

```
count+=1

if count>=10:

    count=0

    write_file()

keys=[]

def write_file():

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

        for key in keys:

            k=str(key).replace("","")

            if k.find("space")>0:

                f.write("\n")

            elif k.find("Key")==-1:

                f.write(k)

f.write(k)

def on_release(key):

    if key==Key.esc:

        return False

with Listener(on_press=on_press, on_release=on_release) as listener:

    listener.join()
```

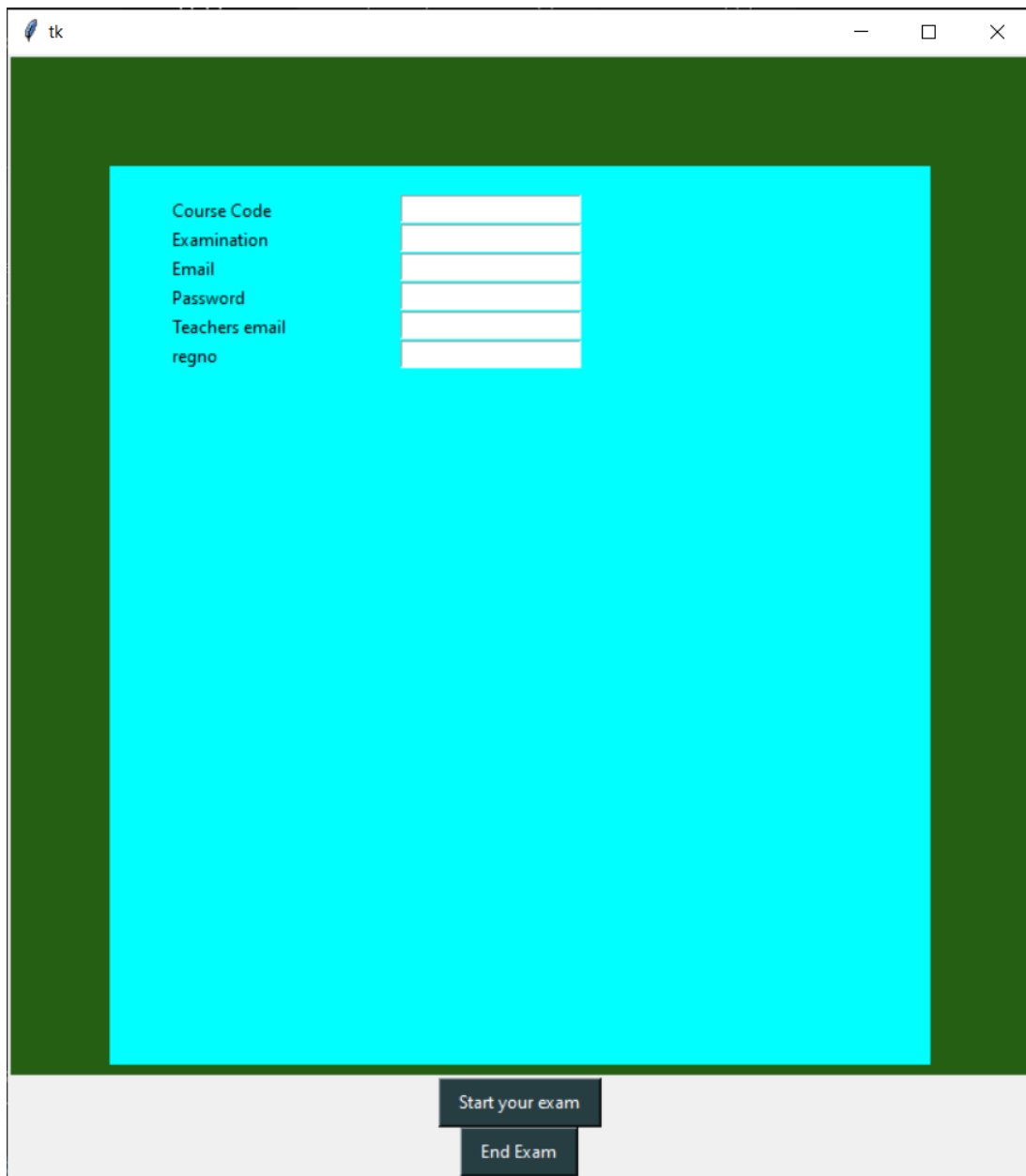
PROPOSED METHOD:

Language used: Python

Tool used: VS code (Visual Studio)

Methodology:

1. Initially the portal which is created using tkinter module in python, asks for general parameters such as registration number, email ...etc.

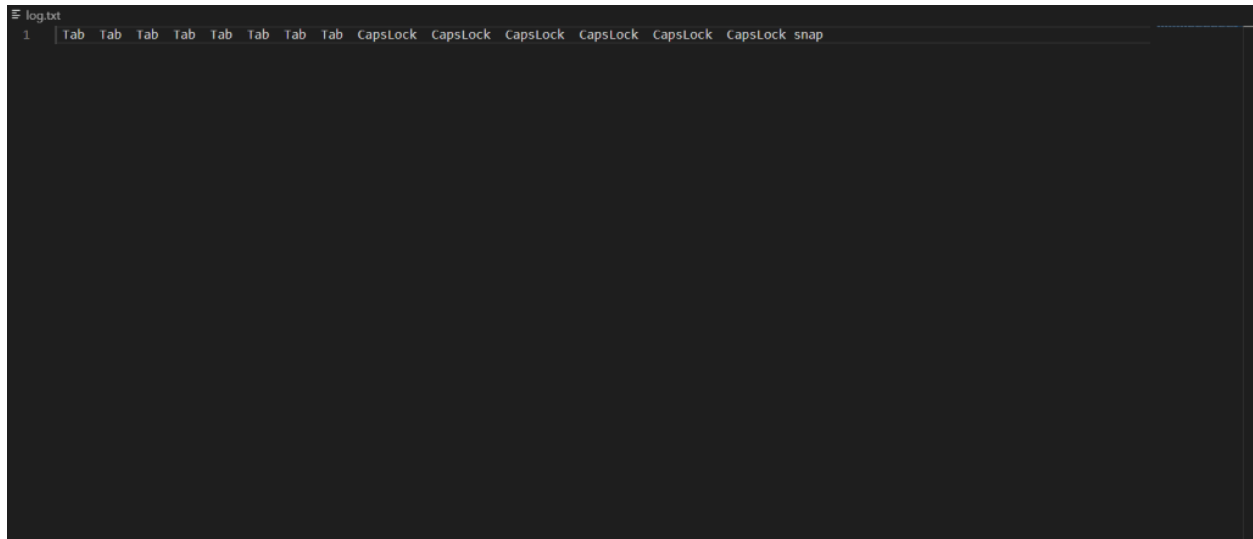


The screenshot shows a Tkinter window titled 'tk' with a dark green background. A white rectangular form is centered on the screen. The form contains the following labels and input fields:

- Course Code
- Examination
- Email
- Password
- Teachers email
- regno

Each label is followed by a white input field. At the bottom of the window, there are two buttons: 'Start your exam' and 'End Exam'.

2. Now on starting the exam the keylogger incorporated with the starts logging all the keystrokes in a text file.

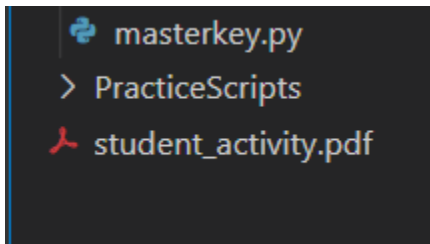


```
log.txt
1 | Tab Tab Tab Tab Tab Tab Tab Tab CapsLock CapsLock CapsLock CapsLock CapsLock CapsLock snap
```

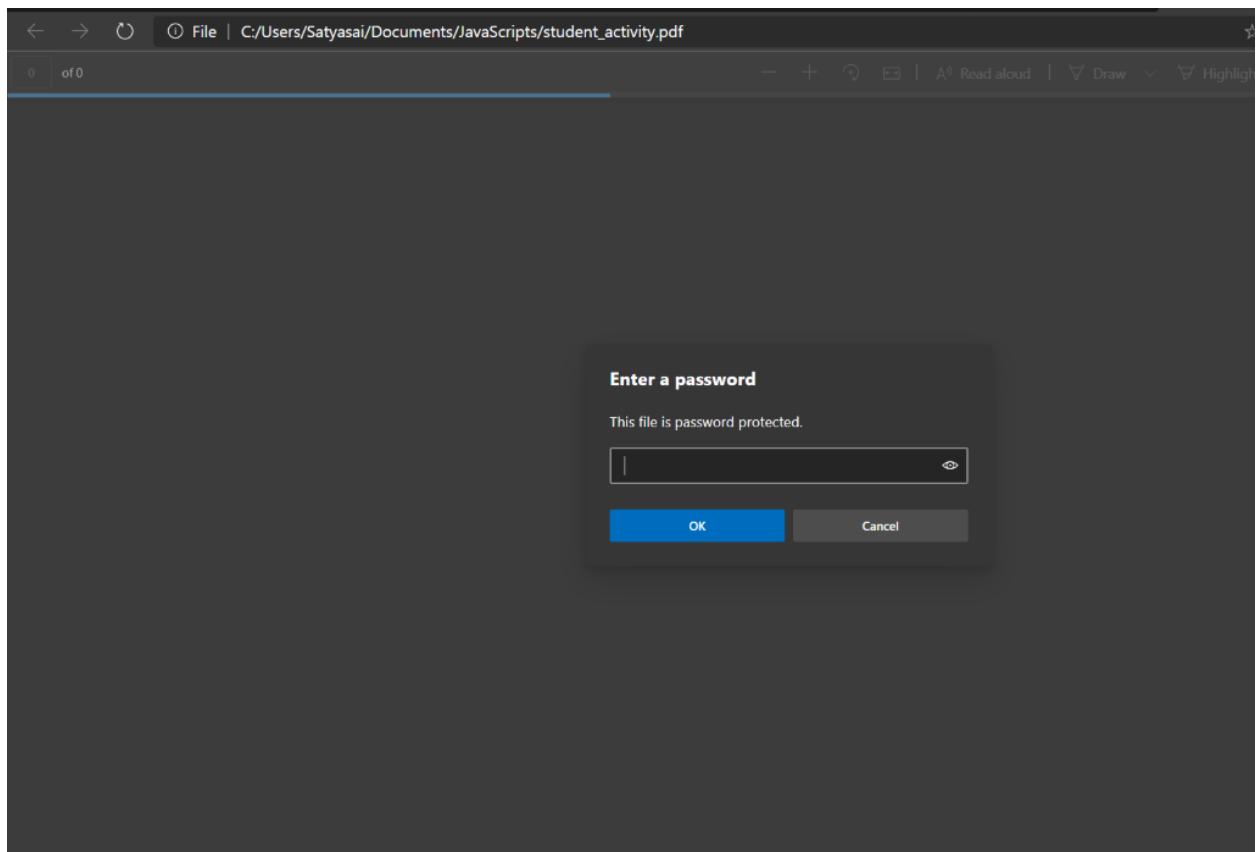
3. Here, all keycodes encoded into understandable codes.

```
if letter == 'Key.space':
    letter = ' '
if letter == 'Key.shift_r' or letter == 'Key.shift_l' :
    letter = ''
if letter == "Key.ctrl_l" or letter == "Key.ctrl_r":
    letter = " ctrl "
if letter == "Key.enter":
    letter = "\n"
if letter == 'Key.tab':
    letter=" Tab "
if letter=='Key.alt_l' or letter=='Key.alt_r':
    letter=" Alt "
if letter=='Key.caps_lock':
    letter=" CapsLock "
```

4. When student ends the exam, the code generates a pdf file where all the content of the text file is copied into this pdf.

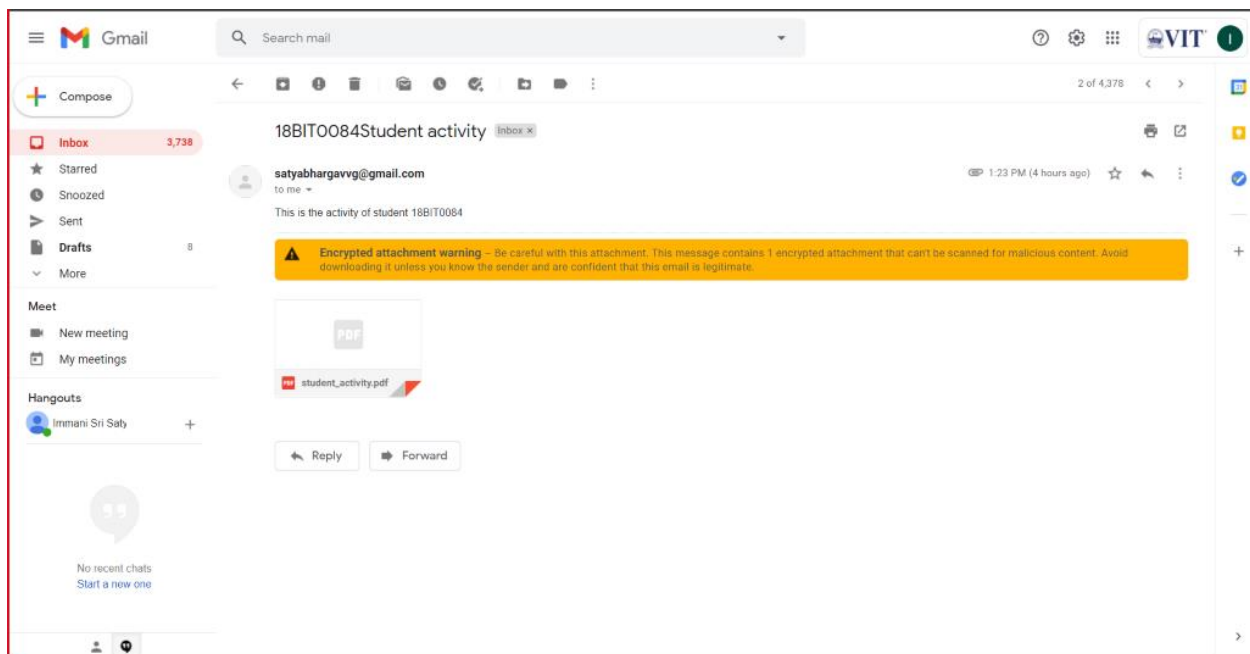


5. Now this pdf will be encrypted using a password generated by a master key regarding which only teacher knows about it.



Tab Tab Tab Tab Tab Tab Tab Tab CapsLock CapsLock CapsLock CapsLock Cap
Key.backspace ctrl \x16

6. And finally, this encrypted pdf is sent to teacher through student's mail using SMTP server initializing a secure tls server.



CODE:

```
import tkinter as tk
from tkinter import *
import os
import threading
import sys,signal
from PyPDF2 import PdfFileWriter, PdfFileReader
import numpy as np
from fpdf import FPDF
import shutil
import glob
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
from email.mime.base import MIMEBase
from email import encoders
#Master Key Generator Ceaser cipher

def Master_Key(coursecode,examtype):

    final1="".join(chr(ord(i)+5) for i in coursecode)
    final2="".join(chr(ord(i)+5) for i in examtype)

    return final1+final2

src="C:\\Users\\Satyasai\\Documents\\JavaScripts"
des="C:\\Users\\Satyasai\\Documents\\JavaScripts\\Keylogger_python"
pid=os.getpid()
#Keylogger
from pynput.keyboard import Listener

    #function that logs the records
def write_to_file(key):
    letter = str(key)
    letter = letter.replace("'", "")

    if letter == 'Key.space':
        letter = ' '
    if letter == 'Key.shift_r' or letter == 'Key.shift_l' :
        letter = ''
    if letter == "Key.ctrl_l" or letter == "Key.ctrl_r":
```

```

        letter = " ctrl "
    if letter == "Key.enter":
        letter = "\n"
    if letter == 'Key.tab':
        letter=" Tab "
    if letter=='Key.alt_l' or letter=='Key.alt_r':
        letter=" Alt "
    if letter=='Key.caps_lock':
        letter=" CapsLock "

    with open("log.txt", 'a') as f:
        f.write(letter)
    #function that starts the keylogger
def keyLogger():
    with Listener(on_press=write_to_file) as l:
        l.join()

#On exam starts
def exam_starts():
    if openFile["state"]=="normal":
        openFile["state"]="disabled"
        logger_thread=threading.Thread(target=keyLogger)
        logger_thread.start()

#On exam ends
def Exam_ends():
    #convert logged text file to protected file
    pdf = FPDF()
    pdf.add_page()
    pdf.set_font("Arial",size=14)
    fd = open("log.txt","r")
    for i in fd:
        pdf.cell(200,10,txt=i,ln=1,align="L")
    pdf.output("Studentactivity.pdf")
    fd.close()
    if os.path.exists("log.txt"):
        os.remove("log.txt")
    files=os.listdir(src)
    files2=os.listdir(des)
    os.chdir(src)
    for i in files:
        if i=="Studentactivity.pdf":
            shutil.copy(i,des)

```



```

pdf_writer=PdfFileWriter()
pdf=PdfFileReader("Studentactivity.pdf")
for i in range(pdf.numPages):
    pdf_writer.addPage(pdf.getPage(i))
passw=Master_Key(Course_code.get().lower(),Exam_type.get().lower())
pdf_writer.encrypt(passw)
print(Master_Key(Course_code.get().lower(),Exam_type.get().lower()))
with open("student_activity.pdf","wb") as f:
    pdf_writer.write(f)
    f.close()
while os.path.exists("Studentactivity.pdf"):
    os.remove("Studentactivity.pdf")
os.chdir(des)
del_files=glob.glob("*.pdf")
for i in del_files:
    os.unlink(i)
os.chdir(src)
sender_email=Stud_email.get()
sender_password=Stud_password.get()
rec_email=teacher.get()
subject=reg.get()+"Student activity"

msg=MIMEMultipart()
msg['From']=sender_email
msg['To']=rec_email
msg['Subject']=subject

body="This is the activity of student "+reg.get()
msg.attach(MIMEText(body,'plain'))

filename="student_activity.pdf"
attachment=open(filename,'rb')

part=MIMEBase('application','octet-stream')
part.set_payload((attachment).read())
encoders.encode_base64(part)
part.add_header('Content-Disposition',"attachment; filename= "+filename)

msg.attach(part)
text=msg.as_string()

server=smtplib.SMTP('smtp.gmail.com',587)
server.starttls()
server.login(sender_email,sender_password)
server.sendmail(sender_email,rec_email,text)

```

```
server.quit()
os.kill(pid,signal.SIGTERM)
#App
root=tk.Tk()

canvas=tk.Canvas(root,width=700,height=700,bg="#245F13")
canvas.pack()

frame=tk.Frame(root,bg="cyan")
frame.place(relwidth=0.8,relheight=0.8,relx=0.1,rely=0.1)

Course_code = Entry(frame,width=20)
Course_code.place(x=200,y=20)

Course_tag= Label(frame,bg="cyan",text="Course Code")
Course_tag.place(x=40,y=20)

Exam_type = Entry(frame,width=20)
Exam_type.place(x=200,y=40)

Exam_type_tag= Label(frame,bg="cyan",text="Examination")
Exam_type_tag.place(x=40,y=40)

Stud_email = Entry(frame,width=20)
Stud_email.place(x=200,y=60)

Stud_email_tag= Label(frame,bg="cyan",text="Email")
Stud_email_tag.place(x=40,y=60)

Stud_password = Entry(frame,width=20,show='*')
Stud_password.place(x=200,y=80)

Stud_password_tag= Label(frame,bg="cyan",text="Password")
Stud_password_tag.place(x=40,y=80)

teacher = Entry(frame,width=20)
teacher.place(x=200,y=100)

teacher_tag= Label(frame,bg="cyan",text="Teachers email")
teacher_tag.place(x=40,y=100)

reg= Entry(frame,width=20)
reg.place(x=200,y=120)

reg_tag= Label(frame,bg="cyan",text="regno")
```

```

reg_tag.place(x=40,y=120)
openFile=tk.Button(root, text="Start your exam",padx=10,pady=5,fg="white",bg="#263D42",command=exam_starts)
openFile.pack()

EndExam=tk.Button(root, text="End Exam",padx=10,pady=5,fg="white",bg="#263D42",command=Exam_ends)
EndExam.pack()
root.mainloop()

```

FUTURE SCOPE:

This project can be developed into a full fledged application supporting windows, linux, and mac OS. For further development we may also include the functionality to capture audio file and screenshots in certain time intervals. This ensures a strong proof availability for the teacher/invigilator in case of any wrong activities performed by the user.

CONCLUSION:

We successfully used keylogger and implemented these techniques using python for monitoring student activities during the course of an online examination. We have managed to send all the details regarding student activity as an encrypted pdf file to the email of the concerned authority. The main advantage of this system is the code is pretty simple to find errors and robust to find the application running as it will be incorporated with in a published app.

REFERNCES:

1. Keyloggers: silent cyber security weapons A Bhardwaj, S Goundar - Network Security, 2020 - Elsevier
2. ADVANCED KEYLOGGER FOR ETHICAL HACKINGS Yadav, A Mahajan, M Prasad, A Kumar - ijeast.com
3. You can type, but you can't hide: A stealthy GPU-based keylogger E Ladakis, L Koromilas, G Vasiliadis... - Proceedings of the ..., 2013 - cs.stonybrook.edu
4. Developing Software Based Key logger and a Method to Protect from Unknown Key loggers S Sivarajeshwaran, G Ramya, G Priya - ijisme.org
5. [PDF] Keystroke logging (keylogging) T Olzak - Adventures in Security, April, 2008 - adventuresinsecurity.com

6. Mobile keylogger detection using machine learning techniqueS Gunalakshmi, P Ezhumalai - Proceedings of IEEE ..., 2014 - ieeexplore.ieee.org
7. Advantages of Remote Proctoring in Online Exams? -Anny Watson- 2019
8. Keyloggers – content monitoring exploits- Serge V. Krasavin-2002
9. Keyloggers–content monitoring exploitsSV Krasavin - URL: <http://skrasavi.ds.uiuc.edu/Info/Keyloggers> ..., 2000 - the vespiary.org
10. Create a Keylogger with Python – Tutorial(<https://www.youtube.com/watch?v=TbMKwl11itQ&feature=youtu.be>)
11. Keyloggers: The Overlooked Threat to Computer Security- Kishore Subramanyam, Charles E. Frank, Donald H. Galli- Northern Kentucky University